

IBM Spectrum Protect for UNIX and Linux
Clients für Sichern/Archivieren
Version 8.1.6

Installations- und Benutzerhandbuch



IBM Spectrum Protect for UNIX and Linux
Clients für Sichern/Archivieren
Version 8.1.6

Installations- und Benutzerhandbuch



Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen“ auf Seite 845 gelesen werden.

Diese Ausgabe bezieht sich auf Version 8, Release 1, Modifikation 6 von IBM Spectrum Protect (Produktnummern 5725-W98, 5725-W99 und auf alle nachfolgenden Releases und Modifikationen, bis dieser Hinweis in einer Neuausgabe geändert wird.

© Copyright IBM Corporation 1993, 2018.

Inhaltsverzeichnis

Tabellen	xi
-----------------	-----------

Informationen zu dieser Veröffentlichung	xiii
---	-------------

Zielgruppe	xiv
Veröffentlichungen	xiv
Konventionen in dieser Veröffentlichung	xiv
Syntaxdiagramme lesen	xiv

Neuerungen für Version 8.1.6	xvii
-------------------------------------	-------------

Kapitel 1. IBM Spectrum Protect-Clients für Sichern/Archivieren installieren

Upgrade des Clients für Sichern/Archivieren durchführen	1
Upgradepfad für Clients und Server	1
Zusätzliche Informationen zum Upgrade	1
Automatische Implementierung des Clients für Sichern/Archivieren	2
Clientumgebungsvoraussetzungen	3
AIX-Clientumgebung	4
Installierbare Komponenten des AIX-Clients	4
Systemvoraussetzungen für den AIX-Client	4
Übertragungsmethoden des AIX-Clients	4
Unter AIX verfügbare Features des Clients für Sichern/Archivieren	4
HP-UX Itanium 2-API-Umgebung	5
Installierbare Komponente der Itanium 2-API	5
Systemvoraussetzungen für die HP-UX Itanium 2-API	5
Übertragungsmethoden für die HP-UX Itanium 2-API	5
Linux on Power Systems-Clientumgebung	5
Installierbare Komponenten des Linux on Power Systems-Clients	5
Systemvoraussetzungen für Linux on Power Systems-Clients	6
Übertragungsmethoden des Linux on Power Systems-Clients	6
Linux x86_64-Clientumgebung	6
Installierbare Komponenten des Linux x86_64-Clients	6
Systemvoraussetzungen für Linux x86_64-Clients	6
Übertragungsmethoden des Linux x86_64-Clients	7
Linux on System z-Clientumgebung	7
Installierbare Komponenten des Linux on System z-Clients	7
Systemvoraussetzungen für Linux on System z-Clients	7
Übertragungsmethoden des Linux on System z-Clients	7
Mac OS X-Clientumgebung	8

Installierbare Komponenten des Mac OS X-Clients	8
Systemvoraussetzungen für Mac OS X-Clients	8
Übertragungsmethoden des Mac OS X-Clients	8
Oracle Solaris-Clientumgebung	9
Installierbare Komponenten des Oracle Solaris-Clients	9
Systemvoraussetzungen für Oracle Solaris-Clients	9
Übertragungsmethoden des Oracle Solaris-Clients	9
Voraussetzungen für NDMP-Unterstützung (nur Extended Edition)	10
Installationsvoraussetzungen für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Clientdaten	10
UNIX- und Linux-Clients für Sichern/Archivieren installieren	11
AIX-Client installieren	11
AIX-Client deinstallieren	15
HP-UX Itanium 2-API installieren	15
Standardbegrenzung für Datensegmentgröße erhöhen	17
HP-UX Itanium 2-API deinstallieren	17
Client für Sichern/Archivieren unter Linux on Power Systems (Little Endian) installieren	18
Client für Sichern/Archivieren unter Linux on Power Systems (Little Endian) deinstallieren	21
Client für Sichern/Archivieren unter Ubuntu Linux on Power Systems (Little Endian) installieren	22
Client unter Ubuntu Linux on Power Systems (Little Endian) deinstallieren	24
API unter Linux on Power Systems (Big Endian) installieren	25
API unter Linux on Power Systems (Big Endian) deinstallieren	27
Linux x86_64-Client installieren	29
Linux x86_64-Client deinstallieren	32
Ubuntu Linux x86_64-Client installieren	34
Ubuntu Linux x86_64-Client deinstallieren	37
Linux on System z-Client installieren	38
Linux on System z-Client deinstallieren	41
Mac OS X-Client installieren	43
Mac OS X-Client deinstallieren	44
Oracle Solaris x86_64-Client installieren	45
Oracle Solaris x86_64-Client deinstallieren	48
Oracle Solaris SPARC-API installieren	48
Oracle Solaris SPARC-API deinstallieren	50
Softwareaktualisierungen	51
Clientverwaltungsservice zur Erfassung von Diagnoseinformationen installieren	51

Kapitel 2. IBM Spectrum Protect-Client konfigurieren 53

Tasks für Rootbenutzer und berechtigte Benutzer UNIX- und Linux-Clients	53
Benutzern ohne Rootberechtigung die Verwaltung eigener Daten ermöglichen	55
Verschlüsselung für Benutzer des Clients für Sichern/Archivieren aktivieren	56
Übersicht über die Clientoptionsdatei	56
Clientsystemoptionsdatei erstellen und ändern	58
Standardclientbenutzeroptionsdatei erstellen	60
Angepasste Clientbenutzeroptionsdatei erstellen	62
Umgebungsvariablen	63
Sprachumgebungsvariablen definieren	63
Umgebungsvariablen für die Verarbeitung definieren	64
Bourne- und Korn-Shell-Variablen definieren	66
C-Shell-Variablen definieren	66
API-Umgebungsvariablen definieren	67
Übersicht über die Konfiguration des Web-Clients	67
Web-Client auf AIX-, Linux-, Mac- und Solaris-Systemen konfigurieren	68
Scheduler konfigurieren	69
Vergleich zwischen vom Clientakzeptor verwalteten Services und traditionellen Scheduler-Services	69
Client für die Verwaltung des Schedulers durch den Clientakzeptorservice konfigurieren	70
Client-Scheduler starten	71
Ereignisse mit dem Befehlszeilenclient planen	72
IBM Spectrum Protect-Client/Server-Übertragung über eine Firewall hinweg konfigurieren	74
IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren	77
Symbolischen Link für den Zugriff auf die neueste GSKit-Bibliothek erstellen	80
Stammzertifikate von Zertifizierungsstellen	82
System für die journalbasierte Sicherung konfigurieren	83
Konfiguration des Journaldämons	83
Zeilengruppe JournalSettings	85
Zeilengruppe JournalExcludeList	86
Zeilengruppe JournaledFileSystemSettings	86
Zeilengruppen überschreiben	90
Clientseitige Datendeduplizierung	90
Client für die Datendeduplizierung konfigurieren	94
Dateien bei der Datendeduplizierung ausschließen	97
Konfiguration und Verwendung der automatisierten Clientübernahme	98
Automatisierte Clientübernahme - Übersicht	98
Voraussetzungen für die automatisierte Clientübernahme	99
Einschränkungen für die automatisierte Clientübernahme	100
Übernahmefunktionalität der IBM Spectrum Protect-Komponenten	101
Client für automatisierte Übernahme konfigurieren	102
Status replizierter Clientdaten bestimmen	104
Automatisierte Clientübernahme verhindern	105
Clientübernahme erzwingen	106

Client für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Daten konfigurieren	106
Konfiguration und Verwendung der Clusterumgebung	108
Übersicht über Clusterumgebungen	108
Aktiv/Aktiv: Pool-Clusterressourcen	108
Aktiv/Passiv: Fehlertolerant	108
Gleichzeitiger Zugriff	108
Client für Sichern/Archivieren in einer Clusterumgebung konfigurieren	108
Web-Client-Zugriff in einer Clusterumgebung aktivieren	115
Traditionelle AIXIBM PowerHA SystemMirror-Konfigurationen migrieren	117
Hinweise zur AIX-Konfiguration vor Ausführung von momentaufnahmebasierten Dateisicherungen und -archivierungen	118
NetApp und IBM Spectrum Protect für Teilsicherungen unter Verwendung der Momentaufnahme-differenz konfigurieren	119
Clustered Data ONTAP NetApp-Dateiserverdatenträger schützen	121
SnapMirror-Unterstützung für momentaufnahmegestützte progressive Teilsicherung von NetApp (snapdiff)	124
Workstation bei einem Server registrieren	128
Geschlossene Registrierung	128
Offene Registrierung	129
Einschluss-/Ausschlussliste erstellen	129
Einschluss-/Ausschlussoptionen	131
Dateibereiche und Verzeichnisse ausschließen	131
Dateien und Verzeichnisse von einer journalbasierten Sicherung ausschließen	132
Verarbeitung mit Ausschlussanweisungen steuern	132
Auszuschließende Systemdateien	134
Dateien mit Platzhalterzeichen einschließen und ausschließen	135
Dateigruppen mit Platzhalterzeichen einschließen und ausschließen	136
Beispiele für Platzhalterzeichen in Einschluss- und Ausschlussmustern	137
Verarbeitung von symbolischen Verbindungen und Aliasnamen	139
Komprimierungs- und Verschlüsselungsverarbeitung festlegen	139
Dateien in der Einschluss-/Ausschlussliste voranzeigen	140
Verarbeitung von Einschluss- und Ausschlussoptionen	141

Kapitel 3. Erste Schritte 145

Sicherheitseinstellungen des Clients konfigurieren, um die Verbindung zum IBM Spectrum Protect-Server der Version 8.1.2 und höher herzustellen	145
Konfiguration mithilfe der Standardsicherheitseinstellungen (Schnellzugriffspfad)	145
Konfiguration ohne automatische Verteilung von Zertifikaten	148
Sicherer Kennwortspeicher	151
IBM Spectrum Protect-Clientauthentifizierung	152

Java-GUI-Sitzung starten	153	Vergleich zwischen Teilsicherung nach Datum, journalbasierter Sicherung sowie NetApp-Mo- mentaufnahmedifferenzsicherung und vollstän- diger Teilsicherung und partieller Teilsicherung	188
IBM Spectrum Protect-Kennwort	154	Momentaufnahmedifferenzsicherung mit einer HTTPS-Verbindung	190
Setup-Assistent	155	Momentaufnahmedifferenzsicherung mit ei- ner HTTPS-Verbindung ausführen	191
Befehlszeilensitzung starten	155	Selektive Sicherung	192
Stapelmodus verwenden	155	Sicherungen der globalen Zone und der nicht globalen Zonen in Solaris	192
Folge von Befehlen im interaktiven Modus aus- geben	156	Zugriffsberechtigungen sichern	192
Eingabezeichenfolgen angeben, die Leerzeichen oder Hochkommas oder Anführungszeichen ent- halten	156	Virtuellen Mountpunkt definieren	193
Weitere Hinweise zum Starten	157	Daten über die Java-GUI sichern	193
Web-Client in der neuen Sicherheitsumgebung ver- wenden	158	Daten über die Befehlszeile sichern	194
Web-Client-Sitzung starten	158	Sicherungsdaten löschen.	197
Benutzerberechtigungen	159	Dateibereiche löschen.	198
Client-Scheduler automatisch starten	160	Dateien aus einem oder mehreren Dateibereichen für eine Gruppensicherung sichern (UNIX und Li- nux)	199
Kennwort ändern	160	Daten mit der Unterstützung für den Clientknoten- Proxy sichern (UNIX und Linux)	200
Dateilisten mithilfe der GUI des Clients für Sichern/Archivieren sortieren	162	Operationen mit mehreren Knoten von der GUI aktivieren	201
Onlinehilfe anzeigen	163	Verschlüsselung definieren	201
Sitzung beenden	164	Sicherungen mit der Unterstützung für den Cli- entknoten-Proxy planen	202
Onlineforen	164	Beispiele für die Planung einer Sicherung ei- nes IBM PowerHA SystemMirror-Clusters	203
Kapitel 4. Daten sichern	167	Sicherung eines GPFS-Dateisystems planen	205
Sicherungen planen	167	Lokale Momentaufnahme einem Serverdateibereich zuordnen (UNIX und Linux)	206
Welche Dateien werden gesichert?	167	Imagesicherung	206
Wann werden Dateien gesichert und wann archi- viert?	168	Vorausgesetzte Tasks vor der Erstellung einer Imagesicherung ausführen	208
Hinweise vor der Sicherung (UNIX und Linux)	169	Unterstützung für eine Imagesicherung nach Einheitentyp des Datenträgers.	209
LAN-unabhängige Datenversetzung	169	Verwendung von Imagesicherungen für die Ausführung von Dateisystemteilsicherungen	210
Voraussetzungen für die LAN-unabhängige Datenversetzung	170	Methode 1: Imagesicherungen mit Teilsiche- rungen des Dateisystems verwenden	211
Optionen für die LAN-unabhängige Daten- versetzung	170	Methode 2: Imagesicherungen mit Imageteil- sicherungen nach Datum verwenden	212
Teilsicherungen auf Systemen mit Speichereng- pässen.	170	Vergleich der Methoden 1 und 2	212
Teilsicherungen auf Systemen mit einer großen Anzahl an Dateien.	171	Imagesicherung über die GUI ausführen	213
Einschluss-/Ausschlussoptionen für die Verar- beitungssteuerung.	172	Imagesicherung über die Befehlszeile ausführen	215
Datenverschlüsselung während Sicherungs- oder Archivierungsoperationen	173	Momentaufnahmebasierte Dateisicherung und -ar- chivierung und momentaufnahmebasierte Imagesi- cherung	215
Dateisystem- und ACL-Unterstützung	174	Btrfs-Dateisysteme schützen	216
Maximale Dateigröße für Operationen	179	Btrfs-Dateisysteme sichern und zurückschreiben	217
Lange Benutzer- und Gruppennamen	179	Btrfs-Unterdatenträger sichern und zurück- schreiben.	218
Mac OS X-Datenträgernamen	180	NAS-Dateisysteme mit Network Data Management Protocol sichern	219
Hinweise in Bezug auf Mac OS X-Datenträ- gernamen	180	NAS-Dateisysteme mit der GUI des Clients für Sichern/Archivieren unter Verwendung des NDMP-Protokolls sichern	221
Hinweise in Bezug auf Datenträgernamen für Mac OS X-Dual-Boot-Systeme	181	NAS-Dateisysteme über die Befehlszeile sichern	222
Unicode-Aktivierung für Mac OS X	181	NFS-Dateien sichern	224
Mac OS X Time Machine-Sicherungsplatte.	182		
Teilsicherung, selektive Sicherung oder Teilsiche- rung nach Datum ausführen (UNIX und Linux)	182		
Vollständige und partielle Teilsicherung	183		
Journalbasierte Sicherung unter AIX und Li- nux.	185		
Teilsicherung nach Datum	187		

NFS-Dateisysteme mit der globalen Namensbereichsfunktion sichern	225
AIX-Workloadpartitionsdateisysteme sichern	226
Solaris Zettabyte-Dateisysteme (ZFS) sichern	227
Verschlüsseltes AIX JFS2-Dateisystem sichern.	228
Erweiterte AIX JFS2-Attribute sichern	229
Virtuelle VMware-Maschinen sichern	230
Umgebung für Gesamtsicherungen virtueller VMware-Maschinen vorbereiten	231
Gesamtsicherungen für virtuelle VMware-Maschinen erstellen	233
Parallele Sicherungen virtueller Maschinen	234
Tivoli Storage Manager FastBack-Daten sichern und archivieren	234
Status der Sicherungsverarbeitung anzeigen	235
Sicherung (UNIX und Linux): Weitere Hinweise	238
Gespeicherte Dateien	238
Spezielle Dateisysteme	239
NFS- oder virtuelle Mountpunkte	239
Verwaltungsklassen	239
Symbolische Verbindungen sichern	240
Beispiele: Teilsicherung oder selektive Sicherung von symbolischen Verbindungen	240
Teilsicherung nur für eine Domäne	242
Feste Verbindungen	242
Dateien mit freien Bereichen	243
Absolute und bedingte NFS-Mounts.	243
Gelöschte Dateisysteme	244
Geöffnete Dateien	244
Platzhalterzeichen	245

Kapitel 5. Daten zurückschreiben . . . 247

Image zurückschreiben	247
Image über die GUI zurückschreiben	249
Image über die Befehlszeile zurückschreiben	250
Daten aus einem Sicherungssatz zurückschreiben	250
Sicherungssätze zurückschreiben: Hinweise und Einschränkungen	253
Zurückschreibung von Sicherungssätzen	254
Sicherungssätze über die GUI zurückschreiben	255
Sicherungssätze mit der Befehlszeilenschnittstelle des Clients zurückschreiben.	256
Daten während einer Übernahme zurückschreiben oder abrufen	257
Image in Datei zurückschreiben	258
GPFS-Dateisystemdaten mit Speicherpools verwalten	259
Daten nach Zeitpunkt zurückschreiben	260
Verschlüsselte AIX-Dateien zurückschreiben	262
AIX-Workloadpartitionsdateisysteme zurückschreiben.	263
NAS-Dateisysteme zurückschreiben	264
NAS-Dateisysteme mit der GUI des Clients für Sichern/Archivieren zurückschreiben	265
Optionen und Befehle für die Zurückschreibung von NAS-Dateisystemen über die Befehlszeile	266
Aktive oder inaktive Sicherungen zurückschreiben	267
Daten über die grafische Benutzerschnittstelle zurückschreiben	267
Beispiele für Zurückschreibungsbefehle.	268

Beispiele: Große Datenvolumen über die Befehlszeile zurückschreiben	270
Standardzurückschreibung mit Abfrage, Zurückschreibung ohne Abfrage und wiederanlauffähige Zurückschreibung	271
Standardzurückschreibungsprozess mit Abfrage	271
Prozess für Zurückschreibung ohne Abfrage	271
Wiederanlauffähiger Zurückschreibungsprozess	272
Solaris Zettabyte-Dateisysteme (ZFS) zurückschreiben.	273
Zusätzliche Zurückschreibungstasks.	274
Einen anderen Benutzer zum Zurückschreiben und Abrufen Ihrer Dateien berechtigen.	274
Dateien von einem anderen Clientknoten zurückschreiben oder abrufen.	275
Dateien auf eine andere Workstation zurückschreiben oder abrufen	276
Platte nach Plattenverlust zurückschreiben	277
Dateibereiche löschen.	277
SELinux für das Zurückschreiben von Dateien auf dem Red Hat Enterprise Linux 5-Client aktivieren	278

Kapitel 6. Daten archivieren und abrufen (UNIX und Linux) 279

Dateien archivieren	279
Daten über die grafische Benutzerschnittstelle archivieren	279
Beispiele für das Archivieren von Daten über die Befehlszeile.	280
Lokale Momentaufnahme einem Serverdateibereich zuordnen	282
Daten mit dem Clientknoten-Proxy archivieren	282
Archivierungsdaten löschen	284
Erweiterte Archivierungstasks	284
Zugriffsberechtigungen	284
Symbolische Verbindungen archivieren und abrufen	285
Feste Verbindungen	286
Archivierungen abrufen	286
Daten über die grafische Benutzerschnittstelle abrufen	287
Beispiele für das Abrufen von Daten über die Befehlszeile	287
Verwaltungsklassen für die Archivierung	288

Kapitel 7. Übersicht über den IBM Spectrum Protect-Scheduler 291

Beispiele: Leerzeichen in Dateinamen in Zeitplandefinitionen	292
Bevorzugte Startzeiten für bestimmte Knoten.	293
Schedulerverarbeitungsoptionen	293
Rückkehrcodes für Zeitpläne in Zeitplanscripts auswerten	294
Rückkehrcodes von preschedulecmd- und post-schedulecmd-Scripts	295
Clientakzeptor-Scheduler-Services gegenüber traditionellen Scheduler-Services	296

Client-Scheduler-Prozess für die Ausführung als Hintergrundtask und den automatischen Start beim Systemstart definieren	297
Beispiele: Informationen zu geplanter Arbeit anzeigen.	299
Informationen zu beendeter Arbeit anzeigen	301
Planungsoptionen angeben	302
Zeitplanungsoptionen für Befehle	302
Geplante Befehle aktivieren oder inaktivieren.	302
Mehrere Zeitplananforderungen auf einem System verwalten	303

Kapitel 8. Clientrückkehrcodes 307

Kapitel 9. Speicherverwaltungsmaßnahmen 309

Maßnahmendomänen und Maßnahmengruppen	309
Verwaltungsklassen und Kopiengruppen	310
Informationen zu Verwaltungsklassen und Kopiengruppen anzeigen	311
Attribut 'Kopiengruppenname'	312
Attribut 'Kopienart'	312
Attribut 'Kopienhäufigkeit'	312
Attribut 'Versionen bestehender Daten'	312
Attribut 'Versionen gelöschter Daten'	313
Attribut 'Extraversionen aufbewahren'	313
Attribut 'Einzigste Version aufbewahren'	313
Attribut 'Kopiennummerierung'	313
Parameter für den Kopienmodus	314
Attribut 'Kopienziel'	315
Attribut 'Version aufbewahren'	315
Attribut 'Daten deduplizieren'	315
Verwaltungsklasse für Dateien auswählen	315
Dateien einer Verwaltungsklasse zuordnen	316
Verwaltungsklasse für archivierte Dateien überschreiben	317
Verwaltungsklasse für Verzeichnisse auswählen	317
Verwaltungsklassen an Dateien binden	318
Sicherungsversionen von Dateien erneut binden	319
Aufbewahrungszeitraum	319
Ereignisgesteuerte Maßnahme für Aufbewahrungsschutz	320
Dateien auf einem Datenaufbewahrungsserver archivieren	320

Kapitel 10. Verarbeitungsoptionen 323

Übersicht über die Verarbeitungsoptionen	323
Übertragungsoptionen	324
TCP/IP-Optionen	324
Optionen für Shared Memory	325
Serveroptionen	325
Verarbeitungsoptionen für Sichern und Archivieren	326
Verarbeitungsoptionen für Zurückschreiben und Abrufen	337
Planungsoptionen	340
Optionen für Format und Sprache	342
Befehlsverarbeitungsoptionen	343
Berechtigungsoptionen	343
Fehlerverarbeitungsoptionen	344
Transaktionsverarbeitungsoptionen	344

Web-Client-Optionen	345
Diagnoseoptionen	346
Optionen in Befehlen verwenden	346
Optionen mit einem Befehl eingeben	347
Ausschließlich in der Anfangsbefehlszeile gültige Optionen	353
Clientoptionen, die vom IBM Spectrum Protect-Server definiert werden können	353
Clientoptionsreferenz	355
Absolute	355
Afmskipuncachedfiles	356
Archmc	357
Archsymlinksfile	358
Asnodename	359
Sitzungseinstellungen und Zeitpläne für eine Proxy-Operation	360
Auditlogging	361
Auditlogname	363
Autodeploy	365
Autofsrename	366
Automount	368
Backmc	369
Backupsetname	370
Basesnapshotname	371
Cadlistenonport	372
Changingretries	373
Class	374
Collocatebyfilespec	375
Commethod	376
Commrestartduration	378
Commrestartinterval	378
Compressalways	379
Compression	380
Console	382
Createnewbase	383
Csv	385
Datacenter	388
Datastore	389
Dateformat	389
Dedupcachepath	393
Dedupcachesize	394
Deduplication	394
Defaultserver	396
Deletefiles	396
Description	397
Detail	398
Diffsnapshot	400
Diffsnapshotname	401
Dirmc	402
Dirsonly	403
Disablenqr	404
Diskbuffsize	405
Diskcachelocation	405
Domain	407
Domain.image	412
Domain.nas	413
Domain.vmfull	414
Dontload	421
Dynamicimage	423
Efsdecrypt	424
Enablearchiveretentionprotection	425

Enablededupcache	426	Managedservices	502
Enableinstrumentation	427	Maxcmdretries	504
Enablelanfree	429	Mbobjrefreshtresh	505
Encryptiontype.	431	Mbpctrefreshtresh	506
Encryptkey	431	Memoryefficientbackup	507
Errorlogmax.	434	Mode	509
Errorlogname	435	Monitor	512
Errorlogretention	436	Myreplicationserver.	513
Exclude-Optionen	438	Nasnodename.	515
Die Verarbeitung symbolischer Verbindungen		Nfstimeout	516
und Aliasnamen steuern.	441	Nodename	517
Steuerung der Komprimierungsverarbeitung	442	Nojournal	519
Verarbeitung von NAS-Dateisystemen	442	Noprompt	519
Exclude-Optionen für virtuelle Maschinen	443	Nrtablepath.	520
Fbbranch	446	Numberformat	521
Fbclientname	447	Optfile	523
Fbpolicyname	448	Password	524
Fbreposlocation	449	Passwordaccess.	525
Fbserver	451	Passworddir.	527
Fbvolumename	452	Pick	528
Filelist	453	Pitdate	529
Filename	456	Pittime	530
Filesonly	457	Postschedulecmd/Postnschedulecmd	531
Followsymbolic.	458	Postsnapshotcmd	533
Forcefailover	460	Preschedulecmd/Prenschedulecmd	534
Fromdate	461	Preservelastaccessdate.	536
Fromnode	461	Preservepath	537
Fromowner	462	Presnapshotcmd.	540
Fromtime	463	Queryschedperiod	541
Groupname	464	Querysummary	542
Groups (veraltet)	464	Quiet	543
Host	464	Quotesareliteral	544
Httpport	465	Removeoperandlimit	546
Hsmreparsetag	465	Replace	547
Ieobjtype	467	Replserverguid.	548
Ifnewer	468	Replservername.	550
Imagegapsize	469	Replsslport.	552
Imagetofile.	470	Repltcpport.	554
Inactive	471	Repltcpserveraddress	555
Incl excl	471	Resourceutilization.	557
Hinweise für Clients, die für Unicode akti-		Sicherungs- und Archivierungssitzungen	
viert wurden	472	steuern	558
Include-Optionen	473	Zurückschreibungssitzungen steuern	559
Die Verarbeitung symbolischer Verbindungen		Hinweise für mehrere Clientsitzungen	559
und Aliasnamen steuern.	478	Retryperiod.	560
Komprimierungs- und Verschlüsselungsver-		Revokeremoteaccess	561
arbeitung bei der Sicherung	479	Schedcmddisabled	562
Verarbeitung von NAS-Dateisystemen	479	Schedcmdexception	563
Include-Optionen für virtuelle Maschinen	480	Schedgroup	564
Incrbydate	490	Schedlogmax.	565
Incremental.	492	Schedlogname	567
Instrlogmax.	492	Schedlogretention	568
Instrlogname	493	Schedmode	570
Lanfreecommmethod	495	Schedrestretrdisabled	572
Lanfreeshmport.	496	Scrolllines.	572
Lanfreetcppport.	497	Scrollprompt	573
Lanfreessl	498	Servername	574
Lanfreetcpsveraddress	499	Sessioninitiation	576
Latest.	499	Setwindowtitle.	578
Localbackupset.	500	Shmport	579
Makesparsefile.	501	Showmembers.	579

Skipacl	580
Skipaclupdatecheck	581
Snapdiff	581
Snapdiffchangelogdir	587
Snapdiffhttps	588
Snapshotcachesize	590
Snapshotproviderfs	591
Snapshotproviderimage	592
Snapshotroot	593
Srvoptsetencryptiondisabled	595
Srvprepostscheddisabled	596
Srvprepostsnapdisabled	597
Ssl	598
Sslacceptcertfromserv	599
Ssldisablelegacytls	600
Sslfipsmode	601
Sslrequired	602
Stagingdirectory	604
Subdir	605
Tapeprompt	607
Tcpadminport	609
Tcpbuffsize	609
Tpcadaddress	610
Tcpclientaddress	611
Tcpclientport	612
Tcpnodelay	613
Tcpport	614
Tcpserveraddress	614
Tcpwindowsize	615
Timeformat	616
Toc	619
Todate	621
Totime	622
Txnbytelimit	622
Type	624
Updatectime	624
Useexistingbase	625
Usereplicationfailover	626
Users (veraltet)	627
V2archive	627
Verbose	628
Verifyimage	629
Virtualfsname	630
Virtualmountpoint	630
Virtualnodename	632
Vmbackdir	633
Vmbackuplocation	634
Vmbackupmailboxhistory	636
Vmbackuptype	636
Vmchost	637
Vmcpw	638
Vmctlmc	639
Vmcuser	640
Vmdatastorethreshold	641
Vmdefaultdvportgroup	643
Vmdefaultdvswitch	644
Vmdefaultnetwork	645
Vmenabletemplatebackups	646
Vmlimitperdatastore	648
Vmlimitperhost	649
Vmmaxbackupsessions	650

Vmmaxparallel	652
Vmmaxrestoresessions	654
Vmmaxrestoreparalleldisks	655
Vmmaxrestoreparallelvms	656
Vmmaxvirtualdisks	658
Vmmc	659
Vmnoprmdisks	660
Vmnovrmdisks	661
Vmpreferdagpassive	662
Vmprocessvmwithindependent	663
Vmprocessvmwithprdm	664
Vmskipctlcompression	665
Vmskipmaxvirtualdisks	666
Vmskipmaxvmdks	667
Vmtagdatamover	668
Vmtagdefaultdatamover	670
Vmverifyifaction	673
Vmverifyiflatest	675
Vmvstorcom	676
Vmvstortransport	677
Vmtimeout	679
Webports	680
Wildcardsareliteral	681

Kapitel 11. Befehle verwenden 683

Clientbefehlssitzung starten und beenden	686
Befehle im Stapelbetrieb verarbeiten	686
Befehle im interaktiven Modus verarbeiten	687
Clientbefehle, Optionen und Parameter eingeben	688
Befehlsname	688
Optionen	688
Optionen im interaktiven Modus	689
Parameter	689
Syntax der Dateispezifikation	689
Platzhalterzeichen	691
Clientbefehlsreferenz	692
Archive	692
Archive FastBack	695
Backup FastBack	697
Backup Group	699
Backup Image	702
Statische, dynamische und Momentaufnah- meimagesicherung	705
Verwendung der Imagesicherung für die Datei- systemteilsicherung	706
Backup NAS	708
Backup VM	710
Cancel Process	719
Cancel Restore	719
Delete Access	720
Delete Archive	721
Delete Backup	722
Delete Filespace	727
Delete Group	728
Expire	729
Help	731
Incremental	732
Journalgestützte Sicherung	737
Teilsicherung nach Datum	738
Lokale Momentaufnahme einem Serverdateibe- reich zuordnen	739

Loop	739	Restore Group	784
Macro	741	Restore Image	786
Monitor Process	742	Restore NAS	789
Preview Archive	742	Restore VM	791
Preview Backup	744	Zurückschreibungsoperationen virtueller Ma-	
Query Access	745	schinen voranzeigen	803
Query Archive	745	Retrieve	805
Query Backup	748	Archivierungen aus nicht Unicode-fähigen Da-	
NAS-Dateisystemimages abfragen	750	teibereichen abrufen	808
Query Backupset	751	Schedule	808
Query Backupset ohne Parameter		Selective	810
backupsetname	753	Lokale Momentaufnahme einem Serverdateibe-	
Query Filespace	754	reich zuordnen	813
NAS-Dateibereiche abfragen	756	Set Access	814
Query Group	756	Set Event	817
Query Image	758	Set Netappsvm	819
Query Inclexcl	760	Set Password	820
Query Mgmtclass	761	Set Vmtags	826
Query Node	762	Übersicht über das Datenschutztagging.	828
Query Options	763	Darstellung von Tags in der IBM Spectrum	
Query Restore	764	Protect vSphere Client-Plug-in.	828
Query Schedule	765	Unterstützte Datenschutztags	829
Query Session	765	Vererbung von Datenschutzeinstellungen	838
Query Systeminfo	766	Tipps für das Datenschutztagging	840
Query VM	768		
Restart Restore	771	Anhang. Funktionen zur behinderten-	
Restore	771	gerechten Bedienung für die IBM	
Aus nicht Unicode-fähigen Dateibereichen zu-		Spectrum Protect-Produktfamilie	843
rückschreiben	776		
Restore Backupset	777	Bemerkungen	845
Sicherungssätze zurückschreiben: Hinweise und			
Einschränkungen	780	Glossar	849
Sicherungssätze in einer SAN-Umgebung zu-			
rückschreiben	781	Index	851
Restore Backupset ohne Parameter			
backupsetname	781		

Tabellen

1. Upgrade für den Client von verschiedenen Serverversionen	2
2. Übertragungsmethoden des AIX-Clients	4
3. Unterstützte Features unter AIX	4
4. Übertragungsmethoden für die HP-UX Itanium 2-API	5
5. Übertragungsmethoden des Linux on Power Systems-Clients	6
6. Übertragungsmethoden des Linux on Intel x86_64-Clients	7
7. Übertragungsmethoden des Linux on System z-Clients	8
8. Übertragungsmethoden des Mac OS X-Clients	8
9. Übertragungsmethoden des Oracle Solaris-Clients	9
10. HP-UX Itanium 2-Client: Sprachencodes für Installationspakete	16
11. Paketnamen, Inhalt und Standardverzeichnis	18
12. Paketnamen, Inhalt und Standardverzeichnis	22
13. Paketnamen, Inhalt und Standardverzeichnis	26
14. Kennungen der Sprachenpakete.	28
15. Paketnamen, Inhalt und Standardverzeichnis	29
16. Kennungen der Sprachenpakete.	33
17. Paketnamen, Inhalt und Standardverzeichnis	34
18. Kennungen der Sprachenpakete.	37
19. Paketnamen, Inhalt und Standardverzeichnis	39
20. Kennungen der Sprachenpakete.	42
21. Namen und Beschreibungen der Installationspakete	46
22. Namen und Beschreibungen der Installationspakete	49
23. Tasks für Roots und berechtigte Benutzer	53
24. Mac OS X-Berechtigungstools und zugeordnete IBM Spectrum Protect-Anwendungen	55
25. Vergleich zwischen vom Clientakzeptor verwalteten Services und traditionellen Scheduler-Services.	70
26. Datendeduplizierungseinstellungen: Client und Server	93
27. Optionen zum Ausschließen von Dateibereichen und Verzeichnissen	131
28. Optionen zur Verarbeitungssteuerung mit Include- und Exclude-Anweisungen.	133
29. Platzhalterzeichen und andere Sonderzeichen	136
30. Platzhalterzeichen in Include- und Exclude-Mustern verwenden	137
31. Optionen für das Steuern der Verarbeitung von symbolischen Verbindungen und Aliasnamen.	139
32. Optionen für die Steuerung der Komprimierung und Verschlüsselung	139
33. Über die GUI des Clients für Sichern/Archivieren mit Ihren Dateien arbeiten	162
34. Unterstützte Dateisysteme und ACL-Unterstützung	174
35. Maximale Dateigröße	179
36. Beispiele für die Sicherung über die Befehlszeile	194
37. Unterstützung für eine Imagesicherung nach Einheitentyp des Datenträgers	209
38. Vergleich der Methoden zur Imageteilsicherung	213
39. Vergleiche der LVM1- und LVM2-Imageoperationen	214
40. NAS-Optionen und -Befehle	223
41. Sicherungs- und Zurückschreibungsfunktionalität für virtuelle VMware-Maschinen auf Linux-Plattformen	230
42. Informationsnachrichten der Clientbefehlszeile	235
43. Einschränkungen beim Zurückschreiben von Sicherungssätzen über die GUI.	252
44. Einschränkungen beim Zurückschreiben von Sicherungssätzen über die Befehlszeile	252
45. Beispielbefehle zum Zurückschreiben von Workloadpartitionen mit der Datei dsm.opt	264
46. NAS-Optionen und -Befehle	266
47. Beispiele für Zurückschreibungsbefehle	269
48. Beispiele für Archivierungsbefehle	280
49. Verwaltung symbolischer Verbindungen für Archivieren und Abrufen	285
50. Beispiele für Befehle zum Abrufen archivierter Dateien	288
51. Beispielausgabe des Befehls 'query schedule' für klassische Zeitpläne	300
52. Beispielausgabe des Befehls 'query schedule' für erweiterte Zeitpläne	301
53. Clientrückkehrcodes und ihre Bedeutung	307
54. Standardattributwerte in der Standardverwaltungsklasse	311
55. TCP/IP-Optionen	324
56. Übertragungsoptionen für Shared Memory	325
57. Beispiel einer Clientsystemoptionsdatei	326
58. Verarbeitungsoptionen für Sichern und Archivieren	326
59. Verarbeitungsoptionen für Zurückschreiben und Abrufen.	337
60. Planungsoptionen	341
61. Optionen für Format und Sprache	342
62. Befehlsverarbeitungsoptionen	343
63. Berechtigungsoptionen	343
64. Fehlerverarbeitungsoptionen	344
65. Transaktionsverarbeitungsoptionen	345
66. Web-Client-Optionen	345
67. Diagnoseoptionen	346
68. Clientbefehlsoptionen.	348
69. Optionen, die nur in der Anfangsbefehlszeile gültig sind	353
70. Optionen, die vom IBM Spectrum Protect-Server definiert werden können	354
71. Namen der Spaltenüberschriften	386

72. Mustereinstellungen für das Zeitformat in der Konfigurationsdatei für die Ländereinstellung (Zeile t_fmt)	392	92. Befehl Expire: Zugehörige Optionen	730
73. Mustereinstellungen für das Datumsformat in der Konfigurationsdatei für die Ländereinstellung (Zeile d_fmt)	393	93. Befehl Incremental: Zugehörige Optionen	735
74. Interaktion zwischen Domänendefinitionen aus mehreren Quellen.	411	94. Befehl 'Query Archive': Zugehörige Optionen	746
75. Weitere optionale Parameter	477	95. Befehl 'Query Backup': Zugehörige Optionen	749
76. Befehl Incremental: Zugehörige Optionen	584	96. Befehl Query Backupset: Zugehörige Optionen	752
77. Auswirkungen der SSL-Einstellungen des Servers und des Clients auf den Erfolg bzw. Misserfolg von Anmeldeversuchen	603	97. Befehl Query Backupset: Zugehörige Optionen	754
78. Mustereinstellungen für das Zeitformat in der Konfigurationsdatei für die Ländereinstellung (Zeile t_fmt)	619	98. Befehl Query Filespace: Zugehörige Optionen	755
79. Mustereinstellungen für das Datumsformat in der Konfigurationsdatei für die Ländereinstellung (Zeile d_fmt)	619	99. Befehl Query Group: Zugehörige Optionen	757
80. Befehle.	683	100. Befehl Query Image: Zugehörige Optionen	759
81. Platzhalterzeichen	691	101. Befehl Query Mgmtclass: Zugehörige Optionen	762
82. Befehl Archive: Zugehörige Optionen	694	102. Befehl Query Node: Zugehörige Optionen	763
83. Befehl Archive FastBack: Zugehörige Optionen	696	103. Befehl Query Options: Zugehörige Optionen	763
84. Befehl Backup FastBack: Zugehörige Optionen	698	104. Befehl Query Systeminfo: Zugehörige Optionen	768
85. Befehl Backup Group: Zugehörige Optionen	701	105. Befehl Query VM: Zugehörige Optionen für Abfragen virtueller VMware-Maschinen.	769
86. Befehl Backup Image: Zugehörige Optionen	704	106. Befehl Restore: Zugehörige Optionen	774
87. Befehl Backup NAS: Zugehörige Optionen	709	107. Befehl Restore Backupset: Zugehörige Optionen	778
88. Befehl Delete Archive: Zugehörige Optionen	721	108. Befehl Restore Group: Zugehörige Optionen	785
89. Befehl Delete Backup: Zugehörige Optionen	725	109. Befehl Restore Image: Zugehörige Optionen	788
90. Befehl Delete Filespace: Zugehörige Optionen	727	110. Befehl Restore NAS: Zugehörige Optionen	790
91. Befehl Delete Group: Zugehörige Optionen	729	111. Befehl Restore VM: Für die Zurückschreibung virtueller VMware-Maschinen verwendete zugehörige Optionen	799
		112. Befehl Retrieve: Zugehörige Optionen	806
		113. Befehl Schedule: Zugehörige Optionen	809
		114. Befehl Selective: Zugehörige Optionen	812
		115. Vorrangregelung bei vSphere-Bestandsobjekten	839

Informationen zu dieser Veröffentlichung

IBM Spectrum Protect ist ein Client/Server-Lizenzprodukt, das Speicherverwaltungsservices in einer plattformübergreifenden Computerumgebung zur Verfügung stellt.

Mit dem Client für Sichern/Archivieren können Benutzer Dateien aus ihren Workstations oder Dateiservern im Speicher sichern oder archivieren und Sicherungsversionen und Archivierungskopien der Dateien auf ihre lokalen Workstations zurückschreiben und abrufen.

Neben dem Client für Sichern/Archivieren umfasst IBM Spectrum Protect die folgenden Komponenten:

- Ein Serverprogramm, das als Sicherungs- und Archivierungsserver für verteilte Workstations und Dateiserver ausgeführt werden kann.
Das Serverprogramm stellt außerdem Services für hierarchische Speicherverwaltung (HSM) bereit und gestattet die Ausführung von Systemen als Umlagerungsserver.
- Ein Verwaltungsclientprogramm, auf das von einem Web-Browser oder von der Befehlszeile aus zugegriffen werden kann. Mit dem Programm kann der IBM Spectrum Protect-Administrator Serveraktivitäten steuern und überwachen, Speicherverwaltungsmaßnahmen für Sicherungs-, Archivierungs- und Speicherverwaltungsservices definieren sowie Zeitpläne erstellen, um diese Services in regelmäßigen Intervallen auszuführen.
- Eine Anwendungsprogrammierschnittstelle (API), mit der Sie eine vorhandene Anwendung durch Speicherverwaltungsservices erweitern können. Wenn eine Anwendung in einem Server als Clientknoten registriert ist, kann sie Objekte im Speicher sichern, zurückschreiben, archivieren und abrufen.
- Ein Web-Client für Sichern/Archivieren, mit dem ein berechtigter Administrator, ein Help-Desk-Benutzer oder ein anderer Benutzer Sicherungen, Zurückschreibungen, Archivierungen und Abrufe mithilfe eines Web-Browsers auf einem fernem System ausführen kann.

Ergänzungen zu IBM Spectrum Protect, die jedoch separat verkauft werden, sind die Clientprogramme IBM Spectrum Protect for Space Management und IBM Spectrum Protect HSM for Windows. Diese Programme lagern auswählbare Dateien automatisch in den Speicher um, um einen bestimmten Stand freien Speicherbereichs in lokalen Dateisystemen aufrechtzuerhalten, und rufen umgelagerte Dateien automatisch zurück, wenn auf sie zugegriffen wird. Außerdem können Benutzer mit ihnen bestimmte Dateien umlagern und zurückrufen.

Die Begriffe *Hierarchische Speicherverwaltung* und *Speicherverwaltung* haben in dieser Veröffentlichung dieselbe Bedeutung.

Zugehörige Konzepte:

„Sicherungen planen“ auf Seite 167

„Neuerungen für Version 8.1.6“ auf Seite xvii

Kapitel 1, „IBM Spectrum Protect-Clients für Sichern/Archivieren installieren“, auf Seite 1

Zielgruppe

Diese Veröffentlichung enthält Anweisungen zur Installation, Konfiguration und Verwendung des IBM Spectrum Protect-Clients.

Veröffentlichungen

Die IBM Spectrum Protect-Produktfamilie umfasst IBM Spectrum Protect Plus, IBM Spectrum Protect for Virtual Environments, IBM Spectrum Protect for Databases und verschiedene andere Speicherverwaltungsprodukte von IBM®.

Die IBM Produktdokumentation finden Sie unter IBM Knowledge Center.

Konventionen in dieser Veröffentlichung

In dieser Veröffentlichung werden die folgenden Konventionen für die Schreibweise verwendet:

Beispiel	Beschreibung
autoexec.ncf hsmgui.exe	Eine Reihe von Kleinbuchstaben mit einer Erweiterung gibt Namen von Programmdateien an.
DSMI_DIR	Eine Reihe von Großbuchstaben gibt Rückkehrcodes und andere Werte an.
dsmQuerySessInfo	Fettdruck gibt einen Befehl an, den Sie in eine Befehlszeile eingeben, den Namen eines Funktionsaufrufs, den Namen einer Struktur, ein Feld innerhalb einer Struktur oder einen Parameter.
<i>timeformat</i>	Kursiver Fettdruck gibt eine Option des Clients für Sichern/Archivieren an. Bei der Einführung der Option oder in einem Beispiel wird Fettdruck verwendet.
<i>dateformat</i>	Kursivdruck wird für eine Option, den Wert einer Option, einen neuen Begriff, einen Platzhalter für von Ihnen anzugebende Informationen oder zur Hervorhebung im Text verwendet.
maxcmdretries	Monospaceschrift wird für Fragmente eines Programms oder am Bildschirm angezeigte Informationen, wie ein Befehlsbeispiel, verwendet.
Pluszeichen (+)	Ein Pluszeichen zwischen zwei Tasten gibt an, dass beide Tasten gleichzeitig gedrückt werden.

Syntaxdiagramme lesen

Folgen Sie beim Lesen eines Syntaxdiagramms für die Befehlseingabe der Linie. Lesen Sie von links nach rechts und von oben nach unten.

- Das Symbol ►— zeigt den Anfang eines Syntaxdiagramms an.
- Das Symbol —► am Ende einer Zeile zeigt an, dass das Syntaxdiagramm in der nächsten Zeile fortgesetzt wird.
- Das Symbol ►— am Anfang einer Zeile zeigt an, dass das Syntaxdiagramm aus der vorherigen Zeile fortgesetzt wird.
- Das Symbol —►◀ zeigt das Ende eines Syntaxdiagramms an.

Syntaxelemente, wie z. B. ein Schlüsselwort oder eine Variable, können sich an folgenden Positionen befinden:

- In der Linie (erforderliches Element)
- Oberhalb der Linie (Standardelement)

- Unterhalb der Linie (optionales Element)

Symbole

Geben Sie diese Symbole *exakt* so ein, wie sie im Syntaxdiagramm dargestellt werden.

- * Stern
- { } Geschweifte Klammern
- : Doppelpunkt
- , Komma
- = Gleichheitszeichen
- - Bindestrich
- () Runde Klammern
- . Punkt
- Leerzeichen
- " Anführungszeichen
- ' Einfaches Anführungszeichen (Hochkomma)

Variablen

Kursiv dargestellte Elemente in Groß-/Kleinschreibung (z. B. *<Variablenname>*) geben Variablen an. In diesem Beispiel können Sie einen *<Variablennamen>* angeben, wenn Sie den Befehl **Befehlsname** eingeben.

»—Befehlsname—*<Variablenname>*—«

Wiederholung

Ein nach links zurückweisender Pfeil bedeutet, dass Sie das Element wiederholen können. Ein Zeichen innerhalb des Pfeils bedeutet, dass Sie die wiederholten Elemente durch dieses Zeichen voneinander trennen müssen.

»—wiederholen—«

Eine Fußnote (1) neben dem Pfeil gibt an, wie oft Sie das Element wiederholen können.

»—wiederholen—«

Anmerkungen:

- 1 Geben Sie *wiederholen* maximal 5 Mal an.

Erforderliche Auswahlmöglichkeiten

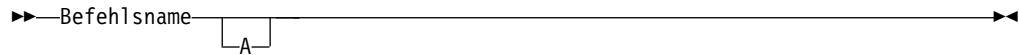
Sind zwei oder mehr Elemente übereinander angeordnet und befindet sich eines von ihnen in der Linie, *müssen* Sie eines der Elemente angeben.

In diesem Beispiel müssen Sie A, B oder C auswählen.



Optionale Auswahlmöglichkeiten

Steht ein Element *unterhalb* der Linie, ist es optional. Im ersten Beispiel können Sie A oder gar nichts auswählen.



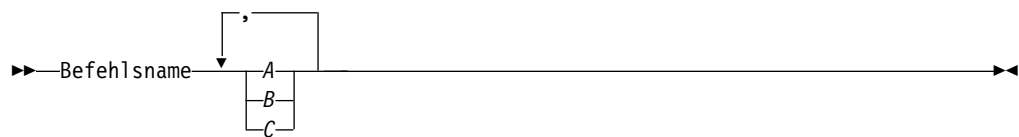
Sind zwei oder mehr Elemente unterhalb der Linie untereinander angeordnet, sind alle Elemente optional. Im zweiten Beispiel können Sie A, B, C oder gar nichts auswählen.



Wiederholbare Auswahlmöglichkeiten

Mehrere übereinander angeordnete Elemente gefolgt von einem nach links zurückweisenden Pfeil bedeuten, dass Sie mehrere Elemente auswählen können oder in einigen Fällen ein einzelnes Element wiederholen können.

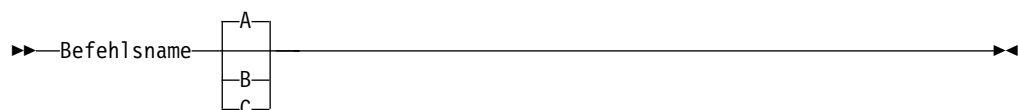
Im vorliegenden Beispiel können Sie eine beliebige Kombination aus A, B oder C auswählen.



Standardwerte

Standardwerte stehen oberhalb der Linie. Der Standardwert wird ausgewählt, wenn er nicht überschrieben wird. Sie können den Standardwert auch explizit auswählen. Wenn der Standardwert überschrieben werden soll, geben Sie eine der unterhalb der Linie aufgeführten Optionen an.

In diesem Beispiel ist A der Standardwert. Wählen Sie B oder C aus, um A zu überschreiben.



Neuerungen für Version 8.1.6

In IBM Spectrum Protect Version 8.1.6 gibt es neue Funktionen und Aktualisierungen.

Neue und geänderte Informationen in dieser Produktdokumentation sind links von der Änderung mit einem vertikalen Strich (|) gekennzeichnet.

Die folgenden Funktionen und Aktualisierungen sind neu für dieses Release:

NAS-Sicherungs- und Zurückschreibungsfunctionalität

Sie können jetzt NAS-Dateisysteme mit der GUI des Clients für Sichern/Archivieren sichern und zurückschreiben.

Informationen zum Sichern und Zurückschreiben von NAS-Dateisysteme finden Sie in den folgenden Abschnitten:

- NAS-Dateisysteme mit Network Data Management Protocol sichern
- NAS-Dateisysteme mit der GUI des Clients für Sichern/Archivieren unter Verwendung des NDMP-Protokolls sichern
- NAS-Dateisysteme zurückschreiben
- NAS-Dateisysteme mit der GUI des Clients für Sichern/Archivieren zurückschreiben

Neue Option für die flexible Konfiguration von Zurückschreibungsoperationen für mehrere VMs mithilfe einer CSV-Datei

Mit der Option `csv` kann auf einem IBM Spectrum Protect-Client eine Datei mit durch Kommas getrennten Werten (CSV-Datei) verwendet werden, um verschiedene Zurückschreibungseinstellungen für eine Reihe von Zurückschreibungsoperationen für virtuelle Maschinen zu definieren und anzuwenden.

Weitere Informationen zu dieser neuen Methode finden Sie in `Csv`.

Neue Option zum Konfigurieren der Transportkomprimierung

Data Protection for VMware unterstützt jetzt das neue NBD-Protokoll (Network Block Device) mit SSL (NBDSSL), das VMware vSphere als Transportmethode hinzugefügt wurde. Dieser LAN-Transport ist der Standardwert, wenn andere Transportmechanismen nicht verfügbar sind, und kann die erforderliche Zeit für die Übertragung einer großen virtuellen Platte durch Komprimierung verkürzen.

Weitere Informationen zu dieser neuen Option finden Sie in `Vmvmstorcom`.

Wartungsaktualisierungen

Aktualisierungen für APARs und andere untergeordnete Aktualisierungen werden bereitgestellt.

Eine Liste der neuen Funktionen und Aktualisierungen in früheren Releases der Version 8.1 finden Sie in Aktualisierungen für den Client für Sichern/Archivieren.

Zugehörige Informationen:

„Informationen zu dieser Veröffentlichung“ auf Seite xiii

Kapitel 1. IBM Spectrum Protect-Clients für Sichern/Archivieren installieren

Mit dem IBM Spectrum Protect-Client für Sichern/Archivieren können Sie die Informationen auf Ihren Workstations schützen.

Sie können Sicherungsversionen Ihrer Dateien verwalten, die Sie zurückschreiben können, wenn die Originaldateien beschädigt werden oder verloren gehen. Sie können auch selten verwendete Dateien archivieren. Die Dateien bleiben dann in ihrem aktuellen Status, und Sie können sie bei Bedarf abrufen.

Der Client für Sichern/Archivieren arbeitet zusammen mit dem IBM Spectrum Protect-Server. Bitten Sie Ihren IBM Spectrum Protect-Serveradministrator um Sicherungs- oder Archivierungszugriff auf den Server oder entnehmen Sie den Serververöffentlichungen Informationen zum Installieren und Konfigurieren des IBM Spectrum Protect-Servers.

Zugehörige Konzepte:

„Neuerungen für Version 8.1.6“ auf Seite xvii

„Sicherungen planen“ auf Seite 167

Upgrade des Clients für Sichern/Archivieren durchführen

In den folgenden Abschnitten wird erläutert, wie Sie von einer vorherigen Version ein Upgrade auf Version 8.1.6 des Clients für Sichern/Archivieren von IBM Spectrum Protect durchführen.

Upgradepfad für Clients und Server

Das Upgrade der IBM Spectrum Protect-Clients kann zu einem anderen Zeitpunkt durchgeführt werden als das der IBM Spectrum Protect-Server. Die kombinierten Server und Clients, die Sie implementieren, müssen untereinander kompatibel sein.

Um eine Unterbrechung Ihrer Sicherungs- und Archivierungsaktivitäten während eines Upgrades von einem Release auf ein anderes zu verhindern, befolgen Sie die Kompatibilitätsrichtlinien für IBM Spectrum Protect-Clients und -Server in Technote 1053218.

Informationen zum Upgrade Ihrer aktuellen IBM PowerHA SystemMirror-Konfigurationen unter AIX finden Sie in „Traditionelle AIXIBM PowerHA SystemMirror-Konfigurationen migrieren“ auf Seite 117.

Zusätzliche Informationen zum Upgrade

Wenn Sie ein Upgrade des Clients für Sichern/Archivieren durchführen, müssen Sie vor der Verwendung der neuen Client-Software zusätzliche Informationen beachten.

Bei einem Upgrade eines Clients für Sichern/Archivieren müssen Sie die folgenden Informationen berücksichtigen:

- Wenn Sie ein Upgrade für den IBM Tivoli Storage Manager-Client für Sichern/Archivieren der Version 7.1.2 oder früher unter dem Betriebssystem Oracle Solaris durchführen, lesen Sie die Informationen in „IBM Tivoli Storage Manager-Client für Sichern/Archivieren unter Oracle Solaris“ auf Seite 117.

ris durchführen, müssen Sie alle zuvor installierten Sprachenpakete deinstallieren, bevor Sie mit dem Upgrade fortfahren.

- Mac-Benutzer müssen bei Aktualisierungen für den Mac OS X-Client in IBM Spectrum Protect Version 6.3 oder höher Folgendes berücksichtigen:
 - Wenn Sie den in diesem Release bereitgestellte Mac OS X-Client verwenden, müssen die Dateien dsm.sys und dsm.opt unter Verwendung von Unicode (UTF-8) codiert werden. Die UTF-8-Codierung gestattet die Verwendung von Zeichen aus beliebigen Sprachen in den Optionsdateien. Falls Ihre Dateien dsm.sys und dsm.opt zuvor mit dem Format MacRoman (oder einem beliebigen anderen Format als UTF-8) codiert waren, öffnen Sie diese Dateien in einem Editor (z. B. TextEdit) und speichern Sie die Dateien mit der UTF-8-Codierung und ohne die Erweiterung .txt. Ihre Einschluss-/Ausschlusslisten können entweder mit UTF-8 oder mit UTF-16 codiert werden. Weitere Informationen zu Unicode finden Sie in „Hinweise für Clients, die für Unicode aktiviert wurden“ auf Seite 472.
 - IBM Spectrum Protect-Serverdateibereiche, die von Mac OS 9-Clients erstellt wurden, können nicht durch den in IBM Spectrum Protect Version 6.3 bereitgestellten Mac OS X-Client verwaltet werden. Verwenden Sie den Befehl `q file Knoten f=d` auf dem Server, um die für einen Knoten gesicherten Dateien aufzulisten. Alle Dateien der Mac-Plattform, die nicht mit einem Schrägstrich (/) beginnen, wurden wahrscheinlich durch einen älteren Mac-Client erstellt. Diese Dateien können mit dem in diesem Release bereitgestellten Mac OS X-Client weder zurückgeschrieben noch anderweitig verwaltet werden. Die Verwaltung dieser Dateien ist zwar möglich, muss jedoch mit einem Mac-Client erfolgen werden, der auf einem Clientknoten der Version 6.2.2 oder älter installiert ist.
- Eine Liste der Nachrichten, die seit dem vorherigen IBM Spectrum Protect-Release hinzugefügt oder geändert wurden, finden Sie in der Datei `client_message.chg` im Clientpaket.

Automatische Implementierung des Clients für Sichern/Archivieren

Der IBM Spectrum Protect-Serveradministrator kann einen Client für Sichern/Archivieren automatisch implementieren, um Workstations zu aktualisieren, auf denen der Client für Sichern/Archivieren bereits installiert ist.

Der IBM Spectrum Protect-Server kann so konfiguriert werden, dass für Clients für Sichern/Archivieren auf Client-Workstations ein Upgrade automatisch durchgeführt wird. Die vorhandenen Clients für Sichern/Archivieren müssen Version 6.4.3 oder höher verwenden.

Die Prozedur für die automatische Implementierung von Client-Upgrades hängt von der Version des IBM Spectrum Protect-Servers ab, von dem der Client aktualisiert wird. Die folgende Tabelle zeigt die Prozeduren für das Client-Upgrade für verschiedene Versionen des Servers.

Tabelle 1. Upgrade für den Client von verschiedenen Serverversionen

Serverversion	Zielclientversion	Prozedur
Version 8.1.3 oder höher	Version 7.1.8 oder höhere V7-Release Version 8.1.2 oder höhere V8-Release	Klicken Sie das IBM Spectrum Protect Operations Center. Weitere Informationen finden Sie in Clientaktualisierungen planen.

Tabelle 1. Upgrade für den Client von verschiedenen Serverversionen (Forts.)

Serverversion	Zielclientversion	Prozedur
Version 8.1.2	Version 7.1.8 oder höhere V7-Release Version 8.1.2 oder höhere V8-Release	IBM-Technote 2004596.
Version 7.1.8 oder frühere V7-Release Version 8.1.1 oder frühere V8-Release	Version 7.1.6 oder frühere V7-Release Version 8.1.0	IBM-Technote 1673299.

Einschränkungen: Für die automatische Clientimplementierung gelten die folgenden Einschränkungen:

- Die Windows-Clusterserviceumgebung wird nicht unterstützt.
- Nur der Client für Sichern/Archivieren kann vom IBM Spectrum Protect-Server aus implementiert werden. Andere zugehörige Produkte wie z. B. IBM Spectrum Protect for Space Management, IBM Spectrum Protect HSM for Windows, IBM Spectrum Protect for Virtual Environments und andere Data Protection-Produkte werden nicht unterstützt. Wenn Sie versuchen, ein nicht unterstütztes Produkt zu implementieren, wird die Implementierung gestoppt und eine Fehlernachricht angezeigt.
- 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

Zugehörige Verweise:

„Autodeploy“ auf Seite 365

Clientumgebungsvoraussetzungen

Für jeden der IBM Spectrum Protect-Clients bestehen Hardware- und Softwarevoraussetzungen.

Die folgende Liste enthält die Position der Umgebungsvoraussetzungen für jede unterstützte Plattform.

- „AIX-Clientumgebung“ auf Seite 4
- „HP-UX Itanium 2-API-Umgebung“ auf Seite 5
- „Linux on Power Systems-Clientumgebung“ auf Seite 5
- „Linux x86_64-Clientumgebung“ auf Seite 6
- „Linux on System z-Clientumgebung“ auf Seite 7
- „Mac OS X-Clientumgebung“ auf Seite 8
- „Oracle Solaris-Clientumgebung“ auf Seite 9
- „Voraussetzungen für NDMP-Unterstützung (nur Extended Edition)“ auf Seite 10

Aktuelle Informationen zu den Clientumgebungsvoraussetzungen für alle unterstützten Plattformen des Clients für Sichern/Archivieren finden Sie in Technote 1243309.

AIX-Clientumgebung

Dieser Abschnitt enthält Informationen zur Clientumgebung, zu Komponenten des Clients für Sichern/Archivieren und zu den Hardware- und Softwarevoraussetzungen für die AIX-Plattform.

Installierbare Komponenten des AIX-Clients

Der Client für Sichern/Archivieren besteht aus mehreren installierbaren Komponenten.

Installierbare Komponenten für den AIX-Client:

- Befehlszeilenclient für Sichern/Archivieren
- Verwaltungsclient
- Grafische Benutzerschnittstelle des Clients für Sichern/Archivieren, die Oracle Java™-Technologie verwendet
- Web-Client für Sichern/Archivieren
- IBM Spectrum Protect-64-Bit-API

Die API kann separat installiert werden. Alle anderen Komponenten werden bei der Installation des AIX-Pakets (`tivoli.tsm.client.api.64bit`) installiert.

Systemvoraussetzungen für den AIX-Client

Für den AIX-Client von IBM Spectrum Protect gelten Mindestanforderungen an die Hardware, den Plattenspeicherplatz, den Hauptspeicher und die Software.

Informationen zu den Hardware- und Softwarevoraussetzungen für alle unterstützten Versionen der AIX-Clients, einschließlich der neuesten Fixpacks, finden Sie in Technote 1052226.

Übertragungsmethoden des AIX-Clients

Für den AIX-Client für Sichern/Archivieren sind die Übertragungsmethoden TCP/IP und Shared Memory verfügbar.

Sie können die folgenden Übertragungsmethoden für den AIX-Client von IBM Spectrum Protect Version 8.1.6 verwenden:

Tabelle 2. Übertragungsmethoden des AIX-Clients

Zur Verwendung dieser Übertragungsmethode:	Diese Software installieren:	Um Verbindung zu diesen IBM Spectrum Protect-Servern herzustellen:
TCP/IP	TCP/IP (Standard bei unterstützten AIX-Plattformen)	AIX, Linux, Windows
Shared Memory	TCP/IP (Standard bei unterstützten AIX-Plattformen)	AIX

Unter AIX verfügbare Features des Clients für Sichern/Archivieren

In diesem Abschnitt sind die Features aufgelistet, die unter AIX unterstützt werden.

Tabelle 3. Unterstützte Features unter AIX

Features	Unter AIX unterstützt?
Befehlszeile und GUI für Sichern/Archivieren	yes

Tabelle 3. Unterstützte Features unter AIX (Forts.)

Features	Unter AIX unterstützt?
Journalbasierte Sicherung	Ja
LAN-unabhängige Operationen	yes
Online-Imagesicherung	yes
Offline-Imagesicherung	yes

HP-UX Itanium 2-API-Umgebung

Lesen Sie die Informationen zur API-Umgebung, zu installierbaren Komponenten sowie zu Hardware- und Softwarevoraussetzungen für die HP-UX Itanium 2-Plattform.

Installierbare Komponente der Itanium 2-API

In IBM Spectrum Protect Version 8.1.6 kann nur die HP-UX Itanium 2-API installiert werden.

Systemvoraussetzungen für die HP-UX Itanium 2-API

Für die HP-UX Itanium 2-API von IBM Spectrum Protect gelten Mindestanforderungen in Bezug auf die Hardware, den Plattenspeicherplatz, den Hauptspeicher und die Software.

Informationen zu den Hardware- und Softwarevoraussetzungen für alle unterstützten Versionen der HP-UX Itanium 2-API, einschließlich der neuesten Fixpacks, finden Sie in Technote 1197146.

Übertragungsmethoden für die HP-UX Itanium 2-API

Für die HP-UX Itanium 2-API sind die Übertragungsmethoden TCP/IP und Shared Memory verfügbar.

Tabelle 4. Übertragungsmethoden für die HP-UX Itanium 2-API

Zur Verwendung dieser Übertragungsmethode:	Diese Software installieren:	Um Verbindung zu diesen IBM Spectrum Protect-Servern herzustellen:
TCP/IP	TCP/IP (Standard bei HP-UX)	AIX, Linux, Windows

Linux on Power Systems-Clientumgebung

Dieser Abschnitt enthält Informationen zur Clientumgebung, zu Komponenten des Clients für Sichern/Archivieren und zu den Hardware- und Softwarevoraussetzungen für die Linux on Power Systems-Clientplattform.

Installierbare Komponenten des Linux on Power Systems-Clients

Die installierbaren Komponenten des Linux on Power Systems-Clients für Sichern/Archivieren umfassen die Befehlszeile des Clients für Sichern/Archivieren, die Java-GUI, den Web-Client für Sichern/Archivieren und die API.

Sie können die folgenden Komponenten mit IBM Spectrum Protect Version 8.1.6 installieren:

- Client für Sichern/Archivieren
- Verwaltungsclient

- Grafische Java-Benutzerschnittstelle (Java-GUI) für Sichern/Archivieren
- Web-Client für Sichern/Archivieren
- IBM Spectrum Protect-API (64-Bit)

Systemvoraussetzungen für Linux on Power Systems-Clients

Für die Linux on Power Systems-Clients von IBM Spectrum Protect gelten Mindestanforderungen an die Hardware, den Plattenspeicherplatz, den Hauptspeicher und die Software.

Informationen zu den Hardware- und Softwarevoraussetzungen für alle unterstützten Versionen der Linux on Power Systems-Clients, einschließlich der neuesten Fixpacks, finden Sie in Technote 1169963.

Übertragungsmethoden des Linux on Power Systems-Clients

Clients für Sichern/Archivieren unter Linux on Power Systems können TCP/IP oder Shared Memory als Übertragungsmethode für die Client/Server-Kommunikation verwenden.

In Tabelle 5 sind die verfügbaren Übertragungsmethoden für Linux on Power Systems-Clients sowie die Betriebssysteme des IBM Spectrum Protect-Servers, für die Sie sie verwenden können, aufgelistet.

Tabelle 5. Übertragungsmethoden des Linux on Power Systems-Clients

Zur Verwendung dieser Übertragungsmethode:	Diese Software installieren:	Um Verbindung zu diesen IBM Spectrum Protect-Servern herzustellen:
TCP/IP	TCP/IP (Standard bei Linux)	AIX, Linux, Windows
Shared Memory	TCP/IP (Standard bei Linux)	Linux on Power Systems

Linux x86_64-Clientumgebung

Dieser Abschnitt enthält Informationen zur Clientumgebung, zu Komponenten des Clients für Sichern/Archivieren und zu den Hardware- und Softwarevoraussetzungen für die Linux on Intel-Plattform (Linux x86_64-Plattform).

Installierbare Komponenten des Linux x86_64-Clients

Die installierbaren Komponenten des Linux on Intel-Clients für Sichern/Archivieren (Linux x86_64-Clients für Sichern/Archivieren) umfassen die Befehlszeile des Clients für Sichern/Archivieren, die Java-GUI, den Web-Client für Sichern/Archivieren, den Verwaltungsclient und die API.

Sie können die folgenden Komponenten mit IBM Spectrum Protect Version 8.1.6 installieren:

- Client für Sichern/Archivieren
- Verwaltungsclient
- Grafische Java-Benutzerschnittstelle (Java-GUI) für Sichern/Archivieren
- Web-Client für Sichern/Archivieren
- IBM Spectrum Protect-API

Systemvoraussetzungen für Linux x86_64-Clients

Für die Linux x86_64-Clients von IBM Spectrum Protect gelten Mindestanforderungen an die Hardware, den Plattenspeicherplatz, den Hauptspeicher und die Software.

Informationen zu den Hardware- und Softwarevoraussetzungen für alle unterstützten Versionen der Linux x86_64-Clients, einschließlich der neuesten Fixpacks, finden Sie in Technote 1052223.

Übertragungsmethoden des Linux x86_64-Clients

Für den Linux on Intel-Client für Sichern/Archivieren (Linux x86_64-Client für Sichern/Archivieren) sind die Übertragungsmethoden TCP/IP und Shared Memory verfügbar.

Sie können die folgenden Übertragungsmethoden für den Linux on Intel-Client (Linux x86_64-Client) von IBM Spectrum Protect Version 8.1.6 verwenden:

Tabelle 6. Übertragungsmethoden des Linux on Intel x86_64-Clients

Zur Verwendung dieser Übertragungsmethode:	Diese Software installieren:	Um Verbindung zu diesen IBM Spectrum Protect-Servern herzustellen:
TCP/IP	TCP/IP (Standard bei Linux)	AIX, Linux, Windows
Shared Memory	TCP/IP (Standard bei Linux)	Linux x86_64

Linux on System z-Clientumgebung

Dieser Abschnitt enthält Informationen zur Clientumgebung, zu Komponenten des Clients für Sichern/Archivieren und zu den Hardware- und Softwarevoraussetzungen für die Linux on System z-Plattform.

Installierbare Komponenten des Linux on System z-Clients

Die installierbaren Komponenten des Linux on System z-Clients für Sichern/Archivieren umfassen die Befehlszeile des Clients für Sichern/Archivieren, den Verwaltungsclient, den Web-Client für Sichern/Archivieren und die API.

Sie können die folgenden Komponenten mit IBM Spectrum Protect Version 8.1.6 installieren:

- Client für Sichern/Archivieren
- Verwaltungsclient
- Web-Client für Sichern/Archivieren
- IBM Spectrum Protect-API

Systemvoraussetzungen für Linux on System z-Clients

Für die Linux System z-Clients von IBM Spectrum Protect gelten Mindestanforderungen an die Hardware, den Plattenspeicherplatz, den Hauptspeicher und die Software.

Informationen zu den Hardware- und Softwarevoraussetzungen für alle unterstützten Versionen der Linux System z-Clients, einschließlich der neuesten Fixpacks, finden Sie in Technote 1066436.

Übertragungsmethoden des Linux on System z-Clients

Für den Linux on System z-Client für Sichern/Archivieren sind die Übertragungsmethoden TCP/IP und Shared Memory verfügbar.

Sie können die folgenden Übertragungsmethoden für den Linux on System z-Client von IBM Spectrum Protect Version 8.1.6 verwenden:

Tabelle 7. Übertragungsmethoden des Linux on System z-Clients

Zur Verwendung dieser Übertragungsmethode:	Diese Software installieren:	Um Verbindung zu diesen IBM Spectrum Protect-Servern herzustellen:
TCP/IP	TCP/IP (Standard bei Linux)	AIX, Linux, Windows
Shared Memory	TCP/IP (Standard bei Linux)	Linux on System z

Mac OS X-Clientumgebung

Dieser Abschnitt enthält Informationen zur Clientumgebung, zu Komponenten des Clients für Sichern/Archivieren und zu den Hardware- und Softwarevoraussetzungen für den Mac OS X-Client.

Installierbare Komponenten des Mac OS X-Clients

Die installierbaren Komponenten des Mac OS X-Clients für Sichern/Archivieren umfassen die Befehlszeile des Clients für Sichern/Archivieren, die Java-GUI, den Web-Client für Sichern/Archivieren und die API.

Die folgenden Komponenten werden mit IBM Spectrum Protect Version 8.1.6 installiert:

- Client für Sichern/Archivieren
- Verwaltungsclient
- Web-Client für Sichern/Archivieren
- IBM Spectrum Protect-API
- Grafische Java-Benutzerschnittstelle (Java-GUI) für Sichern/Archivieren

Tipp: Die Shell-Script-Datei dsmj für die Java-GUI wird an der folgenden Position installiert:

/Library/Application Support/tivoli/tsm/client/ba/bin

Systemvoraussetzungen für Mac OS X-Clients

Für die Mac OS X-Clients von IBM Spectrum Protect gelten Mindestanforderungen an die Hardware, den Plattenspeicherplatz, den Hauptspeicher und die Software.

Informationen zu den Hardware- und Softwarevoraussetzungen für alle unterstützten Versionen der Mac OS X-Clients, einschließlich der neuesten Fixpacks, finden Sie in

Technote 1053584.

Übertragungsmethoden des Mac OS X-Clients

Für den Mac OS X-Client für Sichern/Archivieren sind die TCP/IP-Übertragungsmethoden verfügbar.

Sie können die folgenden Übertragungsmethoden mit dem Mac OS X-Client von IBM Spectrum Protect Version 8.1.6 verwenden:

Tabelle 8. Übertragungsmethoden des Mac OS X-Clients

Zur Verwendung dieser Übertragungsmethode:	Diese Software installieren:	Um Verbindung zu diesen IBM Spectrum Protect-Servern herzustellen:
TCP/IP	TCP/IP (Standard bei Mac OS X)	AIX, Linux, Windows

Oracle Solaris-Clientumgebung

Dieser Abschnitt enthält Informationen zur Clientumgebung, zu Clientkomponenten und zu den Hardware- und Softwarevoraussetzungen für die Oracle Solaris-Plattform.

Ab IBM Spectrum Protect Version 8.1.0 ist der Oracle Solaris-Client für Sichern/Archivieren nur auf der Oracle Solaris x86_64-Plattform verfügbar. Die Oracle Solaris-API ist auf den Oracle Solaris x86_64- und Oracle Solaris SPARC-Plattformen verfügbar.

Installierbare Komponenten des Oracle Solaris-Clients

Die installierbaren Komponenten des Oracle Solaris-Clients für Sichern/Archivieren umfassen die IBM Spectrum Protect-Befehlszeile, die Java-GUI, den Web-Client für Sichern/Archivieren und die API.

Unter Oracle Solaris x86_64 können Sie die folgenden Clientkomponenten installieren:

- Client für Sichern/Archivieren
- Verwaltungsclient
- Grafische Java-Benutzerschnittstelle (Java-GUI) für Sichern/Archivieren
- Web-Client für Sichern/Archivieren
- IBM Spectrum Protect-API

Sie können die IBM Spectrum Protect-API unter Oracle Solaris SPARC installieren.

Systemvoraussetzungen für Oracle Solaris-Clients

Für die Oracle Solaris-Clients von IBM Spectrum Protect gelten Mindestanforderungen an die Hardware, den Plattenspeicherplatz, den Hauptspeicher und die Software.

Informationen zu den Hardware- und Softwarevoraussetzungen für alle unterstützten Versionen der Oracle Solaris-Clients von IBM Spectrum Protect, einschließlich der neuesten Fixpacks, finden Sie auf den folgenden IBM Support-Seiten:

- Für Oracle Solaris x86_64-Clientvoraussetzungen siehe Technote 1232956.
- Für Oracle Solaris SPARC-API-Voraussetzungen siehe Technote 1052211.

Übertragungsmethoden des Oracle Solaris-Clients

Für den Oracle Solaris-Client für Sichern/Archivieren sind die Übertragungsmethoden TCP/IP und Shared Memory verfügbar.

Sie können die folgenden Übertragungsmethoden mit dem Oracle Solaris-Client verwenden:

Tabelle 9. Übertragungsmethoden des Oracle Solaris-Clients

Zur Verwendung dieser Übertragungsmethode:	Diese Software installieren:	Um Verbindung zu diesen IBM Spectrum Protect-Servern herzustellen:
TCP/IP	TCP/IP (Standard bei Solaris)	AIX, Linux, Windows

Voraussetzungen für NDMP-Unterstützung (nur Extended Edition)

Sie können NDMP (Network Data Management Protocol) verwenden, um NAS-Dateisysteme (Network Attached Storage) auf Bandlaufwerke oder Speicherarchive, die lokal an die NAS-Dateiserver von Network Appliance und EMC Celerra angeschlossen sind, zu sichern und von dort zurückzuschreiben.

NDMP-Unterstützung ist nur für IBM Spectrum Protect Extended Edition verfügbar.

NDMP-Unterstützung erfordert die folgende Hardware und Software:

- IBM Spectrum Protect Extended Edition
- Bandlaufwerk und Bandarchiv. Unterstützte Kombinationen finden Sie unter: Produktinformation.

Installationsvoraussetzungen für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Clientdaten

Bevor Sie Ihre FastBack-Clientdaten sichern oder archivieren können, müssen Sie die erforderliche Software installieren.

Sie müssen die folgende Software installieren:

- Tivoli Storage Manager FastBack Version 6.1
- Tivoli Storage Manager-Client Version 6.1.3.x (x ist 1 oder höher) oder Version 6.2 oder höher
- Tivoli Storage Manager-Server Version 6.1.3 oder höher
- Tivoli Storage Manager Administration Center Version 6.1.3
 - Nur erforderlich, wenn die integrierte Tivoli Storage Manager FastBack-Verwaltung verwendet werden soll.

Ab Version 7.1 ist die Komponente 'Administration Center' nicht mehr in Tivoli Storage Manager- oder IBM Spectrum Protect-Verteilungen enthalten. FastBack-Benutzer, die über ein Administration Center aus einem früheren Server-Release verfügen, können damit weiterhin FastBack-Zeitpläne erstellen und ändern.

Wenn noch kein Administration Center installiert ist, können Sie die Vorgängerversion von <ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/admincenter/v6r3/> herunterladen. Wenn noch kein Administration Center installiert ist, müssen Sie FastBack-Zeitpläne auf dem IBM Spectrum Protect-Server erstellen und ändern. Informationen zur Erstellung von Zeitplänen auf dem Server finden Sie in der Dokumentation für den IBM Spectrum Protect-Server.

Die Tivoli Storage Manager FastBack-Umgebung muss aktiv sein. Informationen zur Installation und Konfiguration von Tivoli Storage Manager FastBack finden Sie in der Produktinformation für Tivoli Storage Manager FastBack.

Informationen zur Integration von IBM Spectrum Protect und Tivoli Storage Manager FastBack finden Sie in Tivoli Storage Manager FastBack und IBM Spectrum Protect integrieren.

Sie können den IBM Spectrum Protect-Client mit einem der folgenden Verfahren installieren:

- Installieren Sie den Client für Sichern/Archivieren auf einer Workstation, auf der der FastBack Disaster Recovery Hub installiert ist. In diesem Fall sind die Voraussetzungen: FastBack Disaster Recovery Hub-Konfiguration und FastBack Shell.
- Installieren Sie den Client für Sichern/Archivieren auf einer Workstation, auf der weder der FastBack-Server noch der FastBack Disaster Recovery Hub installiert ist. In diesem Fall ist FastBack Shell weiterhin erforderlich.

Zugehörige Konzepte:

„Client für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Daten konfigurieren“ auf Seite 106

UNIX- und Linux-Clients für Sichern/Archivieren installieren

Dieser Abschnitt enthält Anweisungen zum Installieren und Konfigurieren der UNIX- und Linux-Clients von IBM Spectrum Protect.

Anmerkung: Sie müssen sich als Rootbenutzer anmelden, um den Client für Sichern/Archivieren auf einer UNIX- oder Linux-Workstation zu installieren.

Die unterstützten UNIX- und Linux-Clients sowie die Position der Installationsanweisungen für jeden Client sind hier aufgelistet.

- „AIX-Client installieren“
- „HP-UX Itanium 2-API installieren“ auf Seite 15
- „Client für Sichern/Archivieren unter Linux on Power Systems (Little Endian) installieren“ auf Seite 18
- „Client für Sichern/Archivieren unter Ubuntu Linux on Power Systems (Little Endian) installieren“ auf Seite 22
- „API unter Linux on Power Systems (Big Endian) installieren“ auf Seite 25
- „Linux x86_64-Client installieren“ auf Seite 29
- „Ubuntu Linux x86_64-Client installieren“ auf Seite 34
- „Linux on System z-Client installieren“ auf Seite 38
- „Mac OS X-Client installieren“ auf Seite 43
- „Oracle Solaris x86_64-Client installieren“ auf Seite 45
- „Oracle Solaris SPARC-API installieren“ auf Seite 48

Zugehörige Konzepte:

Kapitel 2, „IBM Spectrum Protect-Client konfigurieren“, auf Seite 53

AIX-Client installieren

Sie können den AIX-Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.

Informationen zu diesem Vorgang

In IBM Spectrum Protect Version 8.1.6 wird in den Verteilungsbibliotheken eine 64-Bit-Version des AIX-Clients bereitgestellt.

Es ist nicht möglich, ein Upgrade für einen zuvor installierten 32-Bit-AIX-Client auf den neuen 64-Bit-AIX-Client durchzuführen. Falls bereits ein 32-Bit-Client einer früheren Version von IBM Spectrum Protect installiert ist, führen Sie die folgenden Schritte mit SMIT aus:

1. Deinstallieren Sie den 32-Bit-Client (tivoli.tsm.client.ba).

2. Deinstallieren Sie alle landessprachlichen Dateien, die zuvor installiert waren.
3. Deinstallieren Sie die API (tivoli.tsm.client.api.32bit).

Verwenden Sie anschließend SMIT, um die folgenden Pakete in den Verteilungsbibliotheken von IBM Spectrum Protect Version 8.1.6 in der folgenden Reihenfolge zu installieren:

1. Installieren Sie die 64-Bit-API (tivoli.tsm.client.api.64bit).
2. Installieren Sie den 64-Bit-Client (tivoli.tsm.client.ba.64bit).

Falls bereits ein 64-Bit-Client von IBM Spectrum Protect Version 6.3 (oder höher) installiert ist, können Sie ein Upgrade des Clients durchführen, statt den Client zu deinstallieren und anschließend erneut zu installieren.

Falls ein 64-Bit-Client einer früheren Version von IBM Spectrum Protect installiert ist (z. B. Version 6.1 oder 6.2), müssen Sie den Client, die Sprachenpakete und die API deinstallieren. Anschließend installieren Sie die neue API und den neuen Client von IBM Spectrum Protect.

Alle zur Installation des Clients benötigten Pakete befinden sich im AIX-Clientpaket; sie überschreiben während der Installation alle älteren ausführbaren Anwendungen auf Ihrem System. Die Laufzeitbibliothek LibC (C Set ++) ist erforderlich.

Wenn Sie für die Installation dieses Clients den Befehl **installp** verwenden, ändern Sie nicht die Standardfeldwerte für die folgenden beiden Auswahlmöglichkeiten:

- **Erforderliche Software AUTOMATISCH installieren?**
- **Dieselbe Version oder neuere Versionen ÜBERSCHREIBEN?**

Werden die Werte inaktiviert oder geändert, kann eine Clientkomponente mit einer niedrigeren Version über eine derzeit installierte Komponente mit einer höheren Version installiert werden. Unter derartigen Umständen könnten Funktionsaufrufe zwischen Komponenten mit unterschiedlichen Versionen nicht mehr gültig sein.

Installieren Sie die folgenden Pakete. Alle diese Pakete sind auf den Installationsmedien verfügbar. Sie benötigen eine Extended Edition-Lizenz für die Verwendung des NAS-Clients.

Die folgenden Dateien sind in der Reihenfolge der Abhängigkeit aufgelistet. Beispielsweise ist die API von Global Security Kit (GSKit) abhängig. Wenn Sie zur Installation aller Dateien SMIT verwenden, können Sie sie in beliebiger Reihenfolge auswählen (F7).

GSKit8.gskcrypt64.ppc.rte und GSKit8.gskssl64.ppc.rte

IBM GSKit 64-Bit (wird von der 64-Bit-Client-API benötigt).

tivoli.tsm.client.api.64bit

Installiert die 64-Bit-API.

tivoli.tsm.client.ba.64bit

Installiert die folgenden 64-Bit-Clientdateien:

- Java-Client für Sichern/Archivieren (GUI)
- Web-Client für Sichern/Archivieren
- NAS-Sicherungsclient

tivoli.tsm.filepath_aix

Installiert die für die journalbasierte Sicherung erforderliche Kernelerweiterung des Dateipfads.

tivoli.tsm.client.jbb.64bit

Installiert die Komponente für die journalbasierte Sicherung.

Jedes Paket wird in dem folgenden Standardinstallationsverzeichnis installiert:

- Die 64-Bit-Dateien des Clients für Sichern/Archivieren, des Web-Clients und des Verwaltungscients (**dsmadm**) werden im Verzeichnis `/usr/tivoli/tsm/client/ba/bin64` installiert.
- Die 64-Bit-Dateien der IBM Spectrum Protect-API werden im Verzeichnis `/usr/tivoli/tsm/client/api/bin64` installiert.
- Das Beispiel für die Systemoptionsdatei, `dsm.sys.smp`, wird in das Installationsverzeichnis gestellt.

Mit diesem Installationsverfahren können neue Verteilungen oder Aktualisierungen von heruntergeladenen Installationsmedien installiert werden. Die heruntergeladenen Dateien, die Sie zum Installieren des Clients verwenden, können gegebenenfalls komprimiert sein. Kopieren oder extrahieren Sie die Dateien abhängig vom Format der Paketdatei auf Platte und installieren Sie die Komponenten gemäß diesen Anweisungen.

Sie können die entsprechende Paketdatei von einer der folgenden Websites herunterladen:

- Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.
- Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.

Wenn Sie die Clientdateien zunächst in ein lokales Verzeichnis kopieren, erstellt der Befehl **installp** automatisch eine `.toc`-Datei. Sie können eine `.toc`-Datei manuell erstellen, indem Sie in dem lokalen Verzeichnis, in das Sie das IBM Spectrum Protect-Image kopiert haben, `/usr/sbin/inutoc` ausführen. Geben Sie in der AIX-Befehlszeile Folgendes ein:

```
/usr/sbin/inutoc /usr/sys/inst.images
```

Daraufhin wird eine `.toc`-Datei in dem betreffenden Verzeichnis erstellt.

Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Stellen Sie den Datenträger bereit, von dem die Installation erfolgt.
3. Geben Sie in der AIX-Befehlszeile `smitty install` ein und drücken Sie die Eingabetaste.
4. Wählen Sie **Software installieren und aktualisieren** aus und drücken Sie die Eingabetaste.
5. Wählen Sie **Neueste verfügbare Software installieren und aktualisieren** und drücken Sie die Eingabetaste.
6. Drücken Sie bei der Eingabeaufforderung `Eingabeeinheit/-verzeichnis` für Software die Taste F4, geben Sie das Verzeichnis an, das die Installationsimages enthält, und drücken Sie die Eingabetaste.
7. Bei der Eingabeaufforderung `Zu installierende Software` drücken Sie die Taste F4. Wählen Sie die gewünschten IBM Spectrum Protect-Dateigruppen für die Installation aus, indem Sie die Taste F7 drücken. Drücken Sie anschließend die Eingabetaste.

8. Drücken Sie in der Anzeige **Von verfügbarer Software installieren und aktualisieren** die Taste F4, um Eingabefelder zu ändern, oder verwenden Sie die Standardfelder. Drücken Sie zweimal die Eingabetaste, um mit der Installation zu beginnen.
9. Drücken Sie nach Abschluss der Installation zum Beenden die Taste F10.

Ergebnisse

Wenn Dateigruppen installiert werden, werden sie automatisch im System festgeschrieben. Die vorherige Version der Software des Clients für Sichern/Archivieren wird durch die neu installierte Version ersetzt.

Die Dateien des Clients für Sichern/Archivieren werden im Verzeichnis `/usr/tivoli/tsm/client/ba/bin64` installiert. Wenn Sie die Clientdateien in ein anderes Verzeichnis versetzen, müssen Sie die folgenden Schritte ausführen:

1. Stellen Sie sicher, dass sich die Berechtigungen der installierten Dateien nicht geändert haben.
2. Aktualisieren Sie die symbolischen Verbindungen für die installierten Dateien in den folgenden Verzeichnissen:
 - Im Verzeichnis `/usr/bin`
 - Im Verzeichnis `/usr/lib` für die IBM Spectrum Protect-Bibliotheken
3. Stellen Sie sicher, dass jeder Benutzer des Clients für Sichern/Archivieren die Umgebungsvariable `DSM_DIR` auf das neu installierte Verzeichnis setzt.

Nächste Schritte

Nach dem Abschluss der Installation sind die in Kapitel 2, „IBM Spectrum Protect-Client konfigurieren“, auf Seite 53 beschriebenen erforderlichen und optionalen Tasks auszuführen, bevor der Client für Sichern/Archivieren verwendet werden kann.

Anmerkung:

- AIX-Workloadpartitionen (WPAR) werden folgendermaßen unterstützt:
 - Unterstützung in globalen Umgebungen
 - Unterstützung mit nicht gemeinsam genutzten System-WPARs
 - Unterstützung mit gemeinsam genutzten System-WPARs (für Protokolle und Konfigurationsdateien des Clients für Sichern/Archivieren müssen andere Positionen als die Standardpositionen definiert sein)
 - Keine Unterstützung für Anwendungs-WPARs
 - Keine Unterstützung für Imagesicherung
 - Keine Unterstützung für Zurückschreibung einer Sicherungsgruppe von Band
- Wenn Sie unter AIX Version 6.1 EFS (Encrypted File System) mit dem Client für Sichern/Archivieren verwenden und das Schlüsselspeicherkennwort des EFS-Benutzers nicht mit dem Anmeldekennwort des Benutzers übereinstimmt, wird der EFS-Schlüsselspeicher bei Ihrer Anmeldung nicht automatisch geöffnet. Wenn der EFS-Schlüsselspeicher bei Ihrer Anmeldung nicht geöffnet ist, schreibt der Client eine Nicht-EFS-Datei möglicherweise nicht in ein EFS-Dateisystem zurück. Sie können das Problem beim Zurückschreiben eines EFS-Dateisystems durch eine der folgenden Maßnahmen verhindern:
 - Starten Sie den Client für Sichern/Archivieren mit dem Befehl **efskeymgr -o**. Zum Beispiel: **efskeymgr -o ./dsmj**
 - Synchronisieren Sie mit dem Befehl **efskeymgr -n** das Schlüsselspeicherkennwort mit dem Anmeldekennwort des Benutzers. Zum Beispiel: **efskeymgr -n**

AIX-Client deinstallieren

Sie können die folgenden Prozeduren verwenden, um den IBM Spectrum Protect AIX-Client für Sichern/Archivieren zu deinstallieren.

Vorbereitende Schritte

Die IBM Spectrum Protect-Clientmodule und -komponenten sind nahtlos integriert und die installierten Dateigruppen werden automatisch festgeschrieben. Es gibt keine Option für ROLLBACK-Operationen deinstallierter Komponenten.

Vorgehensweise

1. Geben Sie den folgenden AIX-Befehl ein: **smitty remove**.
2. Drücken Sie die Eingabetaste.
3. Drücken Sie im Namensfeld **SOFTWARE** die Taste F4, um die IBM Spectrum Protect-Dateigruppen aufzulisten, die Sie deinstallieren wollen; drücken Sie die Eingabetaste.
4. Wählen Sie die IBM Spectrum Protect-Dateigruppen aus, die Sie deinstallieren wollen; drücken Sie die Eingabetaste.

Anmerkung: Das Feature für die journalbasierte Sicherung befindet sich in zwei Dateigruppen. Wählen Sie sowohl `tivoli.tsm.client.jbb.64bit` als auch `tivoli.tsm.filepath_aix` aus. Falls Sie die Dateigruppen nacheinander deinstallieren, deinstallieren Sie zuerst die Dateigruppe `tivoli.tsm.client.jbb.64bit`.

5. Im Feld **Nur Voranzeige?** (es findet keine Löschoperation statt) wählen Sie **Nein** aus; drücken Sie die Eingabetaste.

HP-UX Itanium 2-API installieren

Sie können die HP-UX Itanium 2-API von den Produktinstallationsmedien installieren.

Informationen zu diesem Vorgang

Die folgenden Quellenpakete sind auf den Installationsdatenträgern verfügbar:

tsmcli/hp11ia64/gskcrypt64-8.x.x.x.hpux.ia64.tar.Z und **tsmcli/hp11ia64/gskssl64-8.x.x.x.hpux.ia64.tar.Z**

Enthält das GSKit. Wenn Sie eine vorherige Version des GSKit installiert haben, deinstallieren Sie diese, bevor Sie die neue Version installieren.

tsmcli/hp11ia64/TIVsmCapi64

In diesem Paket ist TIVsm64 der Softwareauswahlname, der von **swlist** für den Produktnamen der höchsten Ebene verwendet wird. Die Komponente unter TIVsm64 ist TIVsm.CLIENT_API64.

Standardinstallationsverzeichnisse

Während der Clientinstallation werden einige Dateien in den folgenden Standardverzeichnissen gespeichert:

- Die Dateien der IBM Spectrum Protect-API werden im Verzeichnis `/opt/tivoli/tsm/client/api/bin64` installiert.
- Die Beispielsystemoptionsdatei `dsm.sys.smp` wird in das Installationsverzeichnis gestellt.

Um frühere Versionen des Clients für Sichern/Archivieren zu entfernen, melden Sie sich als der Rootbenutzer an und geben Sie den folgenden Befehl ein:

```
/usr/sbin/swremove -x mount_all_filesystems=false -v TIVsm64
```

Wenn Sie in einem Client der Version 7.1.2 oder früher zusätzliche Sprachen installiert haben, müssen Sie folgenden Befehl ausführen, um diese zu entfernen:

```
/usr/sbin/swremove -x mount_all_filesystems=false -v TIVsm64.CLIENT_msg_Sprache
```

Ersetzen Sie dabei *Sprache* durch den entsprechenden Sprachencode aus Tabelle 10.

Tabelle 10. HP-UX Itanium 2-Client: Sprachencodes für Installationspakete

Sprache	Sprachencode
Vereinfachtes Chinesisch	ZH_CN
Traditionelles Chinesisch	ZH_TW
Tschechisch	CS_CZ
Französisch	FR_FR
Deutsch	DE_DE
Ungarisch	HU_HU
Italienisch	IT_IT
Japanisch	JA_JP
Koreanisch	KO_KR
Polnisch	PL_PL
Brasilianisches Portugiesisch	PT_BR
Russisch	RU_RU
Spanisch	ES_ES

Mit diesem Installationsverfahren können neue Verteilungen oder Aktualisierungen von heruntergeladenen Installationsmedien installiert werden. Die heruntergeladenen Dateien, die Sie zum Installieren des Clients verwenden, können gegebenenfalls komprimiert sein. Kopieren oder extrahieren Sie die Dateien abhängig vom Format der Paketdatei auf Platte und installieren Sie die Komponenten gemäß diesen Anweisungen.

Sie können die entsprechende Paketdatei von einer der folgenden Websites herunterladen:

- Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.
- Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.

Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Stellen Sie den Datenträger bereit, von dem die Installation erfolgt.
3. Für die Installation des GSKit: Wenn Sie eine vorherige Version von GSKit installiert haben, entfernen Sie diese, bevor Sie die neue Version installieren. Extrahieren Sie den Inhalt der Dateien gskcrypt64-8.x.x.x.hpux.ia64.tar.Z und gskssl64-8.x.x.x.hpux.ia64.tar.Z in ein Verzeichnis auf Ihrer Festplatte. Geben Sie die folgenden Befehle ein, um die Pakete zu installieren:

```

/usr/sbin/swinstall -x mount_all_filesystems=false -v -s `pwd`
/gskcrypt64 gskcrypt64
/usr/sbin/swinstall -x mount_all_filesystems=false -v -s `pwd`
/gskssl64 gskssl64

```

4. Wenn Sie von FTP heruntergeladen haben, wechseln Sie in das Verzeichnis, in dem sich das installierbare Image befindet. Geben Sie den folgenden Befehl ein:

```

/usr/sbin/swinstall -x mount_all_filesystems=false -v -s
`pwd`/TIVsmCapi64 TIVsm64

```

`pwd` kann anstelle des absoluten Namens des aktuellen Verzeichnisses verwendet werden.

Zugehörige Konzepte:

Kapitel 2, „IBM Spectrum Protect-Client konfigurieren“, auf Seite 53

Standardbegrenzung für Datensegmentgröße erhöhen

Die Standardbegrenzung für die Datensegmentgröße eines Prozesses in HP-UX 11i v2 beträgt 64 MB. Wenn große Dateisysteme gesichert werden, wird dieser Grenzwert möglicherweise von der API überschritten und es kann eine abnormale Speicherbedingung auftreten.

Um diesen Grenzwert zu erhöhen, können Sie den Kernel wie folgt ändern:

1. Starten Sie als Root **sam**.
2. Wählen Sie **Kernel Configuration (Kernelkonfiguration)** aus.
3. Wählen Sie **Configurable Parameters (Konfigurierbare Parameter)** aus.
4. Suchen Sie **maxdsize**, und erhöhen Sie den Wert dieses Parameters über den Menüeintrag **Actions/Modify Configurable Parameter... (Aktionen/Konfigurierbare Parameter ändern...)**. (Setzen Sie maxdsize beispielsweise auf 268435456, um eine Maximalgröße von 256 MB für Datensegmente zu definieren.
5. Nach dieser Änderung wird der Kernel von **sam** erneut erstellt. Damit die neue Einstellung wirksam wird, muss ein Warmstart durchgeführt werden.

HP-UX Itanium 2-API deinstallieren

Sie können die folgenden Prozeduren verwenden, um die IBM Spectrum Protect HP-UX Itanium 2-API zu deinstallieren.

Vorbereitende Schritte

Wichtig: Sie müssen die Pakete in der angegebenen Reihenfolge deinstallieren.

Vorgehensweise

1. Geben Sie den folgenden Befehl ein, um die Dateigruppe CLIENT_API zu entfernen:

```

/usr/sbin/swremove -x mount_all_filesystems=false -v TIVsm64

```

2. Geben Sie die folgenden Befehle ein, um Global Security Kit (GSKit) zu entfernen:

```

/usr/sbin/swremove -x mount_all_filesystems=false gskssl64
/usr/sbin/swremoveswremove -x mount_all_filesystems=false gskcrypt64

```

Nächste Schritte

Nach der Deinstallation der HP-UX-API verbleiben mehrere leere Verzeichnisse in dem Dateisystem, wie beispielsweise die folgenden Verzeichnisse:

- Das Lizenzverzeichnis (/opt/tivoli/tsm/license)
- Ein oder mehrere Sprachenverzeichnisse (/opt/tivoli/tsm/client/ba/bin/xx_XX); hierbei ist xx_XX einer der folgenden Sprachencodes: cs_CZ, de_DE, es_ES, it_IT, fr_FR, hu_HU, ja_JP, ko_KR, pl_PL, pt_BR, ru_RU, zh_CN und zh_TW
- /opt/tivoli/tsm/client/ba/bin/cit
- /opt/tivoli/tsm/client/ba/bin/images
- /opt/tivoli/tsm/client/ba/bin/plugin

Sollen diese leeren Verzeichnisse entfernt werden, können Sie sie manuell entfernen.

Client für Sichern/Archivieren unter Linux on Power Systems (Little Endian) installieren

Sie können den Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.

Vorbereitende Schritte

Sie müssen als Rootbenutzer angemeldet sein, um das Produkt installieren zu können.

Mit diesem Installationsverfahren können neue Verteilungen oder Aktualisierungen von heruntergeladenen Installationsmedien installiert werden. Die heruntergeladenen Dateien, die Sie zum Installieren des Clients verwenden, können gegebenenfalls komprimiert sein. Kopieren oder extrahieren Sie die Dateien abhängig vom Format der Paketdatei auf Platte und installieren Sie die Komponenten gemäß diesen Anweisungen.

Sie können die entsprechende Paketdatei von einer der folgenden Websites herunterladen:

- Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.
- Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.

Informationen zu diesem Vorgang

Die folgenden Installationsoptionen sind in nicht komprimierten Paketen auf den Installationsmedien verfügbar.

Tabelle 11. Paketnamen, Inhalt und Standardverzeichnis

Paketname	Inhalt	Standardverzeichnis
gskcrypt64-8.x.x.x.linux.ppcle.rpm gskssl64-8.x.x.x.linux.ppcle.rpm	64-Bit-Version der Global Security Kit- Pakete (GSKit)	/usr/local/ibm/gsk8

Tabelle 11. Paketnamen, Inhalt und Standardverzeichnis (Forts.)

Paketname	Inhalt	Standardverzeichnis
TIVsm-API64.ppc64le.rpm	Anwendungsprogrammierschnittstelle (API), die die gemeinsam genutzten Bibliotheken und Beispiele für die IBM Spectrum Protect-API enthält.	/opt/tivoli/tsm/client/api/bin64
TIVsm-BA.ppc64le.rpm	Client für Sichern/Archivieren (Befehlszeile und GUI), Verwaltungsclient (dsmadm) und Web-Client	<p>/opt/tivoli/tsm/client/ba/bin</p> <p>Dieses Verzeichnis ist normalerweise das Standardinstallationsverzeichnis für viele Dateien des Clients für Sichern/Archivieren. Die Beispielsystemoptionsdatei (dsm.sys.smp) wird in dieses Verzeichnis geschrieben. Wenn Sie die Umgebungsvariable DSM_DIR nicht definieren, werden die ausführbare Datei dsmc, die Ressourcendateien und die Datei dsm.sys in diesem Verzeichnis gespeichert.</p> <p>Wenn Sie die Umgebungsvariable DSM_CONFIG nicht definieren, muss sich die Clientbenutzeroptionsdatei in diesem Verzeichnis befinden.</p> <p>Wenn Sie die Umgebungsvariable DSM_LOG nicht definieren, schreibt der Client für Sichern/Archivieren Nachrichten in die Dateien dsmerror.log und dsmsched.log des aktuellen Arbeitsverzeichnisses.</p>
TIVsm-APIcit.ppc64le.rpm TIVsm-BAcit.ppc64le.rpm	Diese Dateien stellen die Common Inventory Technology-Komponenten bereit, mit denen Sie Informationen zur Anzahl der Client- und Servereinheiten, die mit dem System verbunden sind, sowie zur Nutzung der Prozessor-Value-Units (PVUs) durch Servereinheiten abrufen können. Diese Dateien sind optional. Weitere Informationen zu PVUs finden Sie in Prozessor-Value-Units schätzen in der Dokumentation zum IBM Spectrum Protect-Server.	<p>APIcit wird im Verzeichnis /opt/tivoli/tsm/client/api/bin64/cit installiert.</p> <p>BAcit wird im Verzeichnis /opt/tivoli/tsm/client/ba/bin/cit installiert.</p>
TIVsm-filepath-source.tar.gz TIVsm-JBB.ppc64le.rpm	Für journalbasierte Sicherungen benötigte Dateien.	<p>Filepath wird in /opt/filepath installiert.</p> <p>Das Paket TIVsm-JBB.ppc64le.rpm wird in /opt/tivoli/tsm/client/ba/bin installiert.</p>

Vorgehensweise

1. Stellen Sie den Datenträger bereit, von dem die Pakete installiert werden.
2. Wechseln Sie in das Verzeichnis, in dem die Installationspakete gespeichert sind.
3. Installieren Sie die 64-Bit-Version der GSKit-Pakete. In dem folgenden Befehlsbeispiel stehen die Zeichen „8.x.x.x“ für die GSKit-Version:

```
rpm -U gskcrypt64-8.x.x.x.linux.ppc64le.rpm gskssl64-8.x.x.x.linux.ppc64le.rpm
```
4. Installieren Sie die IBM Spectrum Protect-API und wahlweise das Common Inventory Technology-Paket, das für die Unterstützung von PVU-Berechnungen benötigt wird.

- a. Erforderlich: Installieren Sie die API:

```
rpm -ivh TIVsm-API64.ppc64le.rpm
```

- b. Optional: Installieren Sie das durch die API verwendete Common Inventory Technology-Paket. Dieses Paket ist von der API abhängig und muss daher nach der Installation des API-Pakets installiert werden.

```
rpm -ivh TIVsm-APIcit.ppc64le.rpm
```

Tipp: Wenn Sie ein Upgrade für die API durchführen wollen und das Common Inventory Technology-Paket zuvor installiert wurde, müssen Sie sowohl ein Upgrade der API als auch ein Upgrade des Common Inventory Technology-Pakets durchführen. Sie können beispielsweise den folgenden Befehl ausführen:

```
rpm -U TIVsm-API64.ppc64le.rpm TIVsm-APIcit.ppc64le.rpm
```

Falls Sie lediglich eine Installation der API benötigen, können Sie die Prozedur an dieser Stelle beenden. Die nachfolgenden Schritte in dieser Prozedur beschreiben, wie die Komponenten für den Client für Sichern/Archivieren und ein optionales Clientpaket installiert werden, das nur dann benötigt wird, wenn der Client PVU-Messwerte an den Server senden soll. In den nachfolgenden Schritten ist außerdem die Installation der Pakete beschrieben, die Sie benötigen, wenn Sie journalbasierte Sicherungen ausführen wollen.

5. Installieren Sie den Client für Sichern/Archivieren und wahlweise das Common Inventory Technology-Paket, das für die Unterstützung von PVU-Berechnungen benötigt wird.
 - a. Installieren Sie die Komponenten des Clients für Sichern/Archivieren.

```
rpm -ivh TIVsm-BA.ppc64le.rpm
```
 - b. Optional: Installieren Sie das Common Inventory Technology-Paket, das vom Client verwendet wird, um PVU-Messwerte an den Server zu senden. Dieses Paket ist vom Clientpaket abhängig und muss daher nach der Installation des Clientpakets installiert werden.

```
rpm -ivh TIVsm-BAcit.ppc64le.rpm
```
6. Optional: Falls Sie journalbasierte Sicherungen verwenden wollen, installieren Sie die Pakete, die für die Dateipfadkomponente und die journalbasierten Sicherungen erforderlich sind.
 - a. Extrahieren Sie `TIVsm-filepath-source.tar.gz` und lesen Sie die Kompilier- und Installationsanweisungen in der README-Datei. Das Kernelmodul für den Dateipfad wird gemäß den Bedingungen von 'GNU General Public License' (GPL) lizenziert.

Gelegentlich können Buildprobleme aufgrund der dynamischen Natur des Linux-Kernels auftreten. Wenn die Quelle in Ihrer Linux-Distribution nicht korrekt erstellt wird, senden Sie eine E-Mail an tsmosreq@us.ibm.com, um die neueste Quellendatei anzufordern. Schließen Sie die Version der Linux-Distribution und die Ausgabe des Befehls `uname -a` zusammen mit der Version des IBM Spectrum Protect-Clients, die Sie installieren, ein.

- b. Installieren Sie das Paket für die journalbasierte Sicherung:

```
rpm -ivh TIVsm-JBB.ppc64le.rpm
```

Zugehörige Konzepte:

Kapitel 2, „IBM Spectrum Protect-Client konfigurieren“, auf Seite 53

Client für Sichern/Archivieren unter Linux on Power Systems (Little Endian) deinstallieren

Sie können den IBM Spectrum Protect-Client unter Linux on Power Systems (Little Endian) deinstallieren.

Vorbereitende Schritte

Sie müssen als Rootbenutzer angemeldet sein, um das Produkt deinstallieren zu können. Sie müssen die Pakete in der angezeigten Reihenfolge deinstallieren, andernfalls schlägt die Deinstallation fehl.

Vorgehensweise

Um den Client für Sichern/Archivieren zu deinstallieren, geben Sie die folgenden Befehle ein. Mit diesen Befehlen werden die Pakete für die journalbasierte Sicherung, die Dateipfadkomponente, den Client für Sichern/Archivieren, die API und IBM Global Security Kit (GSKit) entfernt.

Tipp: Die Versionsnummer der Pakete ist nicht erforderlich.

1. Sollen nur die Komponenten für die journalbasierte Sicherung deinstalliert werden, entfernen Sie beide Pakete (journalbasierte Sicherung und Dateipfad). Das Paket TIVsm-JBB ist vom Dateipfadpaket abhängig. Wenn Sie zwei separate Befehle **rpm -e** verwenden, um die Komponenten nacheinander zu deinstallieren, deinstallieren Sie zuerst das Paket TIVsm-JBB.

```
rpm -e TIVsm-JBB TIVsm-filepath
```

2. Deinstallieren Sie das Paket für den Client für Sichern/Archivieren:

```
rpm -e TIVsm-BA
```

3. Deinstallieren Sie die Pakete für den Client für Sichern/Archivieren:

- a. Wenn das Common Inventory Technology-Paket für den Client (TIVsmBAcit) installiert wurde, deinstallieren Sie es:

```
rpm -e TIVsm-BAcit
```

- b. Deinstallieren Sie das Paket für den Client für Sichern/Archivieren:

```
rpm -e TIVsm-BA
```

4. Deinstallieren Sie Produkte, die von der API abhängig sind, wie beispielsweise IBM Spectrum Protect for Databases und IBM Spectrum Protect for Mail. Alle von der API abhängigen Produkte müssen vor der Deinstallation des API-Pakets deinstalliert werden. Falls Sie ein von der API abhängiges Produkt deinstallieren, müssen Sie es nach der Installation einer neueren Version der Pakete für die API und den Client für Sichern/Archivieren erneut installieren. Befolgen Sie die Anweisungen in den von der API abhängigen Produkten, um zu bestimmen, welche Maßnahmen erforderlich sind, um einen Datenverlust beim Deinstallieren und erneuten Installieren der Produkte zu verhindern.

5. Deinstallieren Sie das API-Paket mit dem folgenden Befehl:

```
rpm -e TIVsm-API64
```

6. Deinstallieren Sie die API-Pakete:

- a. Wenn das Common Inventory Technology-Paket für die API (TIVsm-APIcit installiert wurde, deinstallieren Sie es:

```
rpm -e TIVsm-APIcit
```

- b. Deinstallieren Sie das API-Paket mit dem folgenden Befehl:

```
rpm -e TIVsm-API64
```

7. Deinstallieren Sie GSKit, indem Sie den folgenden Befehl eingeben:

```
rpm -e gskcrypt64 gskss164
```

Zugehörige Tasks:

„Client für Sichern/Archivieren unter Linux on Power Systems (Little Endian) installieren“ auf Seite 18

Client für Sichern/Archivieren unter Ubuntu Linux on Power Systems (Little Endian) installieren

Sie können den Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.

Vorbereitende Schritte

Sie müssen als der Rootbenutzer angemeldet sein, um das Produkt installieren zu können.

Mit diesem Installationsverfahren können neue Verteilungen oder Aktualisierungen von heruntergeladenen Installationsmedien installiert werden. Die heruntergeladenen Dateien, die Sie zum Installieren des Clients verwenden, können gegebenenfalls komprimiert sein. Kopieren oder extrahieren Sie die Dateien abhängig vom Format der Paketdatei auf Platte und installieren Sie die Komponenten gemäß diesen Anweisungen.

Sie können die entsprechende Paketdatei von einer der folgenden Websites herunterladen:

- Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.
- Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.

Informationen zu diesem Vorgang

Die folgenden Installationspakete sind auf den Installationsmedien verfügbar.

Tabelle 12. Paketnamen, Inhalt und Standardverzeichnis

Paketname	Inhalt	Standardverzeichnis
gskcrypt64_8.x.x.x.ppc64el.deb	64-Bit-Version der Global Security Kit-Pakete (GSKit)	/usr/local/ibm/gsk8
gskss164_8.x.x.x.ppc64el.deb		
tivsm-api64.ppc64el.deb	Anwendungsprogrammierschnittstelle (API), die die gemeinsam genutzte Bibliothek und Beispiele für die IBM Spectrum Protect-API enthält.	/opt/tivoli/tsm/client/api/bin64

Tabelle 12. Paketnamen, Inhalt und Standardverzeichnis (Forts.)

Paketname	Inhalt	Standardverzeichnis
tivsm-ba.ppc64el.deb	Client für Sichern/ Archivieren (Befehlszeile und GUI), Verwaltungsclient (dsmadm) und Web- Client	/opt/tivoli/tsm/client/ba/bin Dieses Verzeichnis ist normalerweise das Standardinstallationsverzeichnis für viele Da- teien des Clients für Sichern/Archivieren. Die Beispielsystemoptionsdatei (dsm.sys.smp) wird in dieses Verzeichnis geschrieben. Wenn Sie die Umgebungsvariable DSM_DIR nicht definieren, werden die ausführbare Da- tei dsmc, die Ressourcendateien und die Datei dsm.sys in diesem Verzeichnis gespeichert. Wenn Sie die Umgebungsvariable DSM_CONFIG nicht definieren, muss sich die Clientbenutzeroptionsdatei in diesem Verzeichnis befinden. Wenn Sie die Umgebungsvariable DSM_LOG nicht definieren, schreibt der Client für Sichern/Archivieren Nachrichten in die Da- teien dsmerror.log und dsmsched.log des aktuellen Arbeitsverzeichnisses.
tivsm-apicit.ppc64el.deb tivsm-bacit.ppc64el.deb	Optional. Diese Dateien stellen die Com- mon Inventory Technology-Kompo- nenten bereit, mit de- nen Sie Informationen zur Anzahl der Client- und Servereinheiten, die mit dem System verbunden sind, sowie zur Nutzung der Pro- zessor-Value-Units (PVUs) durch Servereinheiten abru- fen können. Weitere Informationen zu PVUs finden Sie in Prozessor-Value-Units schätzen in der Doku- mentation zum IBM Spectrum Protect-Ser- ver.	APicit wird im Verzeichnis /opt/tivoli/tsm/client/api/bin64/cit ins- talliert. BAcit wird im Verzeichnis /opt/tivoli/tsm/client/ba/bin/cit instal- liert.
TIVsm-filepath-source.tar.gz tivsm-jbb.ppc64el.deb	Dateien, die für journalbasierte Siche- rungen erforderlich sind	Das Paket TIVsm-filepath-source.tar.gz wird im Verzeichnis /opt/filepath instal- liert. Das Paket tivsm-jbb.ppc64el.rpm wird im Verzeichnis /opt/tivoli/tsm/client/ba/bin installiert.

Vorgehensweise

1. Stellen Sie den Datenträger bereit, von dem die Pakete installiert werden.

2. Wechseln Sie in das Verzeichnis, in dem die Installationspakete gespeichert sind.
3. Installieren Sie die 64-Bit-Version der GSKit-Pakete. In dem folgenden Befehlsbeispiel stehen die Zeichen "8.x.x.x" für die GSKit-Version:

```
dpkg -i gskcrypt64_8.x.x.x.ppc64el.deb gskssl64_8.x.x.x.ppc64el.deb
```
4. Installieren Sie die IBM Spectrum Protect-API und wahlweise das Common Inventory Technology-Paket, das für die Unterstützung von PVU-Berechnungen benötigt wird.
 - a. Erforderlich: Installieren Sie die API:

```
dpkg -i tivsm-api64.ppc64el.deb
```
 - b. Optional: Installieren Sie das durch die API verwendete Common Inventory Technology-Paket. Dieses Paket ist von der API abhängig und muss daher nach der Installation des API-Pakets installiert werden.

```
dpkg -i tivsm-apicit.ppc64el.deb
```

Tip: Wenn Sie ein Upgrade für die API durchführen wollen und das Common Inventory Technology-Paket zuvor installiert wurde, müssen Sie sowohl ein Upgrade der API als auch ein Upgrade des Common Inventory Technology-Pakets durchführen. Sie können beispielsweise den folgenden Befehl ausführen:

```
dpkg -i tivsm-api64.ppc64el.deb
      tivsm-apicit.ppc64el.deb
```

Falls Sie lediglich eine Installation der API benötigen, können Sie die Prozedur an dieser Stelle beenden. Die nachfolgenden Schritte in dieser Prozedur beschreiben, wie die Komponenten für den Client für Sichern/Archivieren und ein optionales Clientpaket installiert werden, das nur dann benötigt wird, wenn der Client PVU-Messwerte an den Server senden soll. In den nachfolgenden Schritten ist außerdem die Installation der Pakete beschrieben, die Sie benötigen, wenn Sie journalbasierte Sicherungen ausführen wollen.

5. Installieren Sie den Client für Sichern/Archivieren:

```
dpkg -i tivsm-ba.ppc64el.deb
```
6. Optional: Wenn journalbasierte Sicherungen verwendet werden sollen, installieren Sie die folgenden Pakete:
 - a. Extrahieren Sie TIVsm-filepath-source.tar.gz und prüfen Sie die README-Datei auf Anweisungen zur Vorgehensweise beim Kompilieren und Installieren der Software. Das Kernelmodul für den Linux-Dateipfad wird gemäß den Bedingungen von 'GNU General Public License' (GPL) lizenziert.

 Gelegentlich können Buildprobleme aufgrund der dynamischen Natur des Linux-Kernels auftreten. Wenn die Quelle in Ihrer Linux-Distribution nicht korrekt erstellt wird, senden Sie eine E-Mail an tsmosreq@us.ibm.com, um die neueste Quellendatei anzufordern. Schließen Sie die Version der Linux-Distribution und die Ausgabe des Befehls **uname -a** zusammen mit der Version des IBM Spectrum Protect-Clients, die Sie installieren, ein.
 - b. Installieren Sie das Paket für die journalbasierte Sicherung:

```
dpkg -i tivsm-jbb.ppc64el.deb
```

Zugehörige Konzepte:

Kapitel 2, „IBM Spectrum Protect-Client konfigurieren“, auf Seite 53

Client unter Ubuntu Linux on Power Systems (Little Endian) deinstallieren

Sie können den IBM Spectrum Protect-Client für Sichern/Archivieren unter Ubuntu Linux on Power Systems (Little Endian) deinstallieren.

Vorbereitende Schritte

Sie müssen als der Rootbenutzer angemeldet sein, um das Produkt deinstallieren zu können.

Voraussetzung: Sie müssen die Pakete in der angezeigten Reihenfolge deinstallieren, andernfalls schlägt die Deinstallation fehl.

Vorgehensweise

Um den Client für Sichern/Archivieren zu deinstallieren, geben Sie die folgenden Befehle ein. Mit diesen Befehlen werden die Pakete für die journalbasierte Sicherung, den Client für Sichern/Archivieren, die API und IBM Global Security Kit (GSKit) entfernt. Anweisungen zur Deinstallation der Dateipfadkomponente werden mit dem Quellcode für den Dateipfad zusammen mit der Software von IBM bereitgestellt.

Tipp: Die Versionsnummer der Pakete ist nicht erforderlich.

1. Sollen nur die Komponenten für die journalbasierte Sicherung deinstalliert werden, entfernen Sie das Paket `tivsm-jbb` und das Dateipfadpaket. Das Paket `tivsm-jbb` ist vom Dateipfadpaket abhängig. Deinstallieren Sie das Paket `tivsm-jbb` zuerst.
 - a. `dpkg -r tivsm-jbb`
 - b. `dpkg -r TIVsm-filepath`
2. Deinstallieren Sie das Paket für den Client für Sichern/Archivieren:
`dpkg -r tivsm-ba`
3. Deinstallieren Sie alle Produkte, die von der API abhängig sind, wie beispielsweise IBM Spectrum Protect for Databases und IBM Spectrum Protect for Mail. Falls Sie ein von der API abhängiges Produkt deinstallieren, müssen Sie es nach der Installation einer neueren Version der Pakete für die API und den Client für Sichern/Archivieren erneut installieren. Befolgen Sie die Anweisungen in den von der API abhängigen Produkten, um zu bestimmen, welche Maßnahmen erforderlich sind, um einen Datenverlust beim Deinstallieren und erneuten Installieren der Produkte zu verhindern.
4. Deinstallieren Sie das API-Paket, indem Sie den folgenden Befehl ausgeben:
`dpkg -r tivsm-api64`
5. Entfernen Sie die GSKit-Pakete:
`dpkg -r gskcrypt64 gskssl64`

Zugehörige Tasks:

„Client für Sichern/Archivieren unter Ubuntu Linux on Power Systems (Little Endian) installieren“ auf Seite 22

API unter Linux on Power Systems (Big Endian) installieren

Sie können die IBM Spectrum Protect-API von den Produktinstallationsmedien installieren.

Vorbereitende Schritte

Sie müssen als Rootbenutzer angemeldet sein, um das Produkt installieren zu können.

Informationen zu diesem Vorgang

Falls IBM Spectrum Protect Version 6.2 (oder eine frühere Version) installiert ist, entfernen Sie diese Version (**rpm -e**) und alle anderen abhängigen Softwareprogramme, bevor Sie eine höhere Version installieren.

Falls IBM Spectrum Protect Version 6.3 (oder höher) installiert ist, können Sie die Upgradeoption von rpm (**rpm -U**) oder die Aktualisierungsoption von rpm (**rpm -F**) verwenden, um für die vorhandene Software ein Upgrade auf eine höhere Version durchzuführen. Mit dem Befehl **rpm -U** können Sie neue Pakete installieren oder für vorhandene Pakete ein Upgrade durchführen; **rpm -F** kann lediglich zum Aktualisieren von bereits installierten Paketen verwendet werden.

Stoppen Sie alle aktiven Clientprozesse, bevor Sie eine Deinstallation oder ein Upgrade der API oder des Clients für Sichern/Archivieren von IBM Spectrum Protect durchführen. Wenn Sie einen Client der Version 7.1.2 oder früher verwenden, müssen Sie alle Sprachenpakete deinstallieren, bevor Sie mit dem Upgrade fortfahren.

Tabelle 13 zeigt die Installationsoptionen, die in nicht komprimierten Paketen auf den Installationsmedien verfügbar sind.

Tabelle 13. Paketnamen, Inhalt und Standardverzeichnis

Paketname	Inhalt	Standardverzeichnis
gskcrypt64-8.x.x.x.linux.ppc.rpm gskssl64-8.x.x.x.linux.ppc.rpm	64-Bit-Version der Global Security Kit-Pakete (GSKit)	/usr/local/ibm/gsk8
TIVsm-API64.ppc64.rpm	Anwendungsprogrammierschnittstelle (API), die die gemeinsam genutzten Bibliotheken und Beispiele für die IBM Spectrum Protect-API enthält.	/opt/tivoli/tsm/client/api/bin64
TIVsm-APIcit.ppc64.rpm	Optional. Diese Dateien stellen die Common Inventory Technology-Komponenten bereit, mit denen Sie Informationen zur Anzahl der Client- und Servereinheiten, die mit dem System verbunden sind, sowie zur Nutzung der Prozessor-Value-Units (PVUs) durch Servereinheiten abrufen können. Weitere Informationen zu PVUs finden Sie in Prozessor-Value-Units schätzen in der Dokumentation zum IBM Spectrum Protect-Server.	APIcit wird im Verzeichnis /opt/tivoli/tsm/client/api/bin64/cit installiert.

Mit diesem Installationsverfahren können neue Verteilungen oder Aktualisierungen von heruntergeladenen Installationsmedien installiert werden. Die heruntergeladenen Dateien, die Sie zum Installieren des Clients verwenden, können gegebenenfalls komprimiert sein. Kopieren oder extrahieren Sie die Dateien abhängig vom Format der Paketdatei auf Platte und installieren Sie die Komponenten gemäß diesen Anweisungen.

Sie können die entsprechende Paketdatei von einer der folgenden Websites herunterladen:

- Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.
- Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.

Vorgehensweise

1. Stellen Sie den Datenträger bereit, von dem die Installation erfolgt.
2. Wechseln Sie in das Verzeichnis, in dem die Installationspakete gespeichert sind.
3. Installieren Sie die 64-Bit-Version der GSKit-Pakete. In diesem Beispiel stehen die Zeichen „8.x.x.x“ für die GSKit-Version:

```
rpm -U gskcrypt64-8.x.x.x.linux.ppc.rpm gskssl64-8.x.x.x.linux.ppc.rpm
```
4. Installieren Sie die IBM Spectrum Protect-API und wahlweise das Common Inventory Technology-Paket, das für die Unterstützung von PVU-Berechnungen benötigt wird.
 - a. Erforderlich: Installieren Sie die API:

```
rpm -i TIVsm-API64.ppc64.rpm
```
 - b. Optional: Installieren Sie das durch die API verwendete Common Inventory Technology-Paket. Dieses Paket ist von der API abhängig und muss daher nach der Installation des API-Pakets installiert werden.

```
rpm -i TIVsm-APIcit.ppc64.rpm
```

Tipp: Wenn Sie ein Upgrade für die API durchführen wollen und das Common Inventory Technology-Paket zuvor installiert wurde, müssen Sie sowohl ein Upgrade der API als auch ein Upgrade des Common Inventory Technology-Pakets durchführen. Sie können beispielsweise den folgenden Befehl ausführen:

```
rpm -U TIVsm-API64.ppc64.rpm TIVsm-APIcit.ppc64.rpm
```

Zugehörige Konzepte:

Kapitel 2, „IBM Spectrum Protect-Client konfigurieren“, auf Seite 53

API unter Linux on Power Systems (Big Endian) deinstallieren

Sie können die IBM Spectrum Protect-API unter IBM Spectrum Protect Linux on Power Systems (Big Endian) deinstallieren.

Vorbereitende Schritte

Sie müssen als Rootbenutzer angemeldet sein, um das Produkt deinstallieren zu können. Deinstallieren Sie die Pakete in der angezeigten Reihenfolge.

Vorgehensweise

Um ein zuvor installiertes IBM Spectrum Protect-Paket zu deinstallieren, geben Sie die folgenden Befehle ein, um die Pakete für die journalbasierte Sicherung, die Da-

teipfadkomponente, den Client für Sichern/Archivieren (falls zutreffend), die API und IBM Global Security Kit (GSKit) zu entfernen.

Tipp: Die Versionsnummer der Pakete wird für die Deinstallation nicht benötigt.

1. Führen Sie diesen Schritt aus, wenn zuvor ein Client der Version 7.1 oder früher installiert wurde.

Sollen nur die Komponenten für die journalbasierte Sicherung deinstalliert werden, entfernen Sie beide Pakete (journalbasierte Sicherung und Dateipfad). Das Paket TIVsm-JBB ist vom Dateipfadpaket abhängig. Wenn Sie zwei separate Befehle **rpm -e** verwenden, um die Komponenten nacheinander zu deinstallieren, deinstallieren Sie zuerst das Paket TIVsm-JBB.

```
rpm -e TIVsm-JBB TIVsm-filepath
```

2. Wenn zuvor ein Client der Version 7.1 oder früher installiert wurde, deinstallieren Sie die Pakete für den Clients für Sichern/Archivieren.

- a. Wenn das optionale Paket TIVsmBACit installiert wurde, deinstallieren Sie es mithilfe des folgenden Befehls:

```
rpm -e TIVsm-BACit
```

- b. Deinstallieren Sie das Paket für den Client für Sichern/Archivieren:

```
rpm -e TIVsm-BA
```

Anmerkung: Wenn Sprachenpakete in einem Client der Version 7.1.2 oder früher installiert wurden, müssen Sie diese Pakete vor dem Entfernen des API-Pakets entfernen. Geben Sie den folgenden Befehl ein und ersetzen Sie hierbei *xx_xx* jeweils durch den Sprachencode jeder zusätzlichen Sprache, die installiert wurde. Eine Liste der Sprachencodekennungen finden Sie in Tabelle 14.

```
rpm -e TIVsm-BA.msg.xx_xx
```

Tabelle 14. Kennungen der Sprachenpakete

Sprache	Sprachenkennung
Tschechisch	CS_CZ
Französisch	FR_FR
Deutsch	DE_DE
Ungarisch	HU_HU
Italienisch	IT_IT
Japanisch	JA_JP
Koreanisch	KO_KR
Polnisch	PL_PL
Portugiesisch	PT_BR
Russisch	RU_RU
Spanisch	ES_ES
Traditionelles Chinesisch (erweiterter UNIX-Code)	ZH_CN
Traditionelles Chinesisch (Big-5; die fünf wichtigsten DBCS-Sprachen)	ZH_TW

3. Deinstallieren Sie alle Produkte, die von der API abhängig sind, wie beispielsweise IBM Spectrum Protect for Databases und IBM Spectrum Protect for Mail. Alle von der API abhängigen Produkte müssen vor der Deinstallation des API-Pakets deinstalliert werden. Wenn Sie ein API-abhängiges Produkt deinstallieren, müssen Sie es nach der Installation einer neueren Version des API-Pakets

erneut installieren. Anhand der Dokumentation des abhängigen Produkts können Sie ermitteln, welche Maßnahmen erforderlich sind, um einen Datenverlust beim Deinstallieren und erneuten Installieren der Produkte zu verhindern.

4. Wenn das optionale Common Inventory Technology-Paket für die API (TIVsm-APIcit) installiert wurde, deinstallieren Sie dieses Paket mithilfe des folgenden Befehls:

```
rpm -e TIVsm-APIcit
```

5. Deinstallieren Sie das API-Paket mit dem folgenden Befehl:

```
rpm -e TIVsm-API64
```

6. Deinstallieren Sie GSKit mithilfe des folgenden Befehls:

```
rpm -e gskcrypt64 gskssl64
```

Zugehörige Tasks:

„API unter Linux on Power Systems (Big Endian) installieren“ auf Seite 25

Linux x86_64-Client installieren

Sie können den Linux x86_64-Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.

Vorbereitende Schritte

- Sie müssen als Rootbenutzer angemeldet sein, um das Produkt installieren zu können.
- Falls IBM Spectrum Protect Version 6.2 (oder eine frühere Version) installiert ist, entfernen Sie diese Version (**rpm -e**) und alle anderen abhängigen Softwareprogramme, bevor Sie eine höhere Version installieren.
- Falls IBM Spectrum Protect Version 6.3 (oder höher) installiert ist, können Sie die Upgradeoption von rpm (**rpm -U**) oder die Aktualisierungsoption von rpm (**rpm -F**) verwenden, um für die vorhandene Software ein Upgrade auf eine höhere Version durchzuführen. Mit dem Befehl **rpm -U** können Sie nur dann neue Pakete installieren oder für vorhandene Pakete ein Upgrade durchführen, wenn Sie zuvor keine Sprachenpakete installiert haben. Mit dem Befehl **rpm -F** können nur bereits installierte Pakete aktualisiert werden.
- Stoppen Sie alle aktiven Clientprozesse, bevor Sie eine Deinstallation oder ein Upgrade der API oder des Clients für Sichern/Archivieren von IBM Spectrum Protect durchführen.
- Wenn Sprachenpakete installiert sind, müssen Sie diese Pakete vor der Installation oder einem Upgrade der API oder des Clients für Sichern/Archivieren von IBM Spectrum Protect deinstallieren.

Informationen zu diesem Vorgang

Die folgenden Installationsoptionen sind in nicht komprimierten Paketen auf den Installationsmedien verfügbar.

Tabelle 15. Paketnamen, Inhalt und Standardverzeichnis

Paketname	Inhalt	Standardverzeichnis
gskcrypt64-8.x.x.x.linux.x86_64.rpm gskssl64-8.x.x.x.linux.x86_64.rpm	64-Bit-Version der Global Security Kit- Pakete (GSKit)	/usr/local/ibm/gsk8

Tabelle 15. Paketnamen, Inhalt und Standardverzeichnis (Forts.)

Paketname	Inhalt	Standardverzeichnis
TIVsm-API64.x86_64.rpm	Anwendungsprogramm- schnittstelle (API), die die gemeinsam ge- nutzten Bibliotheken und Beispiele für die IBM Spectrum Protect- API enthält.	/opt/tivoli/tsm/client/api/bin64
TIVsm-BA.x86_64.rpm	Client für Sichern/ Archivieren (Befehlszeile und GUI), Verwaltungsclient (dsmadm) und Web- Client	/opt/tivoli/tsm/client/ba/bin Dieses Verzeichnis wird für viele Dateien des Clients für Sichern/Archivieren als Standardinstallationsverzeichnis verwendet. Die Beispielsystemoptionsdatei (dsm.sys.smp) wird in dieses Verzeichnis geschrieben. Falls die Umgebungsvariable DSM_DIR nicht defi- niert ist, werden die ausführbare Datei dsmc, die Ressourcendateien und die Datei dsm.sys in diesem Verzeichnis abgelegt. Falls die Umgebungsvariable DSM_CONFIG nicht definiert ist, muss sich die Clientbenutzeroptionsdatei in diesem Ver- zeichnis befinden. Wenn Sie DSM_LOG nicht definieren, wer- den Nachrichten in die Dateien dsmerror.log und dsmsched.log im aktuellen Arbeitsverzeichnis geschrieben.
TIVsm-APIcit.x86_64.rpm TIVsm-BAcit.x86_64.rpm	Optional. Diese Dateien stellen die Com- mon Inventory Technology-Kompo- nenten bereit, mit de- nen Sie Informationen zur Anzahl der Client- und Servereinheiten, die mit dem System verbunden sind, sowie zur Nutzung der Pro- zessor-Value-Units (PVUs) durch Servereinheiten abruf- en können. Weitere Informationen zu PVUs finden Sie in Prozessor-Value-Units schätzen in der Doku- mentation zum IBM Spectrum Protect-Ser- ver.	APicit wird im Verzeichnis /opt/tivoli/tsm/client/api/bin64/cit/ ins- talliert. BAcit wird im Verzeichnis /opt/tivoli/tsm/client/ba/bin/cit/ instal- liert.
TIVsm-filepath-source.tar.gz TIVsm-JBB.x86_64.rpm	Für die Unterstützung journalbasierter Siche- rungen benötigte Da- teien.	Filepath wird in /opt/filepath installiert. JBB wird in /opt/tivoli/tsm/client/ba/bin installiert.

Tabelle 15. Paketnamen, Inhalt und Standardverzeichnis (Forts.)

Paketname	Inhalt	Standardverzeichnis
TIVsm_BAhdw.x86_64.rpm	Stellt die Unterstützung von Momentaufnahmeteilsicherungen für NetAPP- und N-Series-Dateiserver bereit.	/opt/tivoli/tsm/client/ba/bin/plugins

Mit diesem Installationsverfahren können neue Verteilungen oder Aktualisierungen von heruntergeladenen Installationsmedien installiert werden. Die heruntergeladenen Dateien, die Sie zum Installieren des Clients verwenden, können gegebenenfalls komprimiert sein. Kopieren oder extrahieren Sie die Dateien abhängig vom Format der Paketdatei auf Platte und installieren Sie die Komponenten gemäß diesen Anweisungen.

Sie können die entsprechende Paketdatei von einer der folgenden Websites herunterladen:

- Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.
- Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um den Linux x86_64-Client für Sichern/Archivieren zu installieren:

1. Stellen Sie den Datenträger bereit, von dem die Installation erfolgt.
2. Wechseln Sie in das Verzeichnis, in dem die Installationspakete gespeichert sind.
3. Installieren Sie die 64-Bit-Version der GSKit-Pakete. In diesem Beispiel stehen die Zeichen "8.x.x.x" für die GSKit-Version:

```
rpm -U gskcrypt64-8.x.x.x.linux.x86_64.rpm gskssl64-8.x.x.x.linux.x86_64.rpm
```
4. Installieren Sie die IBM Spectrum Protect-API und wahlweise das Common Inventory Technology-Paket, das für die Unterstützung von PVU-Berechnungen benötigt wird.
 - a. Erforderlich: Installieren Sie die API:

```
rpm -i TIVsm-API64.x86_64.rpm
```
 - b. Optional: Installieren Sie das durch die API verwendete Common Inventory Technology-Paket. Dieses Paket ist von der API abhängig und muss daher nach der Installation des API-Pakets installiert werden.

```
rpm -i TIVsm-APIcit.x86_64.rpm
```

Tipp: Wenn Sie ein Upgrade für die API durchführen wollen und das Common Inventory Technology-Paket zuvor installiert wurde, müssen Sie sowohl ein Upgrade der API als auch ein Upgrade des Common Inventory Technology-Pakets durchführen. Sie können beispielsweise den folgenden Befehl ausführen:

```
rpm -U TIVsm-API64.x86_64.rpm TIVsm-APIcit.x86_64.rpm
```

Falls Sie lediglich eine Installation der API benötigen, können Sie die Prozedur an dieser Stelle beenden. Die nachfolgenden Schritte in dieser Prozedur beschreiben, wie die Komponenten für den Client für Sichern/Archivieren und ein optionales Clientpaket installiert werden, das nur dann benötigt wird, wenn

der Client PVU-Messwerte an den Server senden soll. In den nachfolgenden Schritten ist außerdem die Installation der Pakete beschrieben, die Sie benötigen, wenn Sie journalbasierte Sicherungen ausführen wollen.

5. Installieren Sie den Client für Sichern/Archivieren und wahlweise das Common Inventory Technology-Paket, das für die Unterstützung von PVU-Berechnungen benötigt wird.
 - a. Installieren Sie die Komponenten des Clients für Sichern/Archivieren.

```
rpm -i TIVsm-BA.x86_64.rpm
```
 - b. Optional: Installieren Sie das Common Inventory Technology-Paket, das vom Client verwendet wird, um PVU-Messwerte an den Server zu senden. Dieses Paket ist vom Clientpaket abhängig und muss daher nach der Installation des Clientpakets installiert werden.

```
rpm -i TIVsm-BACit.x86_64.rpm
```
6. Optional: Sollen journalbasierte Sicherungen verwendet werden, müssen Sie die Dateipfadkomponente kompilieren und installieren, die dem Linux-Kernel auf Ihrem Client-Computer entspricht. Extrahieren Sie `TIVsm-filepath-source.tar.gz` und lesen Sie die Kompilier- und Installationsanweisungen in der README-Datei. Das Kernelmodul für den Linux-Dateipfad wird gemäß den Bedingungen von 'GNU General Public License' (GPL) lizenziert.

Gelegentlich können Buildprobleme aufgrund der dynamischen Natur des Linux-Kernels auftreten. Wenn die Quelle in Ihrer Linux-Distribution nicht korrekt erstellt wird, senden Sie eine E-Mail an tmosreq@us.ibm.com, um die neueste Quellendatei anzufordern. Schließen Sie die Version der Linux-Distribution und die Ausgabe des Befehls `uname -a` zusammen mit der Version des IBM Spectrum Protect-Clients, die Sie installieren, ein.
7. Installieren Sie die Unterstützung für Teilsicherungen unter Verwendung der Momentaufnahmedifferenz für NetApp- und N-Series-Dateiserver, indem Sie den folgenden Befehl eingeben:

```
rpm -i TIVsm-BAhdw.x86_64.rpm
```

Zugehörige Konzepte:

Kapitel 2, „IBM Spectrum Protect-Client konfigurieren“, auf Seite 53

Linux x86_64-Client deinstallieren

Sie können die folgende Prozedur verwenden, um den IBM Spectrum Protect Linux x86_64-Client zu deinstallieren.

Vorbereitende Schritte

Sie müssen als Rootbenutzer angemeldet sein, um das Produkt deinstallieren zu können. Deinstallieren Sie die Pakete in der angezeigten Reihenfolge.

Vorgehensweise

Um ein zuvor installiertes IBM Spectrum Protect-Clientpaket zu deinstallieren, geben Sie die folgenden Befehle ein. Mit diesen Befehlen werden die Pakete für die journalbasierte Sicherung, die Dateipfadkomponente, den Client für Sichern/Archivieren, die API und IBM Global Security Kit (GSKit) entfernt.

Tipp: Die Versionsnummer der Pakete wird für die Deinstallation nicht benötigt.

1. Sollen nur die Komponenten für die journalbasierte Sicherung deinstalliert werden, entfernen Sie beide Pakete (journalbasierte Sicherung und Dateipfad). Das Paket `TIVsm-JBB` ist vom Dateipfadpaket abhängig. Wenn Sie zwei separate Be-

fehlt **rpm -e** verwenden, um die Komponenten nacheinander zu deinstallieren, deinstallieren Sie zuerst das Paket TIVsm-JBB.

```
rpm -e TIVsm-JBB TIVsm-filepath
```

2. Deinstallieren Sie die Pakete für den Client für Sichern/Archivieren:

- a. Falls das optionale Paket TIVsm-BACit installiert wurde, deinstallieren Sie es, bevor Sie den Client deinstallieren:

```
rpm -e TIVsm-BACit
```

- b. Deinstallieren Sie den Client für Sichern/Archivieren.

```
rpm -e TIVsm-BA
```

Anmerkung: Wenn Sprachenpakete in einem Client der Version 7.1.2 oder früher installiert wurden, müssen Sie diese Pakete vor dem Entfernen des API-Pakets entfernen. Geben Sie den folgenden Befehl ein und ersetzen Sie hierbei *xx_xx* jeweils durch den Sprachencode jeder zusätzlichen Sprache, die installiert wurde. Eine Liste der Sprachencodierungen finden Sie in Tabelle 16.

```
rpm -e TIVsm-msg.xx_xx
```

Tabelle 16. Kennungen der Sprachenpakete

Sprache	Sprachenkennung
Tschechisch	CS_CZ
Französisch	FR_FR
Deutsch	DE_DE
Ungarisch	HU_HU
Italienisch	IT_IT
Japanisch	JA_JP
Koreanisch	KO_KR
Polnisch	PL_PL
Portugiesisch	PT_BR
Russisch	RU_RU
Spanisch	ES_ES
Traditionelles Chinesisch (erweiterter UNIX-Code)	ZH_CN
Traditionelles Chinesisch (Big-5; die fünf wichtigsten DBCS-Sprachen)	ZH_TW

3. Deinstallieren Sie alle Produkte, die von der API abhängig sind, wie beispielsweise IBM Spectrum Protect for Databases und IBM Spectrum Protect for Mail. Alle von der API abhängigen Produkte müssen vor der Deinstallation des API-Pakets deinstalliert werden. Falls Sie ein von der API abhängiges Produkt deinstallieren, müssen Sie es nach der Installation einer neueren Version der Pakete für die API und den Client für Sichern/Archivieren erneut installieren. Anhand der Dokumentation des abhängigen Produkts können Sie ermitteln, welche Maßnahmen erforderlich sind, um einen Datenverlust beim Deinstallieren und erneuten Installieren der Produkte zu verhindern.

- a. Falls das optionale Common Inventory Technology-Paket für die API (TIVsm-APIcit) installiert wurde, deinstallieren Sie dieses Paket, bevor Sie das API-Paket deinstallieren. Verwenden Sie zum Deinstallieren des Pakets den folgenden Befehl:

```
rpm -e TIVsm-APIcit
```

- b. Deinstallieren Sie das API-Paket mit dem folgenden Befehl:

```
rpm -e TIVsm-API64
```

4. Geben Sie den folgenden Befehl ein, um das 64-Bit-Paket von GSKit zu entfernen:

```
rpm -e gskcrypt64 gskssl64
```

Zugehörige Tasks:

„Linux x86_64-Client installieren“ auf Seite 29

Ubuntu Linux x86_64-Client installieren

Sie können den Ubuntu Linux 64-Bit-Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.

Informationen zu diesem Vorgang

Die folgenden Installationsoptionen sind in nicht komprimierten Paketen auf den Installationsmedien verfügbar.

Tabelle 17. Paketnamen, Inhalt und Standardverzeichnis

Paketname	Inhalt	Standardverzeichnis
gskcrypt64_8.0-50.40.linux.x86_64.deb gskssl64_8.0-50.40.linux.x86_64.deb	64-Bit-Version der Global Security Kit-Pakete (GSKit)	/usr/local/ibm/gsk8
tivsm-api64.amd64.deb	Anwendungsprogrammierschnittstelle (API), die die gemeinsam genutzten Bibliotheken und Beispiele für die IBM Spectrum Protect-API enthält.	/opt/tivoli/tsm/client/api/bin64
tivsm-ba.amd64.deb	Client für Sichern/Archivieren (Befehlszeile und GUI), Verwaltungsclient (dsmadm) und Web-Client	<p>/opt/tivoli/tsm/client/ba/bin</p> <p>Dieses Verzeichnis wird für viele Dateien des Clients für Sichern/Archivieren als Standardinstallationsverzeichnis verwendet. Die Beispielsystemoptionsdatei (dsm.sys.smp) wird in dieses Verzeichnis geschrieben. Falls die Umgebungsvariable DSM_DIR nicht definiert ist, werden die ausführbare Datei dsmc, die Ressourcendateien und die Datei dsm.sys in diesem Verzeichnis abgelegt.</p> <p>Falls die Umgebungsvariable DSM_CONFIG nicht definiert ist, muss sich die Clientbenutzeroptionsdatei in diesem Verzeichnis befinden.</p> <p>Wenn Sie DSM_LOG nicht definieren, werden Nachrichten in die Dateien dsmerror.log und dsmsched.log im aktuellen Arbeitsverzeichnis geschrieben.</p>

Tabelle 17. Paketnamen, Inhalt und Standardverzeichnis (Forts.)

Paketname	Inhalt	Standardverzeichnis
tivsm-apicit.amd64.deb tivsm-bacit.amd64.deb	Optional. Diese Dateien stellen die Common Inventory Technology-Komponenten bereit, mit denen Sie Informationen zur Anzahl der Client- und Servereinheiten, die mit dem System verbunden sind, sowie zur Nutzung der Prozessor-Value-Units (PVUs) durch Servereinheiten abrufen können. Weitere Informationen zu PVUs finden Sie in Prozessor-Value-Units schätzen in der Dokumentation zum IBM Spectrum Protect-Server.	APicit wird im Verzeichnis /opt/tivoli/tsm/client/api/bin64/cit installiert. BACit wird im Verzeichnis /opt/tivoli/tsm/client/ba/bin/cit installiert.
tivsm-filepath-source.tar.gz tivsm-jbb.amd64.deb	Für die Unterstützung journalbasierter Sicherungen benötigte Dateien.	Die Pakete filepath und tivsm-jbb sind nur erforderlich, wenn Sie journalbasierte Sicherungen verwenden wollen. Das Paket tivsm-jbb.x86_64.deb wird in /opt/tivoli/tsm/client/ba/bin installiert.
tivsm-bahdw.amd64.deb	Stellt die Unterstützung von Momentaufnahmeteilsicherungen für NetAPP- und N-Series-Dateiserver bereit.	/opt/tivoli/tsm/client/ba/bin/plugins

Mit diesem Installationsverfahren können neue Verteilungen oder Aktualisierungen von heruntergeladenen Installationsmedien installiert werden. Die heruntergeladenen Dateien, die Sie zum Installieren des Clients verwenden, können gegebenenfalls komprimiert sein. Kopieren oder extrahieren Sie die Dateien abhängig vom Format der Paketdatei auf Platte und installieren Sie die Komponenten gemäß diesen Anweisungen.

Sie können die entsprechende Paketdatei von einer der folgenden Websites herunterladen:

- Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.
- Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um den Ubuntu Linux x86_64-Client für Sichern/Archivieren zu installieren.

1. Stellen Sie den Datenträger bereit, von dem die Installation erfolgt.

2. Wechseln Sie in das Verzeichnis, in dem die Installationspakete gespeichert sind.
3. Installieren Sie die 64-Bit-Version der GSKit-Pakete.

```
sudo dpkg -i gskcrypt64_8.0-50.40.linux.x86_64.deb gskssl64_8.0-50.40.linux.x86_64.deb
```
4. Installieren Sie die IBM Spectrum Protect-API und wahlweise das Common Inventory Technology-Paket, das für die Unterstützung von PVU-Berechnungen benötigt wird.
 - a. Erforderlich: Installieren Sie die API:

```
sudo dpkg -i tivsm-api64.amd64.deb
```
 - b. Optional: Installieren Sie das durch die API verwendete Common Inventory Technology-Paket. Dieses Paket ist von der API abhängig und muss daher nach der Installation des API-Pakets installiert werden.

```
sudo dpkg -i tivsm-apicit.amd64.deb
```

Tipp: Wenn Sie ein Upgrade für die API durchführen wollen und das Common Inventory Technology-Paket zuvor installiert wurde, müssen Sie sowohl ein Upgrade der API als auch ein Upgrade des Common Inventory Technology-Pakets durchführen. Sie können beispielsweise den folgenden Befehl ausführen:

```
sudo dpkg -i tivsm-api64.amd64.deb
tivsm-apicit.amd64.deb
```

Falls Sie lediglich eine Installation der API benötigen, können Sie die Prozedur an dieser Stelle beenden. Die nachfolgenden Schritte in dieser Prozedur beschreiben, wie die Komponenten für den Client für Sichern/Archivieren und ein optionales Clientpaket installiert werden, das nur dann benötigt wird, wenn der Client PVU-Messwerte an den Server senden soll. In den nachfolgenden Schritten ist außerdem die Installation der Pakete beschrieben, die Sie benötigen, wenn Sie journalbasierte Sicherungen ausführen wollen.

5. Installieren Sie den Client für Sichern/Archivieren und wahlweise das Common Inventory Technology-Paket, das für die Unterstützung von PVU-Berechnungen benötigt wird.
 - a. Installieren Sie die Komponenten des Clients für Sichern/Archivieren.

```
sudo dpkg -i tivsm-ba.amd64.deb
```
 - b. Optional: Installieren Sie das Common Inventory Technology-Paket, das vom Client verwendet wird, um PVU-Messwerte an den Server zu senden. Dieses Paket ist vom Clientpaket abhängig und muss daher nach der Installation des Clientpakets installiert werden.

```
sudo dpkg -i tivsm-bacit.amd64.deb
```
6. Optional: Führen Sie diesen Schritt nur aus, wenn Sie journalbasierte Sicherungen verwenden wollen.
 - a. Extrahieren Sie `tivsm-filepath-source.tar.gz` und lesen Sie die Kompilier- und Installationsanweisungen in der README-Datei. Das Kernelmodul für den Dateipfad wird gemäß den Bedingungen von 'GNU General Public License' (GPL) lizenziert.

Gelegentlich können Buildprobleme aufgrund der dynamischen Natur des Linux-Kernels auftreten. Wenn die Quelle in Ihrer Linux-Distribution nicht korrekt erstellt wird, senden Sie eine E-Mail an tsmosreq@us.ibm.com, um die neueste Quellendatei anzufordern. Schließen Sie die Version der Linux-Distribution und die Ausgabe des Befehls `uname -a` zusammen mit der Version des IBM Spectrum Protect-Clients, die Sie installieren, ein.
 - b. Installieren Sie das Paket für die journalbasierte Sicherung: `dpkg -i tivsm-jbb.amd64.deb`.

7. Installieren Sie die Unterstützung für Teilsicherungen unter Verwendung der Momentaufnahmedifferenz für NetApp- und N-Series-Dateiserver, indem Sie den folgenden Befehl eingeben:

```
sudo dpkg -i tivsm-bahdw.amd64.deb
```

Zugehörige Konzepte:

Kapitel 2, „IBM Spectrum Protect-Client konfigurieren“, auf Seite 53

Ubuntu Linux x86_64-Client deinstallieren

Verwenden Sie die folgende Prozedur, um den IBM Spectrum Protect Ubuntu Linux x86_64-Client zu deinstallieren.

Vorgehensweise

Um ein zuvor installiertes IBM Spectrum Protect-Clientpaket zu deinstallieren, geben Sie die folgenden Befehle ein, um die Pakete für die journalbasierte Sicherung, den Client für Sichern/Archivieren, die API und IBM Global Security Kit (GSKit) zu entfernen. Anweisungen zur Deinstallation der Dateipfadkomponente erhalten Sie mit dem Quellcode für den Dateipfad zusammen mit der Software von IBM.

1. Wenn Sie lediglich die Komponenten für die journalbasierte Sicherung deinstallieren wollen, entfernen Sie tivsm-jbb und die Dateipfadkomponente. Das Paket tivsm-jbb ist vom Dateipfadpaket abhängig. Deinstallieren Sie das Paket tivsm-jbb zuerst.
 - a. `sudo dpkg -r tivsm-jbb`
 - b. `sudo dpkg -r tivsm-filepath`
2. Deinstallieren Sie die Pakete für den Client für Sichern/Archivieren:
 - a. Falls das optionale Paket tivsm-bacit installiert wurde, deinstallieren Sie es, bevor Sie den Client deinstallieren:
`sudo dpkg -r tivsm-bacit`
 - b. Deinstallieren Sie den Client für Sichern/Archivieren.
`sudo dpkg -r tivsm-ba`

Anmerkung: Wenn Sprachenpakete in einem Client der Version 7.1.2 oder früher installiert wurden, müssen Sie diese Pakete vor dem Entfernen des API-Pakets entfernen. Geben Sie den folgenden Befehl ein und ersetzen Sie hierbei `xx-xx` jeweils durch den Sprachencode jeder zusätzlichen Sprache, die installiert wurde. Eine Liste der Sprachencodekennungen finden Sie in Tabelle 18.

```
dpkg -r tivsm-msg.xx-xx
```

Tabelle 18. Kennungen der Sprachenpakete

Sprache	Sprachenkennung
Tschechisch	cs-cz
Französisch	fr-fr
Deutsch	de-de
Ungarisch	hu-hu
Italienisch	it-it
Japanisch	ja-jp
Koreanisch	ko-kr
Polnisch	pl-pl
Portugiesisch	pt-br

Tabelle 18. Kennungen der Sprachenpakete (Forts.)

Sprache	Sprachenkennung
Russisch	ru-ru
Spanisch	es-es
Traditionelles Chinesisch (erweiterter UNIX-Code)	zh-cn
Traditionelles Chinesisch (Big-5; die fünf wichtigsten DBCS-Sprachen)	zh-tw

3. Deinstallieren Sie alle Produkte, die von der API abhängig sind, z. B. IBM Spectrum Protect Data Protection-Produkte. Alle von der API abhängigen Produkte müssen vor der Deinstallation des API-Pakets deinstalliert werden. Falls Sie ein von der API abhängiges Produkt deinstallieren, müssen Sie es nach der Installation einer neueren Version der Pakete für die API und den Client für Sichern/Archivieren erneut installieren. Anhand der Dokumentation des abhängigen Produkts können Sie ermitteln, welche Maßnahmen erforderlich sind, um einen Datenverlust beim Deinstallieren und erneuten Installieren der Produkte zu verhindern.
 - a. Falls das optionale Common Inventory Technology-Paket für die API (tivsm-apicit) installiert wurde, deinstallieren Sie dieses Paket, bevor Sie das API-Paket deinstallieren. Verwenden Sie zum Deinstallieren des Pakets den folgenden Befehl:


```
sudo dpkg -r tivsm-apicit
```
 - b. Deinstallieren Sie das API-Paket mit dem folgenden Befehl:


```
sudo dpkg -r tivsm-api64
```
4. Geben Sie den folgenden Befehl ein, um die 64-Bit-Pakete von GSKit zu entfernen:


```
sudo dpkg -r gskcrypt64 gskssl64
```

Zugehörige Tasks:

„Ubuntu Linux x86_64-Client installieren“ auf Seite 34

Linux on System z-Client installieren

Sie können den Linux on System z-Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.

Vorbereitende Schritte

Sie müssen als Rootbenutzer angemeldet sein, um das Produkt installieren zu können.

Informationen zu diesem Vorgang

Falls IBM Spectrum Protect Version 6.2 (oder eine frühere Version) installiert ist, entfernen Sie diese Version (**rpm -e**) und alle anderen abhängigen Softwareprogramme, bevor Sie eine höhere Version installieren.

Falls IBM Spectrum Protect Version 6.3 (oder höher) installiert ist, können Sie die Upgradeoption von rpm (**rpm -U**) oder die Aktualisierungsoption von rpm (**rpm -F**) verwenden, um für die vorhandene Software ein Upgrade auf eine höhere Version durchzuführen. Mit dem Befehl **rpm -U** können Sie neue Pakete installieren oder für vorhandene Pakete ein Upgrade durchführen; **rpm -F** kann lediglich zum Aktualisieren von bereits installierten Paketen verwendet werden.

Stoppen Sie alle aktiven Clientprozesse, bevor Sie eine Deinstallation oder ein Upgrade der API oder des Clients für Sichern/Archivieren von IBM Spectrum Protect durchführen. Wenn Sie einen Client der Version 7.1.2 oder früher verwenden, müssen Sie alle Sprachenpakete deinstallieren, bevor Sie mit dem Upgrade fortfahren.

Die folgenden Installationsoptionen sind in nicht komprimierten Paketen auf den Installationsmedien verfügbar.

Tabelle 19. Paketnamen, Inhalt und Standardverzeichnis

Paketname	Inhalt	Standardverzeichnis
gskcrypt64-8.x.x.x.linux.s390x.rpm gskssl64-8.x.x.x.linux.s390x.rpm	64-Bit-Version der Global Security Kit-Pakete (GSKit)	/usr/local/ibm/gsk8
TIVsm-API64.s390x.rpm	Anwendungsprogrammierschnittstelle (API), die die gemeinsam genutzten Bibliotheken und Beispiele für die IBM Spectrum Protect-API enthält.	/opt/tivoli/tsm/client/api/bin64
TIVsm-BA.s390x.rpm	Client für Sichern/Archivieren (Befehlszeile und GUI), Verwaltungsclient (dsmadm) und Web-Client	<p>/opt/tivoli/tsm/client/ba</p> <p>Dieses Verzeichnis wird für viele Dateien des Clients für Sichern/Archivieren als Standardinstallationsverzeichnis verwendet. Die Beispielsystemoptionsdatei (dsm.sys.smp) wird in dieses Verzeichnis geschrieben. Falls die Umgebungsvariable DSM_DIR nicht definiert ist, werden die ausführbare Datei dsmc, die Ressourcendateien und die Datei dsm.sys in diesem Verzeichnis abgelegt.</p> <p>Falls die Umgebungsvariable DSM_CONFIG nicht definiert ist, muss sich die Clientbenutzeroptionsdatei in diesem Verzeichnis befinden.</p> <p>Wenn Sie DSM_LOG nicht definieren, schreibt der Client für Sichern/Archivieren Nachrichten in die Dateien dsmerror.log und dsmsched.log im aktuellen Arbeitsverzeichnis.</p>

Tabelle 19. Paketnamen, Inhalt und Standardverzeichnis (Forts.)

Paketname	Inhalt	Standardverzeichnis
TIVsm-APIcit.s390x.rpm TIVsm-BAcit.s390x.rpm	Optional. Diese Dateien stellen die Common Inventory Technology-Komponenten bereit, mit denen Sie Informationen zur Anzahl der Client- und Servereinheiten, die mit dem System verbunden sind, sowie zur Nutzung der Prozessor-Value-Units (PVUs) durch Servereinheiten abrufen können. Weitere Informationen zu PVUs finden Sie in Prozessor-Value-Units schätzen in der Dokumentation zum IBM Spectrum Protect-Server.	APIcit wird im Verzeichnis /opt/tivoli/tsm/client/api/bin64/cit installiert. BAcit wird im Verzeichnis /opt/tivoli/tsm/client/ba/bin/cit installiert.
TIVsm-filepath-source.tar.gz TIVsm-JBB.s390x.rpm	Für die Unterstützung journalbasierter Sicherungen benötigte Dateien.	Filepath wird in /opt/filepath installiert. JBB wird in /opt/tivoli/tsm/client/ba/bin installiert.

Mit diesem Installationsverfahren können neue Verteilungen oder Aktualisierungen von heruntergeladenen Installationsmedien installiert werden. Die heruntergeladenen Dateien, die Sie zum Installieren des Clients verwenden, können gegebenenfalls komprimiert sein. Kopieren oder extrahieren Sie die Dateien abhängig vom Format der Paketdatei auf Platte und installieren Sie die Komponenten gemäß diesen Anweisungen.

Sie können die entsprechende Paketdatei von einer der folgenden Websites herunterladen:

- Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.
- Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.

Vorgehensweise

1. Stellen Sie den Datenträger bereit, von dem die Installation erfolgt.
2. Wechseln Sie in das Verzeichnis, in dem die Pakete gespeichert sind.
3. Installieren Sie die 64-Bit-Version der GSKit-Pakete. In diesem Beispiel stehen die Zeichen "8.x.x.x" für die GSKit-Version:
rpm -U gskcrypt64-8.x.x.x.linux.s390x.rpm gskssl64-8.x.x.x.linux.s390x.rpm
4. Installieren Sie die IBM Spectrum Protect-API und wahlweise das Common Inventory Technology-Paket, das für die Unterstützung von PVU-Berechnungen benötigt wird.
 - a. Erforderlich: Installieren Sie die API:
rpm -i TIVsm-API64.s390x.rpm

- b. Optional: Installieren Sie das durch die API verwendete Common Inventory Technology-Paket. Dieses Paket ist von der API abhängig und muss daher nach der Installation des API-Pakets installiert werden.

```
rpm -i TIVsm-APIcit.s390x.rpm
```

Tipp: Wenn Sie ein Upgrade für die API durchführen wollen und das Common Inventory Technology-Paket zuvor installiert wurde, müssen Sie sowohl ein Upgrade der API als auch ein Upgrade des Common Inventory Technology-Pakets durchführen. Sie können beispielsweise den folgenden Befehl ausführen:

```
rpm -U TIVsm-API64.s390x.rpm TIVsm-APIcit.s390x.rpm
```

Falls Sie lediglich eine Installation der API benötigen, können Sie die Prozedur an dieser Stelle beenden. Die nachfolgenden Schritte in dieser Prozedur beschreiben, wie die Komponenten für den Client für Sichern/Archivieren und ein optionales Clientpaket installiert werden, das nur dann benötigt wird, wenn der Client PVU-Messwerte an den Server senden soll. In den nachfolgenden Schritten ist außerdem die Installation der Pakete beschrieben, die Sie benötigen, wenn Sie journalbasierte Sicherungen ausführen wollen.

5. Installieren Sie den Client für Sichern/Archivieren und wahlweise das Common Inventory Technology-Paket, das für die Unterstützung von PVU-Berechnungen benötigt wird.
 - a. Installieren Sie die Komponenten des Clients für Sichern/Archivieren.

```
rpm -i TIVsm-BA.s390x.rpm
```
 - b. Optional: Installieren Sie das Common Inventory Technology-Paket, das vom Client verwendet wird, um PVU-Messwerte an den Server zu senden. Dieses Paket ist vom Clientpaket abhängig und muss daher nach der Installation des Clientpakets installiert werden.

```
rpm -i TIVsm-BACit.s390x.rpm
```
6. Optional: Sollen journalbasierte Sicherungen verwendet werden, müssen Sie die Dateipfadkomponente kompilieren und installieren, die dem Linux-Kernel auf Ihrem Client-Computer entspricht. Extrahieren Sie `TIVsm-filepath-source.tar.gz` und lesen Sie die Kompilier- und Installationsanweisungen in der README-Datei. Das Kernelmodul für den Linux-Dateipfad wird gemäß den Bedingungen von 'GNU General Public License' (GPL) lizenziert.

Gelegentlich können Buildprobleme aufgrund der dynamischen Natur des Linux-Kernels auftreten. Wenn die Quelle in Ihrer Linux-Distribution nicht korrekt erstellt wird, senden Sie eine E-Mail an tmosreq@us.ibm.com, um die neueste Quellendatei anzufordern. Schließen Sie die Version der Linux-Distribution und die Ausgabe des Befehls `uname -a` zusammen mit der Version des IBM Spectrum Protect-Clients, die Sie installieren, ein.

Zugehörige Konzepte:

Kapitel 2, „IBM Spectrum Protect-Client konfigurieren“, auf Seite 53

Linux on System z-Client deinstallieren

Sie können die folgenden Prozeduren verwenden, um den IBM Spectrum Protect Linux on System z-Client zu deinstallieren.

Vorbereitende Schritte

Sie müssen als Rootbenutzer angemeldet sein, um das Produkt installieren zu können. Deinstallieren Sie die Pakete in der angezeigten Reihenfolge.

Informationen zu diesem Vorgang

Um ein zuvor installiertes IBM Spectrum Protect-Clientpaket zu deinstallieren, geben Sie die folgenden Befehle ein. Mit diesen Befehlen werden die Pakete für die journalbasierte Sicherung, die Dateipfadkomponente, den Client für Sichern/Archivieren, die API und IBM Global Security Kit (GSKit) entfernt.

Tipp: Die Versionsnummer der Pakete wird für die Deinstallation nicht benötigt.

Vorgehensweise

1. Sollen nur die Komponenten für die journalbasierte Sicherung deinstalliert werden, entfernen Sie beide Pakete (journalbasierte Sicherung und Dateipfad). Das Paket TIVsm-JBB ist vom Dateipfadpaket abhängig. Wenn Sie zwei separate Befehle **rpm -e** verwenden, um die Komponenten nacheinander zu deinstallieren, deinstallieren Sie zuerst das Paket TIVsm-JBB.

```
rpm -e TIVsm-JBB TIVsm-filepath
```

2. Deinstallieren Sie die Pakete für den Client für Sichern/Archivieren:

- a. Falls das optionale Paket TIVsm-BACit installiert wurde, deinstallieren Sie es, bevor Sie den Client deinstallieren:

```
rpm -e TIVsm-BACit
```

- b. Deinstallieren Sie den Client für Sichern/Archivieren.

```
rpm -e TIVsm-BA
```

Anmerkung: Wenn Sprachenpakete in einem Client der Version 7.1.2 oder früher installiert wurden, müssen Sie diese Pakete vor dem Entfernen des API-Pakets entfernen. Geben Sie den folgenden Befehl ein und ersetzen Sie hierbei *xx_xx* jeweils durch den Sprachencode jeder zusätzlichen Sprache, die installiert wurde. Eine Liste der Sprachencodierungen finden Sie in Tabelle 20.

```
rpm -e TIVsm-msg.xx_xx
```

Tabelle 20. Kennungen der Sprachenpakete

Sprache	Sprachenkennung
Tschechisch	CS_CZ
Französisch	FR_FR
Deutsch	DE_DE
Ungarisch	HU_HU
Italienisch	IT_IT
Japanisch	JA_JP
Koreanisch	KO_KR
Polnisch	PL_PL
Portugiesisch	PT_BR
Russisch	RU_RU
Spanisch	ES_ES
Traditionelles Chinesisch (erweiterter UNIX-Code)	ZH_CN
Traditionelles Chinesisch (Big-5; die fünf wichtigsten DBCS-Sprachen)	ZH_TW

3. Deinstallieren Sie alle Produkte, die von der API abhängig sind, wie beispielsweise IBM Spectrum Protect for Databases und IBM Spectrum Protect for Mail.

Alle von der API abhängigen Produkte müssen vor der Deinstallation des API-Pakets deinstalliert werden. Falls Sie ein von der API abhängiges Produkt deinstallieren, müssen Sie es nach der Installation einer neueren Version der Pakete für die API und den Client für Sichern/Archivieren erneut installieren. Anhand der Dokumentation des abhängigen Produkts können Sie ermitteln, welche Maßnahmen erforderlich sind, um einen Datenverlust beim Deinstallieren und erneuten Installieren der Produkte zu verhindern.

- a. Falls das optionale Common Inventory Technology-Paket für die API (TIVsm-APIcit) installiert wurde, deinstallieren Sie dieses Paket, bevor Sie das API-Paket deinstallieren. Verwenden Sie zum Deinstallieren des Pakets den folgenden Befehl:

```
rpm -e TIVsm-APIcit
```

- b. Deinstallieren Sie das API-Paket mit dem folgenden Befehl:

```
rpm -e TIVsm-API64
```

4. Geben Sie den folgenden Befehl ein, um das 64-Bit-Paket von GSKit zu entfernen:

```
rpm -e gskcrypt64 gskssl64
```

Zugehörige Tasks:

„Linux on System z-Client installieren“ auf Seite 38

Mac OS X-Client installieren

Sie können den IBM Spectrum Protect Mac OS X-Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.

Vorbereitende Schritte

Sie müssen ein Systemadministrator sein, um den Client für Sichern/Archivieren installieren zu können.

Informationen zu diesem Vorgang

Mit diesem Installationsverfahren können neue Verteilungen oder Aktualisierungen von heruntergeladenen Installationsmedien installiert werden. Die heruntergeladenen Dateien, die Sie zum Installieren des Clients verwenden, können gegebenenfalls komprimiert sein. Kopieren oder extrahieren Sie die Dateien abhängig vom Format der Paketdatei auf Platte und installieren Sie die Komponenten gemäß diesen Anweisungen.

Sie können die entsprechende Paketdatei von einer der folgenden Websites herunterladen:

- Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.
- Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.

Für MAC OS X-Clients können Sie einen Installationsassistenten verwenden, der die Eingabe von Informationen während der Installation des Produkts anfordert, oder Sie können den Client über die Befehlszeile installieren. Wenn Sie den Client mit dem Installationsverfahren über die Befehlszeile installieren, wird die Installation ohne Benutzerinteraktion ausgeführt. Die Installation über die Befehlszeile ist nützlich, wenn Sie ein Installationsskript erstellen und auf vielen Knoten ausführen wollen oder wenn Sie die Software auf einem System ohne Monitor installieren müssen.

Vorgehensweise

Wählen Sie eine Installationsmethode aus und installieren Sie den Client. Verwenden Sie entweder den Installationsassistenten oder installieren Sie den Client über die Befehlszeile.

Installationsmethode	Prozedur
Installationsassistent	<ol style="list-style-type: none">1. Doppelklicken Sie auf die Datei 8.1.6.0.0-TIV-TSMBAC-Mac.dmg, um das Plattenimage anzuhängen.2. Doppelklicken Sie auf das Symbol für das IBM Spectrum Protect-Installationspaket und befolgen Sie die Bedienerführungen, um die Installation durchzuführen.
Befehlszeile:	<ol style="list-style-type: none">1. Wechseln Sie in das Verzeichnis, in dem sich das IBM Spectrum Protect-Installationsprogramm befindet.2. Installieren Sie das Paket für die angepasste Installation mit dem folgenden Befehl: <pre>/usr/sbin/installer -pkg "/Volumes/IBM Spectrum Protect/ IBM Spectrum Protect.pkg" -target /</pre>

Nächste Schritte

Im Installationsverzeichnis wird ein Muster der Clientsystemoptionsdatei, dsm.sys-.smp, erstellt. Sie können diese Musterdatei kopieren und ändern, um die Clientsystemoptionsdatei für Ihren Knoten zu erstellen. Der Standardname der Clientsystemoptionsdatei lautet dsm.sys.

Nach der Installation des Clients müssen Sie u. U. Umgebungsvariablen definieren, bevor Sie den Client verwenden. Weitere Informationen zum Definieren von Umgebungsvariablen finden Sie in „Umgebungsvariablen für die Verarbeitung definieren“ auf Seite 64.

Mac OS X-Client deinstallieren

Sie können den IBM Spectrum Protect Mac OS X-Client deinstallieren, wenn er nicht mehr benötigt wird.

Vorbereitende Schritte

Wenn der IBM Spectrum Protect-Scheduler als Starteintrag konfiguriert ist, verwenden Sie die Funktion 'IBM Spectrum Protect-Tools für Administratoren' oder das Shell-Skript StopCad.sh, um den Scheduler zu stoppen und zu deinstallieren, bevor Sie mit dieser Prozedur beginnen.

Informationen zu diesem Vorgang

Sie können den Client für Sichern/Archivieren mit einem Shell-Skript deinstallieren. Der Name des Shell-Skripts lautet uninstall.sh und es befindet sich im Stan-

productinstallationsverzeichnis /Library/Application Support/tivoli/tsm/client/ba/bin. Verwenden Sie den Befehl **sudo**, um das Script auszuführen.

Anstatt das Script zu verwenden, können Sie die folgenden Schritte ausführen:

Vorgehensweise

1. Versetzen Sie die folgenden Ordner in den Papierkorb:
 - /Applications/IBM Spectrum Protect
 - /Library/Application Support/tivoli
2. Entfernen Sie die folgenden symbolischen Verbindungen:
 - /usr/bin/dsmc
 - /usr/bin/dsmcad
 - /usr/bin/dsmadmc
 - /usr/bin/dsmtrace
 - /usr/bin/dsmagent
 - /usr/lib/libxmlutil-6.2.0.dylib
 - /usr/lib/libtsm620xerces-c1_6_0.dylib
3. Optional: Entfernen Sie die Protokolldateien und Optionsdateien, wenn Sie sie nicht aufbewahren wollen. Während des Deinstallationsprozesses bleiben sie auf der Platte, damit Ihre Einstellungen für den Fall erhalten bleiben, dass Sie das Produkt später erneut installieren.
Vom Client für Sichern/Archivieren wurden möglicherweise Protokolldateien an den folgenden Positionen erstellt:
 - a. /Library/Logs/tivoli
 - b. ~/Library/Logs/tivoliDie Clientoptionsdateien (dsm.opt und dsm.sys) werden normalerweise an den folgenden Positionen gespeichert:
 - a. /Library/Preferences/Tivoli Storage Manager
 - b. ~/Library/Preferences/Tivoli Storage Manager

Oracle Solaris x86_64-Client installieren

Sie können den IBM Spectrum Protect Oracle Solaris x86_64-Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.

Vorbereitende Schritte

Ab IBM Spectrum Protect Version 8.1.0 ist der Oracle Solaris-Client für Sichern/Archivieren nur auf der Oracle Solaris x86_64-Plattform verfügbar. Auf der Oracle Solaris SPARC-Plattform ist der Client für Sichern/Archivieren nicht mehr verfügbar. Unter Oracle Solaris SPARC ist nur die IBM Spectrum Protect-API verfügbar. Informationen zur Installation der Solaris SPARC-API finden Sie in „Oracle Solaris SPARC-API installieren“ auf Seite 48.

Informationen zu diesem Vorgang

Wenn eine vorherige Version des Clients für Sichern/Archivieren installiert ist, müssen Sie diese entfernen, bevor Sie eine neue Version installieren. Informationen zum Entfernen vorheriger Solaris-Clientpakete finden Sie in „Oracle Solaris x86_64-Client deinstallieren“ auf Seite 48.

Die IBM Spectrum Protect-Installationsverwaltungsdatei (tsmadmin) wird anstelle der Standardverwaltungsdatei (/var/sadm/install/admin) verwendet, damit Sie während der Installation nicht nach der Berechtigung für setuid, setgid oder superuser gefragt werden. Wenn die Standardverwaltungsdatei verwendet werden soll, entfernen Sie die Option -a ./tsmadmin aus den angezeigten Befehlen und beantworten Sie die Fragen zur die Berechtigung für setuid, setgid oder superuser bei der Installation mit Y.

Tabelle 21. Namen und Beschreibungen der Installationspakete

Paket	Paketname	Paketbeschreibung
IBM Global Security Kit (GSKit) 64 Bit	gsk8cry64.pkg und gsk8ssl64.pkg	Enthält IBM GSKit, das SSL-Datenverschlüsselung (SSL = Secure Sockets Layer) mit 64-Bit für die Kommunikation zwischen dem IBM Spectrum Protect-Client und -Server bereitstellt.
IBM Spectrum Protect-Anwendungsprogrammierschnittstelle (API)	TIVsmCapi.pkg	Enthält die gemeinsam genutzten Bibliotheken und Beispiele der 64-Bit-API von IBM Spectrum Protect.
Client für Sichern/Archivieren	TIVsmCba.pkg	<p>Enthält die folgenden 64-Bit-Komponenten:</p> <ul style="list-style-type: none"> • Client für Sichern/Archivieren (Befehlszeile und GUI) • Verwaltungsclient (Befehlszeile) • Web-Client für Sichern/Archivieren <p>Anmerkung:</p> <ol style="list-style-type: none"> 1. TCP/IP und gemeinsam genutzter Speicher werden als Übertragungsmethoden unterstützt. 2. Der Web-Client ist eine Komponente des Pakets des Clients für Sichern/Archivieren und kann nicht ohne dieses installiert werden.

Mit diesem Installationsverfahren können neue Verteilungen oder Aktualisierungen von heruntergeladenen Installationsmedien installiert werden. Die heruntergeladenen Dateien, die Sie zum Installieren des Clients verwenden, können gegebenenfalls komprimiert sein. Kopieren oder extrahieren Sie die Dateien abhängig vom Format der Paketdatei auf Platte und installieren Sie die Komponenten gemäß diesen Anweisungen.

Sie können die entsprechende Paketdatei von einer der folgenden Websites herunterladen:

- Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.

- Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.

Installieren Sie die Pakete in der angezeigten Reihenfolge; einige Pakete sind vom Vorhandensein anderer Pakete abhängig. Beispielsweise ist GSKit eine Voraussetzung für die API und die API ist eine Voraussetzung für das Paket des Clients für Sichern/Archivieren.

Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Stellen Sie den Datenträger bereit, von dem die Installation erfolgt.
3. Wechseln Sie in das Verzeichnis, in dem die Pakete gespeichert sind.
4. IBM GSKit ist eine Voraussetzung des Pakets für die IBM Spectrum Protect-API. Installieren Sie GSKit mit den folgenden Befehlen:

```
pkgadd -n -a ./tsmadmin -d ./gsk8cry64.pkg gsk8cry64
pkgadd -n -a ./tsmadmin -d ./gsk8ss164.pkg gsk8ss164
```

Anmerkung: Unter Solaris 10 wird mit diesen Befehlen die 64-Bit-Version von GSKit in der globalen Zone und in allen aktiven nicht globalen Zonen installiert. Um den Client nur in einer nicht globalen Sparse-Root-Zone zu installieren, muss GSKit zunächst in der globalen Zone installiert werden. Unter Solaris 11 werden die Pakete nur in der Zone installiert, in der diese Befehle ausgeführt werden.

5. Installieren Sie die IBM Spectrum Protect-API mit dem folgenden Befehl:

```
pkgadd -n -a ./tsmadmin -d ./TIVsmCapi.pkg TIVsmCapi
```

Anmerkung: Unter Solaris 10 installiert dieser Befehl die 64-Bit-API von IBM Spectrum Protect in der globalen Zone und in allen aktiven nicht globalen Zonen. Falls Sie die API nur in der globalen Zone installieren wollen, verwenden Sie den Parameter **-G** des Befehls **pkgadd**. Unter Solaris 11 wird die API nur in der Zone installiert, in der dieser Befehl ausgeführt wird.

6. Verwenden Sie den folgenden Befehl, um den Client für Sichern/Archivieren zu installieren:

```
pkgadd -n -a ./tsmadmin -d ./TIVsmCba.pkg TIVsmCba
```

Anmerkung: Unter Solaris 10 installiert dieser Befehl die Komponenten des Clients für Sichern/Archivieren in der globalen Zone und in allen aktiven nicht globalen Zonen. Falls diese nur in der globalen Zone installiert werden sollen, verwenden Sie den Parameter **-G** des Befehls **pkgadd**. Unter Solaris 11 werden die Clientkomponenten nur in der Zone installiert, in der dieser Befehl ausgeführt wird.

Ergebnisse

Wichtig: Für eine nicht globale Sparse-Root-Zone unter Solaris 10 wird das Dateisystem /usr normalerweise in der globalen Zone als schreibgeschützt (LOFS) bereitgestellt und es gelten die folgenden Bedingungen:

- Wenn der Client nicht in der globalen Zone installiert wird, wird am Ende der Installation eine Warnung angezeigt. In der Nachricht wird der globale Administrator zum Erstellen der erforderlichen Verknüpfungen aufgefordert, die in den Warnungen angegeben sind.
- Wenn der Client bereits in der globalen Zone installiert ist, ist die Erstellung dieser Verknüpfungen nicht erforderlich. Die Verknüpfungen sind bereits vorhanden und verweisen auf die korrekten ausführbaren Dateien und Bibliotheken.

Zugehörige Konzepte:

Kapitel 2, „IBM Spectrum Protect-Client konfigurieren“, auf Seite 53

Oracle Solaris x86_64-Client deinstallieren

Sie können alle Pakete deinstallieren, die zum IBM Spectrum Protect Oracle Solaris x86_64-Client gehören, einschließlich der Komponenten Befehlszeilenclient, GUI, Web-GUI und Verwaltungsclient.

Informationen zu diesem Vorgang

Wichtig: Stellen Sie sicher, dass Sie die Pakete in der angegebenen Reihenfolge deinstallieren.

Die IBM Spectrum Protect-Installationsverwaltungsdatei (tsmadmin) wird anstelle der Standardverwaltungsdatei (/var/sadm/install/admin) verwendet, damit Sie während der Installation nicht nach der Berechtigung für setuid, setgid oder superuser gefragt werden. Wenn die Standardverwaltungsdatei verwendet werden soll, entfernen Sie die Option -a ./tsmadmin aus den folgenden Befehlen und beantworten Sie die Fragen zur Berechtigung für setuid, setgid oder superuser bei der Installation mit y.

Vorgehensweise

1. Geben Sie den folgenden Befehl ein, um den Client für Sichern/Archivieren zu deinstallieren:

```
pkgrm -n -a ./tsmadmin TIVsmCba
```

Dieser Befehl deinstalliert alle Komponenten des Clients für Sichern/Archivieren (Befehlszeile, GUI, Web-GUI und Verwaltungsclient). Die Deinstallation einzelner Komponenten dieses Pakets (z. B. des Befehlszeilenclients) ist nicht möglich.

Anmerkung: Wenn landessprachliche Nachrichtenpakete in Clients der Version 7.1.2 oder früher installiert wurden, müssen Sie diese Pakete vor dem Entfernen des API-Pakets entfernen. Geben Sie den folgenden Befehl als Rootbenutzer ein:

```
pkgrm -n -a ./tsmadmin TIVsmC1Cs TIVsmC1De TIVsmC1Es TIVsmC1Fr \
TIVsmC1Hu TIVsmC1It TIVsmC1Ja TIVsmC1Ko \
TIVsmC1Pl TIVsmC1Pt TIVsmC1Ru TIVsmC1Sc TIVsmC1Tc
```

2. Geben Sie den folgenden Befehl ein, um die IBM Spectrum Protect-API zu deinstallieren:

```
pkgrm -n -a ./tsmadmin TIVsmCapi
```

Die API kann nicht entfernt werden, wenn der Client für Sichern/Archivieren installiert ist. Der Client für Sichern/Archivieren muss zuerst entfernt werden.

3. Geben Sie die folgenden Befehle ein, um GSKit zu deinstallieren:

```
pkgrm -n -a ./tsmadmin gsk8ssl64
pkgrm -n -a ./tsmadmin gsk8cry64
```

Oracle Solaris SPARC-API installieren

Sie können die IBM Spectrum Protect Oracle Solaris SPARC-API von den Produktinstallationsmedien installieren.

Informationen zu diesem Vorgang

Wenn eine vorherige Version der API installiert ist, müssen Sie diese entfernen, bevor Sie eine neue Version installieren. Informationen zum Entfernen vorheriger Solaris-API-Pakete finden Sie in „Oracle Solaris SPARC-API deinstallieren“ auf Seite 50.

Die IBM Spectrum Protect-Installationsverwaltungsdatei (tsmadmin) wird anstelle der Standardverwaltungsdatei (/var/sadm/install/admin) verwendet, damit Sie während der Installation nicht nach der Berechtigung für setuid, setgid oder superuser gefragt werden. Wenn die Standardverwaltungsdatei verwendet werden soll, entfernen Sie die Option -a ./tsmadmin aus den angezeigten Befehlen und beantworten Sie die Fragen zur Berechtigung für setuid, setgid oder superuser bei der Installation mit Y.

Tabelle 22. Namen und Beschreibungen der Installationspakete

Paket	Paketname	Paketbeschreibung
IBM Global Security Kit (GSKit) 64 Bit	gsk8cry64.pkg und gsk8ssl64.pkg	Enthält IBM GSKit, das SSL-Datenverschlüsselung (SSL = Secure Sockets Layer) mit 64-Bit für die Kommunikation zwischen der IBM Spectrum Protect-API und dem Server bereitstellt.
IBM Spectrum Protect-Anwendungsprogrammierschnittstelle (API)	TIVsmCapi.pkg	Enthält die gemeinsam genutzten Bibliotheken und Beispiele der 64-Bit-API von IBM Spectrum Protect.

Mit diesem Installationsverfahren können neue Verteilungen oder Aktualisierungen von heruntergeladenen Installationsmedien installiert werden. Die heruntergeladenen Dateien, die Sie zum Installieren des Clients verwenden, können gegebenenfalls komprimiert sein. Kopieren oder extrahieren Sie die Dateien abhängig vom Format der Paketdatei auf Platte und installieren Sie die Komponenten gemäß diesen Anweisungen.

Sie können die entsprechende Paketdatei von einer der folgenden Websites herunterladen:

- Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.
- Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.

Installieren Sie die Pakete in der angezeigten Reihenfolge.

Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Stellen Sie den Datenträger bereit, von dem die Installation erfolgt.
3. Wechseln Sie in das Verzeichnis, in dem die Pakete gespeichert sind.
4. IBM GSKit ist eine Voraussetzung des Pakets für die IBM Spectrum Protect-API. Installieren Sie GSKit mit den folgenden Befehlen:

```
pkgadd -n -a ./tsmadmin -d ./gsk8cry64.pkg gsk8cry64
pkgadd -n -a ./tsmadmin -d ./gsk8ssl64.pkg gsk8ssl64
```

Anmerkung: Unter Solaris 10 wird mit diesen Befehlen die 64-Bit-Version von GSKit in der globalen Zone und in allen aktiven nicht globalen Zonen installiert. Um die API nur in einer nicht globalen Sparse-Root-Zone zu installieren, muss GSKit zunächst in der globalen Zone installiert werden. Unter Solaris 11 werden die Pakete nur in der Zone installiert, in der diese Befehle ausgeführt werden.

5. Installieren Sie die IBM Spectrum Protect-API mit dem folgenden Befehl:

```
pkgadd -n -a ./tsmadmin -d ./TIVsmCapi.pkg TIVsmCapi
```

Anmerkung: Unter Solaris 10 installiert dieser Befehl die 64-Bit-API von IBM Spectrum Protect in der globalen Zone und in allen aktiven nicht globalen Zonen. Falls Sie die API nur in der globalen Zone installieren wollen, verwenden Sie den Parameter **-G** des Befehls **pkgadd**. Unter Solaris 11 wird die API nur in der Zone installiert, in der dieser Befehl ausgeführt wird.

Ergebnisse

Wichtig: Für eine nicht globale Sparse-Root-Zone unter Solaris 10 wird das Dateisystem /usr normalerweise in der globalen Zone als schreibgeschützt (LOFS) bereitgestellt und es gelten die folgenden Bedingungen:

- Wenn die API nicht in der globalen Zone installiert wird, wird am Ende der Installation eine Warnung angezeigt. In der Nachricht wird der globale Administrator zum Erstellen der erforderlichen Verknüpfungen aufgefordert, die in den Warnungen angegeben sind.
- Wenn die API bereits in der globalen Zone installiert ist, ist die Erstellung dieser Verknüpfungen nicht erforderlich. Die Verknüpfungen sind bereits vorhanden und verweisen auf die korrekten ausführbaren Dateien und Bibliotheken.

Zugehörige Konzepte:

Kapitel 2, „IBM Spectrum Protect-Client konfigurieren“, auf Seite 53

Oracle Solaris SPARC-API deinstallieren

Sie können alle Pakete deinstallieren, die zur IBM Spectrum Protect Oracle Solaris SPARC-API gehören.

Informationen zu diesem Vorgang

Wichtig: Stellen Sie sicher, dass Sie die Pakete in der angegebenen Reihenfolge deinstallieren.

Die IBM Spectrum Protect-Installationsverwaltungsdatei (tsmadmin) wird anstelle der Standardverwaltungsdatei (/var/sadm/install/admin) verwendet, damit Sie während der Installation nicht nach der Berechtigung für setuid, setgid oder superuser gefragt werden. Wenn die Standardverwaltungsdatei verwendet werden soll, entfernen Sie die Option -a ./tsmadmin aus den folgenden Befehlen und beantworten Sie die Fragen zur Berechtigung für setuid, setgid oder superuser bei der Installation mit y.

Vorgehensweise

1. Geben Sie den folgenden Befehl ein, um die IBM Spectrum Protect-API zu deinstallieren:

```
pkgrm -n -a ./tsmadmin TIVsmCapi
```

2. Geben Sie die folgenden Befehle ein, um GSKit zu deinstallieren:

```
pkgrm -n -a ./tsmadmin gsk8ssl64  
pkgrm -n -a ./tsmadmin gsk8cry64
```

Softwareaktualisierungen

IBM kann Softwareaktualisierungen regelmäßig für den Download bereitstellen.

Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal for IBM Spectrum Protect.

Clientverwaltungsservice zur Erfassung von Diagnoseinformationen installieren

Sie können die IBM Spectrum Protect-Clientverwaltungsservices installieren, um Diagnoseinformationen zum Client für Sichern/Archivieren zu erfassen. Der Clientverwaltungsservice macht IBM Spectrum Protect Operations Center die Informationen für grundlegende Überwachungsfunktionen verfügbar.

Informationen zu diesem Vorgang

Nachdem Sie den Client für Sichern/Archivieren installiert haben, installieren Sie den Clientverwaltungsservice auf demselben Computer, damit der IBM Spectrum Protect-Serveradministrator Diagnoseinformationen aus Operations Center anzeigen kann.

Der Clientverwaltungsservice kann auf Systemen mit dem Linux-Client für Sichern/Archivieren installiert werden.

Installationsanweisungen und weitere Informationen zum Clientverwaltungsservice finden Sie in Diagnoseinformationen mit IBM Spectrum Protect-Clientverwaltungsservices erfassen.

Kapitel 2. IBM Spectrum Protect-Client konfigurieren

Nachdem Sie den Client für Sichern/Archivieren installiert haben, müssen Sie ihn vor der Ausführung von Operationen konfigurieren.

Wenn Sie ein Upgrade des Clients für Sichern/Archivieren durchführen, ist es nicht erforderlich, den Scheduler, den Web-Client oder andere Konfigurationseinstellungen zu rekonfigurieren. Wenn die von der vorherigen Clientinstallation verwendeten Dateien `dsm.opt` und `dsm.sys` im Standardinstallationsverzeichnis bzw. in dem Verzeichnis oder der Datei verfügbar sind, auf das/die die Umgebungsvariablen `DSM_CONFIG` und `DSM_DIR` verweisen, greift der Client auf diese Dateien zu, um Konfigurationsdaten abzurufen.

Einige Konfigurationstasks sind erforderlich, andere sind optional. Die folgenden Konfigurationstasks sind erforderlich:

- „Clientsystemoptionsdatei erstellen und ändern“ auf Seite 58
- „Workstation bei einem Server registrieren“ auf Seite 128

Die folgenden Konfigurationstasks sind optional:

- „Standardclientbenutzeroptionsdatei erstellen“ auf Seite 60
- „Angepasste Clientbenutzeroptionsdatei erstellen“ auf Seite 62
- „Umgebungsvariablen“ auf Seite 63
- „Web-Client auf AIX-, Linux-, Mac- und Solaris-Systemen konfigurieren“ auf Seite 68
- „Scheduler konfigurieren“ auf Seite 69
- „Einschluss-/Ausschlussliste erstellen“ auf Seite 129
- Parallele Sicherungen von virtuellen VMware-Maschinen konfigurieren. Siehe „Parallele Sicherungen virtueller Maschinen“ auf Seite 234.

Tasks für Rootbenutzer und berechtigte Benutzer UNIX- und Linux-Clients

Ein berechtigter Benutzer ist jeder Benutzer ohne Rootberechtigung, der über Lese- und Schreibzugriff auf das gespeicherte Kennwort (Datei `TSM.sth`) verfügt, oder eine beliebige Person, die das Kennwort kennt und interaktiv eingibt. Berechtigte Benutzer definieren das Verzeichnis, in dem ihre Kopie der Kennwortdatei gespeichert ist, mit der Option `passworddir`.

In Tabelle 23 sind die Tasks aufgeführt, die ein Root, berechtigter Benutzer und andere Benutzer ausführen können bzw. nicht ausführen können.

Tabelle 23. Tasks für Roots und berechtigte Benutzer

Task	Root	Berechtigter Benutzer
Mit einem LDAP-Server zur Authentifizierung der Berechtigungsnachweise beim IBM Spectrum Protect-Server anmelden.	Ja	Ja

Tabelle 23. Tasks für Roots und berechtigte Benutzer (Forts.)

Task	Root	Berechtigter Benutzer
Neue Knoten auf dem IBM Spectrum Protect-Server registrieren (wenn die offene Registrierung auf dem Server angegeben ist).	Ja	Ja
IBM Spectrum Protect-Kennwort für Client-Workstations definieren oder erneut erstellen.	Ja	Ja
Sichern	Ja Anmerkung: Der IBM Spectrum Protect-Administrator kann entweder für den Befehl Register Node oder für den Befehl Update Node eine Option angeben, um zu definieren, wer zum Sichern von Daten für einen Knoten berechtigt sein soll. Wird für BACKUPINITiation die Einstellung root verwendet, schränkt dies Sicherungen dahingehend ein, dass nur Rootbenutzer oder berechtigte Benutzer die Dateien auf einem Knoten sichern dürfen. Wird für BACKUPINITiation die Einstellung all verwendet, kann jeder beliebige Benutzer Daten auf einem Knoten sichern. Informationen zu diesen Befehlen und Optionen finden Sie in der Dokumentation zum IBM Spectrum Protect-Server.	Ja, wenn Sie über Lesezugriff verfügen, unabhängig vom Eigentumsrecht
Zurückschreibung	Ja; beim Zurückschreiben an eine neue Position oder an dieselbe Position werden Dateiberechtigung und Eigentumsrecht beibehalten	Ja; das Betriebssystem verhindert jedoch das Schreiben an dieselbe Position, wenn die Datei nur Lesezugriff hat. Beim Zurückschreiben an dieselbe Position werden Dateiberechtigungen und Eigentumsrecht beibehalten. Beim Zurückschreiben an eine andere Position werden die Berechtigungen der zurückgeschriebenen Datei beibehalten, das Eigentumsrecht geht jedoch auf den aktuellen Benutzer über.
Archivieren	Ja	Ja, wenn Sie über Lesezugriff verfügen, unabhängig vom Eigentumsrecht
Abruf	Ja. Beim Abrufen an eine neue Position oder an dieselbe Position werden Dateiberechtigungen und Eigentumsrecht beibehalten.	Ja. Das Betriebssystem verhindert jedoch das Schreiben an dieselbe Position, wenn die Datei nur Lesezugriff hat. Das Eigentumsrecht aller abgerufenen Objekte geht auf den aktuellen Benutzer über.

Tabelle 23. Tasks für Roots und berechtigte Benutzer (Forts.)

Task	Root	Berechtigter Benutzer
Client-Scheduler	Ja	Ja, wenn der Clientakzeptordämon nicht verwendet wird. Für die Verwaltung des Clientakzeptordämons müssen Sie Root sein. Ein berechtigter Benutzer ohne Rootberechtigung kann den Scheduler (dsmc sched) verwenden.
Benutzerzugriff auf Dateien auf dem IBM Spectrum Protect-Server erteilen	Ja	Ja
Dateibereiche auf dem IBM Spectrum Protect-Server löschen	Ja, wenn der IBM Spectrum Protect-Serveradministrator dem Knoten die Berechtigung zum Löschen von Sicherungen oder Archivierungen erteilt hat.	Ja, wenn der IBM Spectrum Protect-Serveradministrator dem Knoten die Berechtigung zum Löschen von Sicherungen oder Archivierungen erteilt hat.

Auf Mac OS X-Systemen ist ein Systemadministrator jeder Benutzer, der das System verwalten darf. Sie können Ihren Kontotyp mithilfe des Tools **Systemvorgaben** > **Accounts** überprüfen. Der Kontotyp von Systemadministratoren lautet **Admin**.

Es ist Aufgabe des Systemadministrators, den Client für Sichern/Archivieren so zu konfigurieren, dass Benutzer ohne Administratorberechtigung eigene Daten verwalten können. Benutzer ohne Administratorberechtigung (oder nicht berechtigte Benutzer) entsprechen den folgenden Kriterien:

- Sie haben nicht die Benutzer-ID 0 und sind nicht der Rootbenutzer.
- Sie haben ein Benutzerkonto, das nicht als Systemadministrator konfiguriert ist.

Wenn für die Ausführung einer Task zusätzliche Berechtigung erforderlich ist, müssen Sie zum Starten des Clients für Sichern/Archivieren die Berechtigungsanwendung verwenden. Dies ermöglicht die Ausführung des Clients mit ausreichenden Systemberechtigungen zur Ausführung der Task. In der folgenden Tabelle sind die zu verwendenden Berechtigungstools aufgelistet.

Tabelle 24. Mac OS X-Berechtigungstools und zugeordnete IBM Spectrum Protect-Anwendungen

Mac OS X-Berechtigungstool	Zugeordnete IBM Spectrum Protect-Anwendung
IBM Spectrum Protect For Administrators	IBM Spectrum Protect StartCad.sh StopCad.sh
sudo	dsmc

Benutzern ohne Rootberechtigung die Verwaltung eigener Daten ermöglichen

Damit Benutzer ohne Rootberechtigung eigene Daten mithilfe des Clients für Sichern/Archivieren verwalten können, muss der Systemadministrator zusätzlich zu den normalen Konfigurationsschritten weitere Schritte ausführen, mit denen berechtigte Erstbenutzer für Benutzer ohne Rootberechtigung konfiguriert werden.

Zusätzlich zu den normalen Konfigurationsschritten muss der Systemadministrator die folgenden Schritte ausführen, mit denen berechtigte Benutzer für Benutzer ohne Rootberechtigung konfiguriert werden:

1. Eine Zeilengruppe für den Benutzer ohne Rootberechtigung in der Clientsystemoptionsdatei, `dsm.sys`, hinzufügen.
2. In dieser Zeilengruppe mit der Option `passworddir` auf ein Verzeichnis zeigen, dessen Eigner der Benutzer ohne Rootberechtigung ist. Der Benutzer ohne Rootberechtigung kann dann eine Datei in diesem `passworddir`-Verzeichnis erstellen.
3. Dem Benutzer ohne Rootberechtigung einen eindeutigen TSM-Knotennamen zuordnen.
4. Sicherstellen, dass im `passworddir`-Verzeichnis keine vorherige Datei `TSM.PWD`, deren Eigner nicht der Benutzer ohne Rootberechtigung ist, vorhanden ist. Ist eine solche Datei vorhanden, das Eigentumsrecht dieser Datei dem Benutzer ohne Rootberechtigung übertragen oder die Datei entfernen.
5. Sicherstellen, dass im `passworddir`-Verzeichnis keine Datei `TSM.KDB`, `TSM.IDX` oder `TSM.sth`, deren Eigner nicht der Benutzer ohne Rootberechtigung ist, vorhanden ist. Sind diese Dateien vorhanden, müssen sie entfernt werden.

Nachdem der Systemadministrator diese Schritte ausgeführt hat, muss der Benutzer ohne Rootberechtigung die folgenden Schritte ausführen:

1. Eine Clientsystemoptionsdatei, `dsm.opt`, erstellen und mit der Option `servername` den Namen der Zeilengruppe angeben.
2. Sicherstellen, dass die Datei `dsm.opt` von der Umgebungsvariablen `DSM_CONFIG` standardmäßig gelesen werden kann. Eine Überprüfung kann durch Ausgabe des Befehls `export DSM_CONFIG=<dsm.opt>` in einem Shellbefehlsfenster erfolgen.
3. Den Befehl `dsmc q f` ausführen, um Kennwortdateien zu verwenden, auf die die Option `passworddir` zeigt. Sind keine Kennwortdateien vorhanden, erfolgt eine Benutzereingabeaufforderung.

Verschlüsselung für Benutzer des Clients für Sichern/Archivieren aktivieren

Wenn Sie in der Konfiguration des Clients für Sichern/Archivieren festlegen, dass Daten während Sicherungs- und Archivierungsoperationen verschlüsselt werden sollen, und wenn Sie die Option für die Speicherung des Kennworts für den Verschlüsselungsschlüssel (**encryptkey save**) angeben, können standardmäßig nur Rootbenutzer und berechtigte IBM Spectrum Protect-Benutzer das gespeicherte Kennwort zur Verschlüsselung oder Entschlüsselung von Dateien verwenden. Berechtigte Benutzer sind alle Benutzer ohne Rootberechtigung, die über Lese- und Schreibzugriff auf das gespeicherte Kennwort (Datei `TSM.sth`) verfügen, oder Benutzer, die das Kennwort kennen und interaktiv eingeben.

Übersicht über die Clientoptionsdatei

In einer Clientoptionsdatei können Sie Clientoptionen und Werte festlegen (angeben). Clientoptionen können auch auf dem Server in einer *Clientoptionsgruppe* definiert werden. In einer Clientoptionsgruppe auf dem Server festgelegte Clientoptionen setzen die in der Clientoptionsdatei definierten Clientoptionen außer Kraft.

Auf AIX-, Linux-, Mac- und Solaris-Systemen hat die Clientoptionsdatei standardmäßig den Namen `dsm.opt`. Bei diesen Betriebssystemen enthalten zwei Dateien Optionen für den Client für Sichern/Archivieren:

- Die *Clientbenutzeroptionsdatei*. Der Standardname für diese Datei lautet `dsm.opt`. Häufig wird diese Datei kurz auch als *Clientoptionsdatei* bezeichnet.
- Die *Clientsystemoptionsdatei*. Der Standardname für diese Datei lautet `dsm.sys`. Die *Clientsystemoptionsdatei* ist eine editierbare Datei, die den Server und die Übertragungsmethode festlegt und die Konfiguration für die Sicherung, Archivierung, hierarchische Speicherverwaltung und Zeitplanung bereitstellt. Häufig wird diese Datei kurz auch als *Systemoptionsdatei* bezeichnet.

Sie können mehrere Clientoptionsdateien erstellen. Falls Ihre Clientoptionsdatei nicht `dsm.opt` heißt oder die Datei `dsm.opt` nicht im Standardverzeichnis vorhanden ist, teilen Sie dem Client für Sichern/Archivieren mit der Clientoption `OPTFILE` mit, aus welcher Datei die Optionen und Parameter beim Starten des Clients für Sichern/Archivieren gelesen werden sollen.

Der Name der Clientsystemoptionsdatei kann nicht geändert werden. Er muss `dsm.sys` lauten.

Mit einer Texteditoranwendung können Sie die Clientoptionsdatei direkt editieren. Zum Festlegen von Optionen können Sie auch die GUI des Clients für Sichern/Archivieren verwenden. Wählen Sie in der GUI die Optionen **Editieren > Vorgaben** aus und legen Sie die Clientoptionen im Profileditor fest. Optionen, die Sie im Profileditor festlegen, werden in der Clientoptionsdatei gespeichert. Im Profileditor können allerdings nicht alle Clientoptionen festgelegt werden.

Einschränkung: Bei Mac OS X müssen die Clientbenutzeroptionsdatei und die Clientsystemoptionsdatei einfache, in Unicode (UTF-8) codierte Textdateien sein. Standardmäßig sichert TextEdit Dateien nicht als einfache Textdatei. Wählen Sie die Optionen **Format > Make Plain Text** aus, um die Dateien als einfache Textdateien zu speichern. Wählen Sie den Eintrag **Unicode (UTF-8)** in der Dropdown-Liste **Plain Text Encoding** aus. Fügen Sie beim Speichern der Datei nicht die Erweiterung `.txt` hinzu.

Sie können den Befehl **query options** verwenden, um alle oder einen Teil der Optionen und ihre aktuellen Einstellungen anzuzeigen. In diesem Befehl können Sie ein Argument eingeben, das eine Untergruppe von Optionen angibt. Standardmäßig werden alle Optionen angezeigt.

Einige Optionen bestehen nur aus dem Optionsnamen, z. B. `verbose` und `quiet`. Sie können den vollständigen Optionsnamen oder seine Abkürzung eingeben. Sie können beispielsweise die Option `verbose` wie folgt angeben:

```
verbose
ve
```

Richten Sie sich beim Hinzufügen von Optionen zu Optionsdateien nach den folgenden Regeln:

- Sie können Optionseinstellungen mit Anmerkungen versehen, indem Sie Kommentare zur Optionsdatei hinzufügen. Beginnen Sie jeden Kommentar mit einem Stern (*) als erstem Zeichen in der Zeile.
- Geben Sie Optionen nicht in einer Zeile an, die einen Kommentar enthält.
- Optional können Sie Optionen mit Leerzeichen oder Tabstopps einrücken, damit die in der Datei angegebenen Optionen und Werte besser zu erkennen sind.
- Geben Sie jede Option in einer separaten Zeile ein und geben Sie alle Parameter für eine Option in derselben Zeile ein. Dies ist in den folgenden Beispielen dargestellt:

```
domain /home /mfg /planning /mrktng /mgmtdomain / /Volumes/fs2 /Volumes/fs2 /Volumes/fs3 /V
```

- Um eine Option in dieser Datei zu definieren, geben Sie den Optionsnamen und eines oder mehrere Leerzeichen gefolgt vom Optionswert ein.
- Geben Sie eines oder mehrere Leerzeichen zwischen Parametern ein.
- Die Länge der Datei- und Pfadnamen in der Clientoptionsdatei darf die folgenden Grenzwerte nicht überschreiten:
 - Bei AIX, Mac OS und Solaris beträgt die maximale Länge für einen Dateinamen 255 Byte. Die maximale Länge der Kombination aus Dateiname und Pfadname ist 1024 Zeichen. Die Unicode-Darstellung eines Zeichens kann mehrere Byte in Anspruch nehmen, sodass die maximale Anzahl Zeichen, die ein Dateiname enthalten könnte, variieren kann.
 - Bei Linux beträgt die maximale Länge für einen Dateinamen 255 Byte. Die maximale Länge der Kombination aus Dateiname und Pfadname beträgt 4096 Byte. Dies entspricht dem vom Betriebssystem unterstützten Wert für **PATH_MAX**. Die Unicode-Darstellung eines Zeichens kann mehrere Byte in Anspruch nehmen, sodass die maximale Anzahl Zeichen, aus denen ein Pfad- und Dateiname besteht, variieren kann. Die Begrenzung ist die Anzahl Byte in den Pfad- und Dateikomponenten, die einer gleichen Anzahl Zeichen entsprechen kann, aber nicht muss.
 - Für Archivierungs- oder Abrufoperationen beträgt die maximale Länge, die Sie für eine Kombination aus Pfad- und Dateiname angeben können, 1024 Byte.

Wenn Sie die Clientbenutzeroptionsdatei aktualisieren, während eine Sitzung aktiv ist, müssen Sie die Sitzung erneut starten, damit die Änderungen in Kraft treten.

Zugehörige Verweise:

„Optfile“ auf Seite 523

„Query Options“ auf Seite 763

Clientsystemoptionsdatei erstellen und ändern

Die Clientsystemoptionsdatei ist eine editierbare Datei, die den Server und die Übertragungsmethode festlegt und die Konfiguration für die Sicherung, Archivierung, hierarchische Speicherverwaltung und Zeitplanung bereitstellt.

Informationen zu diesem Vorgang

Die Erstellung und Änderung der Clientsystemoptionsdatei (dsm.sys) ist eine erforderliche Task.

Die GUI des Clients für Sichern/Archivieren stellt einen Konfigurationsassistenten bereit, mit dem Sie Basiskonfigurationsdateien erstellen und die Verbindung zum IBM Spectrum Protect-Server testen können. Der Konfigurationsassistent wird automatisch gestartet, wenn die Konfigurationsdateien beim Starten der GUI nicht gefunden werden. Wenn Sie die Konfigurationsdateien zu einem Zeitpunkt nach der Erstellung ändern wollen, klicken Sie auf **Setup-Assistent** im Menü **Dienstprogramme** der GUI.

Wenn Sie den Konfigurationsassistenten nicht verwenden, können Sie die Clientoptionsdatei manuell erstellen und ändern.

Für Mac OS X: Kopieren Sie die Datei dsm.sys.smp an einer der folgenden Positionen in dsm.sys. Die Standardpositionen sind in der Reihenfolge aufgelistet, in der sie durchsucht werden.

1. Eine Position, die durch die Umgebungsvariable DSM_DIR angegeben wird

2. /Library/Application Support/tivoli/tsm/client/ba/bin/
3. /Library/Preferences/Tivoli Storage Manager/

Der Client verwendet die erste Optionsdatei, die gefunden wird. Sie müssen für diese Datei den Namen `dsm.sys` verwenden. Die Datei `dsm.sys` wird vom Systemadministrator gesteuert.

Bei Oracle Solaris-Systemen ist das Kopieren der Datei `dsm.sys.smp` in `dsm.sys` nicht erforderlich. Die Clientoptionsdateien (`dsm.opt` und `dsm.sys`) werden automatisch im Verzeichnis `/usr/bin` erstellt, wenn sie noch nicht vorhanden sind, und bei der Installation des Clients mit dem Clientinstallationsverzeichnis verbunden. Beachten Sie, dass die Dateien beim Deinstallieren des Clients nicht entfernt werden und Sie Ihre Einstellungen daher bei einem Upgrade oder einer Neuinstallation des Clients wiederverwenden können.

Kopieren Sie bei den anderen Plattformen die Datei `dsm.sys.smp` als Rootbenutzer in `dsm.sys` und editieren Sie anschließend diese Datei, um Ihre Einstellungen zu konfigurieren. Der Client sucht nach der Datei `dsm.sys` in dem Verzeichnis, das durch die Umgebungsvariable **DSM_DIR** angegeben wird (sofern festgelegt und exportiert). Anschließend wird im Installationsverzeichnis nach der Datei gesucht.

Wichtig: Wenn Sie eine erneute Installation ausführen und die vorhandene Datei `dsm.sys` unverändert beibehalten wollen, kopieren Sie die Datei `dsm.sys.smp` nicht in `dsm.sys`.

Verwenden Sie die Datei `dsm.sys`, um einen oder mehrere Server anzugeben, die für Services kontaktiert werden sollen, sowie um die Übertragungsoptionen für jeden Server anzugeben. Diese Datei kann außerdem Berechtigungsoptionen, Verarbeitungsoptionen für Sichern und Archivieren sowie Planungsoptionen enthalten.

Editieren Sie `dsm.sys` und fügen Sie den Server oder die Server hinzu, zu dem oder denen eine Verbindung hergestellt werden soll. Das folgende Beispiel zeigt eine Zeilengruppe einer Clientsystemoptionsdatei, die die erforderlichen Optionen für einen Server enthält, zu dem die Benutzer eine Verbindung herstellen sollen. Sie können Optionen für mehrere Server angeben:

Servename	server_a
COMMethod	TCPip
TCPPort	1500
TCPServeraddress	node.domain.company.com

Wichtig: Wenn Sie den Web-Client verwenden wollen, müssen Sie auch die Option `passwordaccess=generate` angeben und sich mit dem Client anmelden, um das Kennwort zu speichern.

Standardmäßig kontaktiert Ihr Clientknoten den ersten Server, der in der Datei `dsm.sys` angegeben ist. Sie können einen anderen Server angeben, zu dem eine Verbindung hergestellt werden soll, indem Sie die Option `servename` in Ihrer Clientbenutzeroptionsdatei (`dsm.opt`) angeben oder mit einem Befehl eingeben.

Sie können auch einen Standardserver und einen Umlagerungsserver (falls auf Ihrer Workstation der HSM-Client installiert ist) in Ihrer Datei `dsm.sys` angeben.

Die Datei `dsm.sys` kann außerdem die folgenden Optionskategorien enthalten:

- Optionen für die Datenübertragung
- Verarbeitungsoptionen für Sichern und Archivieren
- Verarbeitungsoptionen für Zurückschreiben und Abrufen

- Planungsoptionen
- Berechtigungsoptionen
- Fehlerverarbeitungsoptionen
- Transaktionsverarbeitungsoptionen
- Web-Client-Optionen

Sie können Ihre Datei `dsm.sys` über eine der folgenden Methoden ändern:

- Wählen Sie im Hauptfenster der Java-GUI des Clients die Optionen **Editieren** > **Clientvorgaben** aus.
- Verwenden Sie Ihren bevorzugten Texteditor.

Wichtig: Für Mac OS X: Die Systemoptionsdatei muss eine einfache in Unicode (UTF-8) codierte Textdatei sein. Standardmäßig sichert TextEdit Dateien nicht als unverschlüsselte Textdatei. Wählen Sie **Format** > **Make PlainText (Als einfachen Text speichern)** aus, um die Benutzeroptionsdatei als unverschlüsselte Textdatei zu speichern. Legen Sie für **Plain Text Encoding (Codierung für unverschlüsselten Text)** den Wert Unicode (UTF-8) fest. Fügen Sie nicht die Erweiterung `.txt` hinzu.

Wenn Sie die Datei `dsm.sys` aktualisieren, während der Client aktiv ist, müssen Sie den Prozess erneut starten, um die Änderungen in Kraft zu setzen.

Zugehörige Konzepte:

„Übersicht über die Clientoptionsdatei“ auf Seite 56

Kapitel 10, „Verarbeitungsoptionen“, auf Seite 323

Zugehörige Verweise:

„Defaultserver“ auf Seite 396

„Passwordaccess“ auf Seite 525

Standardclientbenutzeroptionsdatei erstellen

In einer Clientbenutzeroptionsdatei werden die Verarbeitungsoptionen des Clients für Sichern/Archivieren gespeichert. Bei der Installation des Clients für Sichern/Archivieren speichert das Installationsprogramm für die Sicherung/Archivierung ein Beispiel für die Clientbenutzeroptionsdatei auf der Platte. Ein Systemadministrator oder Root kann diese Datei editieren, um eine Standardclientoptionsdatei zu erstellen, und die Datei den Workstationbenutzern zugänglich machen, die den Client für Sichern/Archivieren verwenden. Einzelne Benutzer können eigene Clientoptionsdateien erstellen und verwenden.

Vorbereitende Schritte

Sie müssen ein Root oder ein Systemadministrator sein, um diese Prozedur ausführen zu können.

Informationen zu diesem Vorgang

Die Erstellung einer Standardclientbenutzeroptionsdatei ist eine optionale Task.

Die Clientbenutzeroptionsdatei heißt standardmäßig `dsm.opt` und enthält die folgenden Typen von Clientoptionen:

- Verarbeitungsoptionen für Sichern und Archivieren
- Verarbeitungsoptionen für Zurückschreiben und Abrufen
- Planungsoptionen
- Formatoptionen
- Befehlsverarbeitungsoptionen
- Berechtigungsoptionen

- Fehlerverarbeitungsoptionen
- Transaktionsverarbeitungsoptionen
- Web-Client-Optionen

Bei Mac-Clients speichert das Clientinstallationsprogramm ein Beispiel für die Clientbenutzeroptionsdatei namens `dsm.opt.smp` an der Position `/Libraries/Preferences/Tivoli Storage Manager/`. In diesem Verzeichnis speichert das Installationsprogramm auch ein Beispiel für die Clientsystemoptionsdatei (`dsm.sys.smp`).

Bei AIX- und Linux-Clients speichert das Clientinstallationsprogramm ein Beispiel für die Clientbenutzeroptionsdatei mit dem Namen `dsm.opt.smp` im standardmäßigen Clientinstallationsverzeichnis. In diesem Verzeichnis speichert das Installationsprogramm auch ein Beispiel für die Clientsystemoptionsdatei (`dsm.sys.smp`).

Bei Oracle Solaris-Clients speichert das Installationsprogramm eine anfängliche Clientbenutzeroptionsdatei namens `dsm.opt` im Verzeichnis `/usr/bin`. In diesem Verzeichnis speichert das Installationsprogramm auch ein Beispiel für die Clientsystemoptionsdatei (`dsm.sys`).

Bei allen Clientbetriebssystemen werden Sie in der folgenden Prozedur angewiesen, das Beispiel für die Clientbenutzeroptionsdatei zu editieren und unter dem Standardnamen `dsm.opt` zu speichern. Sie können die Datei auf Wunsch auch unter einem anderen Namen oder Pfad speichern. Falls Sie jedoch den Dateinamen ändern oder die Datei aus dem Standardinstallationsverzeichnis versetzen, müssen Sie den Pfad und den Namen der Clientbenutzeroptionsdatei mit einem der folgenden Verfahren angeben:

- Legen Sie die Umgebungsvariable `DSM_CONFIG` so fest, dass sie den Pfad und Dateinamen der Clientbenutzeroptionsdatei (`dsm.opt`) angibt. Legen Sie die Umgebungsvariable `DSM_DIR` so fest, dass sie den Pfad und Dateinamen der Clientsystemoptionsdatei (`dsm.sys`) angibt. Weitere Informationen zu den Umgebungsvariablen finden Sie in „Umgebungsvariablen für die Verarbeitung definieren“ auf Seite 64.
- Geben Sie mit der Option `optfile` des Clients für Sichern/Archivieren den Pfad und Dateinamen der Clientbenutzeroptionsdatei an.

Anmerkung: Alle Knotenbenutzer müssen Lesezugriff auf die Plattenposition besitzen, an der Sie die Clientbenutzeroptionsdatei speichern.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis, in dem sich das Beispiel für die Clientbenutzeroptionsdatei befindet.
2. Kopieren Sie die Datei nach `dsm.opt`.
3. Fügen Sie Optionen für Ihren Knoten zur Datei `dsm.opt` hinzu. Verwenden Sie zum Festlegen der Clientbenutzeroptionen eines der folgenden Verfahren:
 - Editieren Sie die Datei `dsm.opt` in einem Texteditor und fügen Sie die für den Knoten benötigten Optionen zur Datei hinzu.

Anmerkung: Unter Mac OS X muss die Datei `dsm.opt` als einfache Textdatei gespeichert und Unicode (UTF-8) als Schema für die Codeumsetzung verwendet werden. Standardmäßig sichert TextEdit Dateien nicht als einfache Textdatei. Um die Datei `dsm.opt` in TextEdit zu speichern, wählen Sie die Optionen **Format > Make Plain Text** aus. Wählen Sie in der Dropdown-Liste **Plain Text Encoding** den Eintrag **Unicode (UTF-8)** aus. Fügen Sie nicht die Erweiterung `.txt` zum Dateinamen hinzu.

- Legen Sie Clientoptionen mit dem Profileditor fest. Wählen Sie in der grafischen Benutzerschnittstelle (GUI) des Clients für Sichern/Archivieren die Optionen **Editieren** > **Clientvorgaben** und dann die Optionen aus, die Sie konfigurieren wollen. Der Profileditor aktualisiert die Clientkonfigurationsdateien dsm.opt und dsm.sys, falls Sie Optionen hinzufügen, ändern oder entfernen. Wenn Sie die Datei dsm.opt aktualisieren, während der Client für Sichern/Archivieren ausgeführt wird, müssen Sie den Client für Sichern/Archivieren erneut starten, damit die Aktualisierungen erkannt werden.

Der Profileditor ermittelt anhand der Umgebungsvariablen DSM_DIR die Clientsystemoptionsdatei (dsm.sys) sowie anhand der Umgebungsvariablen DSM_CONFIG die Clientbenutzeroptionsdatei (dsm.opt). Falls sich die Datei dsm.opt an einer anderen als der Standardposition befinden soll, legen Sie die Umgebungsvariable DSM_CONFIG fest, bevor Sie den Client für Sichern/Archivieren starten, und verwenden Sie anschließend den Profileditor, um die Optionen festzulegen. Der Profileditor fragt den Server nach Optionen auf dem Server ab, kann aber die Serveroptionsdatei nicht ändern.

Zugehörige Konzepte:

Kapitel 10, „Verarbeitungsoptionen“, auf Seite 323

„Umgebungsvariablen für die Verarbeitung definieren“ auf Seite 64

Zugehörige Tasks:

„Clientsystemoptionsdatei erstellen und ändern“ auf Seite 58

Angepasste Clientbenutzeroptionsdatei erstellen

Wenn Sie andere Optionen als die in der Standardclientbenutzeroptionsdatei (dsm.opt) angegebenen Optionen verwenden wollen, können Sie eine eigene Clientbenutzeroptionsdatei erstellen.

Informationen zu diesem Vorgang

Sie können alle Optionen definieren, die in der Standardbenutzeroptionsdatei angegeben werden können. Die Erstellung einer angepassten Clientbenutzeroptionsdatei (dsm.opt) ist eine optionale Task. Verwenden Sie die folgende Methode, um eine Clientbenutzeroptionsdatei zu erstellen oder zu ändern:

Vorgehensweise

1. Fragen Sie den IBM Spectrum Protect-Administrator für Ihre Workstation nach der Position der Muster-Clientbenutzeroptionsdatei dsm.opt.smp, nach der TCP/IP-Adresse des Sicherungsservers, zu dem Sie eine Verbindung herstellen, und nach dem Anschluss, an dem er empfangsbereit ist.
2. Kopieren Sie dsm.opt.smp in Ihr Ausgangsverzeichnis als dsm.opt oder mit einem neuen Dateinamen Ihrer Wahl. Sie können Ihre Clientbenutzeroptionsdatei in jedem Verzeichnis speichern, auf das Sie Schreibzugriff haben.
3. Definieren Sie die Umgebungsvariable DSM_CONFIG so, dass sie auf Ihre neue Clientbenutzeroptionsdatei zeigt.
4. Editieren Sie die Datei dsm.opt gemäß Ihrem System oder verwenden Sie den Profileditor, indem Sie **Editieren** > **Clientvorgaben** in der GUI des Clients für Sichern/Archivieren auswählen.

Ergebnisse

Nachdem Sie eine Optionsdatei erstellt haben, können Sie sie mit den folgenden Schritten über die grafische Benutzerschnittstelle editieren:

1. Öffnen Sie das Menü **Editieren** und wählen Sie **Clientvorgaben** aus.

2. Nehmen Sie die erforderlichen Änderungen vor und klicken Sie anschließend auf **OK**, um diese Änderungen zu speichern.

Wichtig: Für Mac OS X: Die Systemoptionsdatei muss eine einfache in Unicode (UTF-8) codierte Textdatei sein. Standardmäßig sichert TextEdit Dateien nicht als unverschlüsselte Textdatei. Wählen Sie **Format > Make PlainText (Als einfachen Text speichern)** aus, um die Benutzeroptionsdatei als unverschlüsselte Textdatei zu speichern. Legen Sie die Auswahl in der Dropdown-Liste **Plain Text Encoding (Codierung für unverschlüsselten Text)** mit Unicode (UTF-8) fest. Fügen Sie nicht die Erweiterung .txt hinzu.

Zugehörige Konzepte:

„Umgebungsvariablen“

„Übersicht über die Clientoptionsdatei“ auf Seite 56

Umgebungsvariablen

Im Allgemeinen ist die Definition von Umgebungsvariablen eine optionale Task. Wenn Sie diese Variablen definieren, erleichtert dies die Verwendung der Befehlszeile.

Sprachumgebungsvariablen definieren

Der Client für Sichern/Archivieren erkennt automatisch die Sprache der Systemländereinstellung und wird dieser Sprache angezeigt.

Beispielsweise zeigt ein französisches Betriebssystem den Client für Sichern/Archivieren standardmäßig in Französisch an. Wenn der Client für Sichern/Archivieren den französischen Nachrichtenkatalog nicht laden kann, wird standardmäßig amerikanisches Englisch verwendet. Wenn der Client beispielsweise mit einer nicht unterstützten Kombination aus Sprache und Ländereinstellung wie Französisch/Kanada oder Spanisch/Mexiko ausgeführt wird, wird für den Client standardmäßig amerikanisches Englisch angenommen.

Sie können die Umgebungsvariable **LANG** verwenden, um die Sprache für die UNIX- und Linux-Clients anzugeben.

Anmerkung: Die Ländereinstellung des Betriebssystems, der Zeichensatz der Datenstation und die Zeichensatzcodierung für Dateinamen müssen übereinstimmen, damit Dateinamen ordnungsgemäß angezeigt oder eingegeben werden können.

Soll die Umgebungsvariable **LANG** für Französisch definiert werden, geben Sie die folgende Anweisung ein:

```
export LANG=fr_FR
```

Anmerkung:

- Diese Task gilt nicht für Mac OS X.
- Wenn die IBM Spectrum Protect-Hilfemenüs in der Sprache der aktuellen Ländereinstellung angezeigt werden sollen, muss sichergestellt werden, dass in der Umgebungsvariablen NLSPATH in der Datei /etc/profile folgende Pfadangabe enthalten ist:

```
NLSPATH=/usr/dt/lib/nls/msg/%L/%N.cat:$NLSPATH
export NLSPATH
```

Wenn die Ländereinstellung des Clients für Sichern/Archivieren mit der Zeichencodierung der Dateinamen übereinstimmt, werden alle diese Dateien korrekt gesi-

chert oder zurückgeschrieben. Wenn Sie mit einem beliebigen Einzelbytezeichensatz (SBCS) arbeiten, sind alle Dateinamen gültig und werden vom Client für Sichern/Archivieren gesichert oder zurückgeschrieben.

Wenn Sie mit einer DBCS- oder UTF-8-Ländereinstellung arbeiten, können Dateinamen mit Zeichen, die in der DBCS- oder UTF-8-Ländereinstellung nicht gültig sind, nicht in der Befehlszeile des Clients für Sichern/Archivieren eingegeben werden. Die Dateien werden möglicherweise übersprungen, wenn Sie eine Sicherung mit Platzhalterzeichen ("*") für Dateinamenspezifikationen ausführen. Werden Dateien übersprungen, wird eine Fehlermeldung wie im folgenden Beispiel ausgegeben:

```
ANS4042E Objektname '/testData/en_US_files/file3?'  
enthält ein oder mehrere unbekannte Zeichen und ist nicht gültig.
```

Wurden Ihre Verzeichnisse und Dateien mit verschiedenen Ländereinstellungen erstellt, führen Sie geplante Sicherungen mit einer Ländereinstellung für Einzelbytezeichensatz aus. Damit ist sichergestellt, dass Dateien nicht übersprungen werden, weil der Dateiname Zeichen enthält, die nicht in der aktuellen Ländereinstellung definiert sind. Die Zurückschreibung von Dateien führen Sie in der Ländereinstellung durch, die der Codierung der Dateinamen entspricht.

Beispiel: Aus japanischen Zeichen bestehende Dateinamen enthalten möglicherweise ungültige Mehrbytezeichen, wenn sie in einer chinesischen Ländereinstellung angezeigt werden. Diese Dateien werden weder gesichert noch in der grafischen Benutzerschnittstelle angezeigt. Werden solche Dateien während der Sicherung festgestellt, werden die übersprungenen Dateien in der Datei `dsmerror.log` aufgelistet.

Tipp: Wenn Sie den Planungsmodus des Clients für Sichern/Archivieren für die Sicherung eines gesamten Systems verwenden, setzen Sie die Umgebungsvariable **LANG** auf `en_US` (oder eine andere SBCS-Sprache), um übersprungene Dateien zu vermeiden.

Umgebungsvariablen für die Verarbeitung definieren

Unter bestimmten Umständen ist es erforderlich, Umgebungsvariablen zu definieren, um sicherzustellen, dass IBM Spectrum Protect-Anwendungen die Dateien finden können, die für die Ausführung von Clientoperationen benötigt werden, und dass Anwendungen Protokolldateien erstellen können, in denen Ereignisse und Fehler aufgezeichnet werden, die während Clientoperationen auftreten.

Sie müssen die Umgebungsvariablen in jeder der folgenden Situationen definieren:

- Der Client für Sichern/Archivieren soll von einem anderen Verzeichnis als dem Installationsverzeichnis des Clients für Sichern/Archivieren aufgerufen werden.
- Es soll eine andere Optionsdatei für den Client für Sichern/Archivieren und/oder den Verwaltungsclient angegeben werden.
- Protokolldateien sollen nicht im Standardinstallationsverzeichnis gespeichert werden.

Tipp: Sie können auch eine andere Clientoptionsdatei für den Befehlszeilenclient (nicht den Verwaltungsclient) angeben, wenn Sie die Option `optfile` verwenden.

Es können vier Umgebungsvariablen definiert werden, die sich auf die Verarbeitung durch den Client für Sichern/Archivieren auswirken:

PATH Schließt das Verzeichnis ein, in dem sich die ausführbare Datei für die ausführbaren Dateien des Clients (`dsmc`, `dsmadm`, `dsmj`) befindet.

DSM_DIR

Gibt das Verzeichnis an, in dem sich die ausführbare Datei für die ausführbaren Dateien des Clients (dsmc, dsmadm, dsmj), die Ressourcendateien und die Datei dsm.sys befinden. Das Stammverzeichnis (/) kann für DSM_DIR nicht angegeben werden.

Informationen zum Standardinstallationsverzeichnis finden Sie im Installationsabschnitt für Ihr Betriebssystem.

Wenn Sie eine Imagesicherung, eine Imagezurückschreibung, eine momentaufnahmebasierte Dateisicherung, eine NAS-Sicherung oder eine NAS-Zurückschreibung anfordern, lokalisiert der Client die entsprechende Plug-In-Bibliothek mithilfe der Umgebungsvariablen DSM_DIR. Wenn für DSM_DIR kein Wert festgelegt wurde, sucht der Client in folgenden Verzeichnissen nach den Plug-in-Bibliotheken:

AIX /usr/tivoli/tsm/client/ba/bin/plugins

Oracle Solaris- und alle Linux-Clients

/opt/tivoli/tsm/client/ba/bin/plugins

DSM_CONFIG

Gibt den vollständig qualifizierten Pfad und Dateinamen der Clientbenutzeroptionsdatei für Benutzer an, die ihre persönliche Optionsdatei erstellen. Ist DSM_CONFIG nicht definiert oder wird die Clientoption optfile nicht verwendet, muss die Clientbenutzeroptionsdatei die folgenden Anforderungen erfüllen:

1. Die Optionsdatei muss den Namen dsm.opt haben.
2. Für andere UNIX-Clients als Mac OS X: Ist DSM_DIR *nicht* definiert, muss die Datei sich im Standardinstallationsverzeichnis befinden. Ist DSM_DIR *definiert*, muss die Datei sich in dem Verzeichnis befinden, das von DSM_DIR angegeben ist.
3. Für Mac OS X: Die Datei kann sich an einer der folgenden Positionen befinden. Diese Verzeichnisse werden in der angegebenen Reihenfolge durchsucht und die erste gefundene Optionsdatei wird verwendet.
~/Library Preferences/Tivoli Storage Manager, /Library Preferences/Tivoli Storage Manager oder /Library/Application Support/tivoli/tsm/client/ba/bin.

Informationen zum Standardinstallationsverzeichnis finden Sie im Installationsabschnitt für Ihr Betriebssystem.

DSM_LOG

Verweist auf das Verzeichnis, in dem die IBM Spectrum Protect-Protokoll-dateien gespeichert werden sollen. Das Stammverzeichnis (/) kann für DSM_LOG nicht angegeben werden. Die Protokolldateien enthalten Informationen zu Fehlern und Ereignissen, die während der Verarbeitung auftreten. Der Client erstellt die Protokolle, um den Mitarbeitern der technischen Unterstützung die Diagnose schwerwiegender Fehler zu erleichtern.

Informationen zum Standardinstallationsverzeichnis finden Sie im Installationsabschnitt für Ihr Betriebssystem.

Wichtig: Geben Sie für die Umgebungsvariable DSM_LOG ein Verzeichnis an, in dem die Schreib-/Leseberechtigungen dem Benutzer den erforderlichen Schreibzugriff ermöglichen, um die Protokolldatei erstellen und Daten in sie schreiben zu können. Dadurch werden Fehler beim Schreiben in das Protokoll und Prozessbeendigungen verhindert. Erteilen Sie mit den Befehlen **chmod** oder **setacl** die Berechtigungen für die Dateien, die allen Clientbenutzer-IDs das Lesen der Dateien und das Schreiben in die Dateien ge-

statten. Wenn die Protokollnamen die Standardnamen sind, setzen Sie einfach die Umgebungsvariable `DSM_LOG`, sodass sie auf das Verzeichnis zeigt, in dem sich die Protokolle befinden. Wenn der Client keine Daten in die Protokolldatei schreiben kann, wird eine Fehlnachricht in `stderr` und in den `syslog`-Dämon geschrieben. Der `syslog`-Dämon muss aktiv und so konfiguriert sein, dass Nachrichten mit der Priorität `LOG_ERR` verarbeitet werden, damit die Fehlnachricht im Systemprotokoll angezeigt wird. Das Starten und Konfigurieren des `syslog`-Dämons erfolgt systemspezifisch. Mit dem Befehl **man syslogd** können Sie Informationen zum Starten des `syslog`-Dämons abrufen. Verwenden Sie **man syslog.conf**, um Informationen zum Konfigurieren des `syslog`-Dämons abzurufen.

Anmerkung:

1. Die Optionen `errorlogname` und `schedlogname` überschreiben `DSM_LOG`. Wenn Sie die Clientoption `errorlogname` angeben, wird die Datei nicht an der durch `DSM_LOG` angegebenen Position, sondern in dem durch die Option `errorlogname` angegebenen Verzeichnis gespeichert. Wenn Sie die Clientoption `schedlogname` angeben, wird sie nicht an die durch `DSM_LOG` angegebene Position, sondern in das durch die Option `schedlogname` angegebene Verzeichnis geschrieben.
2. Die Protokolldateien dürfen keine symbolischen Verbindungen sein. Der Client erkennt derartige Verbindungen, löscht die Verbindungen und beendet die Operation. Mit dieser Aktion wird verhindert, dass der Client geschützte Daten überschreibt. Die betroffenen Protokolle werden in einer nachfolgenden Operation als Dateien erstellt.

Damit die Java-GUI des Clients für Sichern/Archivieren verwendet werden kann, müssen Sie das Verzeichnis, in dem die Java-Binärdatei installiert ist, exportieren. Geben Sie z. B. den folgenden Befehl ein:

```
export PATH=$PATH:Verzeichnis_für_Java-Binärdatei
```

Dabei ist *Verzeichnis_für_Java-Binärdatei* der Pfad zu der ausführbaren Java-Binärdatei in Ihrem Dateisystem.

Zugehörige Verweise:

„Optfile“ auf Seite 523

Bourne- und Korn-Shell-Variablen definieren

Geben Sie die Umgebungsvariablen in die Datei `.profile` (Korn-Shell) oder in die Datei `.bash_profile` (Bourne-Shell) im Verzeichnis `$HOME` ein.

Im folgenden Beispiel ist `/home/davehil/dsm.opt` der Pfad und Dateiname für Ihre Clientbenutzeroptionsdatei und `/home/davehil` ist das Verzeichnis, in dem Sie die Datei `dsmerror.log`, die ausführbaren Dateien, die Ressourcendateien und die Datei `dsm.sys` speichern wollen.

```
DSM_DIR=/home/davehil
DSM_CONFIG=/home/davehil/dsm.opt
DSM_LOG=/home/davehil
export DSM_DIR DSM_CONFIG DSM_LOG
```

C-Shell-Variablen definieren

Für die C-Shell fügen Sie die Variablen `DSM_CONFIG`, `DSM_LOG` und `DSM_DIR` der Datei `.cshrc` im Verzeichnis `$HOME` hinzu.

Im folgenden Beispiel ist /home/davehil/dsm.opt der Pfad und Dateiname für Ihre Clientbenutzeroptionsdatei und /home/davehil ist das Verzeichnis, in dem Sie die Datei dsmerror.log, die ausführbaren Dateien, die Ressourcendateien und die Datei dsm.sys speichern wollen.

```
setenv DSM_DIR /home/davehil
setenv DSM_CONFIG /home/davehil/dsm.opt
setenv DSM_LOG /home/davehil
```

API-Umgebungsvariablen definieren

Wenn Sie die IBM Spectrum Protect-API installiert haben, definieren Sie die folgenden Umgebungsvariablen.

DSMI_DIR

Zeigt auf das Installationsverzeichnis. Die Datei dsm.sys muss sich in dem Verzeichnis befinden, auf das DSMI_DIR zeigt. Diese Umgebungsvariable muss vorhanden sein.

DSMI_CONFIG

Vollständiger Pfadname Ihrer eigenen Clientbenutzeroptionsdatei (dsm.opt).

DSMI_LOG

Pfad für dsierror.log (dieser Pfad kann keine symbolische Verbindung sein).

Anmerkung: Endbenutzer von Anwendungen, die mit der API entwickelt wurden, können anhand der Installationsanweisungen für diese Anwendung feststellen, ob bestimmte Pfadnamen oder Richtlinien für Optionen einzuhalten sind.

Weitere Informationen zur IBM Spectrum Protect-API finden Sie in Anwendungsprogrammierschnittstelle.

Übersicht über die Konfiguration des Web-Clients

Der IBM Spectrum Protect-Web-Client stellt die Fernverwaltung eines Clientknotens über einen Web-Browser zur Verfügung. Die Prozeduren für die Konfiguration des Web-Clients variieren abhängig davon, welches Betriebssystem auf dem Clientknoten verwendet wird.

Ab IBM Spectrum Protect Version 8.1.2 können Sie nicht mehr die Web-Client-GUI verwenden, um eine Verbindung zum IBM Spectrum Protect-Server der Version 8.1.2 oder höher herzustellen. Weitere Informationen enthält der Abschnitt „Web-Client in der neuen Sicherheitsumgebung verwenden“ auf Seite 158.

Zum Konfigurieren der Web-Client-Einstellungen werden Optionen des Clients für Sichern/Archivieren verwendet. Hierzu gehören die Optionen httpport, managed-services, webports und revokeRemoteAccess.

Auf AIX-, Linux-, Mac- und Solaris-Clientknoten fügen Sie die Web-Client-Optionen zur Clientsystemoptionsdatei (dsm.sys) hinzu.

Um den Web-Client über die Schnittstelle des IBM Spectrum Protect Operations Center zu verwenden, geben Sie die Web-Client-Adresse im Parameter URL des Befehls **REGISTER NODE** oder **UPDATE NODE** an. Die Webadresse muss den DNS-Namen oder die IP-Adresse des Knotens sowie die Anschlussnummer enthalten, die der Web-Client verwendet. Beispiel: http://node.example.com:1581. Ersetzen Sie in diesem Beispiel den Hostnamen durch die IP-Adresse oder den Hostna-

men Ihres Clientknotens. Wenn Sie mithilfe eines Web-Browsers auf den Web-Client zugreifen, geben Sie dieselbe Syntax in der Adressleiste des Browsers ein.

Alle Web-Client-Nachrichten werden in die Protokolldatei des Web-Clients geschrieben. Diese Datei heißt `dsmwebcl.log`. Die Datei `dsmwebcl.log` und die Fehlerprotokolldatei des Clients für Sichern/Archivieren (`dsmerror.log`) werden standardmäßig im Clientinstallationsverzeichnis erstellt. Mit der Umgebungsvariablen `DSM_LOG` können Sie die Standardpositionen für die Fehlerprotokolle überschreiben. Falls Sie die Umgebungsvariable `DSM_LOG` festlegen, geben Sie als Position für die Fehlerprotokolle nicht das Stammverzeichnis an. Die Position der Fehlerprotokolldateien können Sie auch mit der Option `errorlogname` des Clients für Sichern/Archivieren ändern. Falls Sie diese Option angeben, setzt sie die Einstellung der Umgebungsvariablen `DSM_LOG` außer Kraft.

Zugehörige Konzepte:

„Web-Client-Optionen“ auf Seite 345

Zugehörige Tasks:

„Web-Client auf AIX-, Linux-, Mac- und Solaris-Systemen konfigurieren“

Web-Client auf AIX-, Linux-, Mac- und Solaris-Systemen konfigurieren

Zur Konfiguration des Web-Clients müssen Sie die Clientsystemoptionsdatei (`dsm.sys`) editieren und die erforderlichen Optionen angeben. Anschließend starten Sie den Clientakzeptordämon.

Vorgehensweise

1. Legen Sie die folgenden Optionen in der Datei `dsm.sys` fest: `managedservices webclient schedule` und `passwordaccess generate`.
2. Generieren Sie das IBM Spectrum Protect-Kennwort. Geben Sie `dsmc query session` ein. Sobald die Berechtigungsnachweise von Ihnen angefordert werden, geben Sie den Benutzernamen und das Kennwort für IBM Spectrum Protect ein.

Auf Mac OS X-Systemen können Sie zum Generieren des Kennworts auch die Anwendung 'IBM Spectrum Protect-Tools für Administratoren' verwenden. Wählen Sie in der Anwendung **IBM Spectrum Protect** aus, um den Client zu starten.

3. Starten Sie den Clientakzeptordämon. Geben Sie `dsmcad` ein.

Unter Mac OS X können Sie zum Starten des Clientakzeptordämons auch die Anwendung 'IBM Spectrum Protect-Tools für Administratoren' verwenden. Wählen Sie in der Anwendung die Option zum Starten des Clientakzeptordämons aus.

4. Um aus einem Browser auf den Web-Client zuzugreifen, geben Sie in der Adressleiste des Browsers den Hostnamen oder die IP-Adresse des Clientknotens gefolgt von der Anschlussnummer des Web-Clients an. Die Standardanschlussnummer ist 1581. Um beispielsweise auf den Web-Client auf dem Knoten namens `myserver.example.com` zuzugreifen, geben Sie `http://myserver.example.com:1581` an.

Falls Sie die Standardanschlussnummer des Web-Clients ändern müssen, verwenden Sie die Option `httpport` des Clients für Sichern/Archivieren, um eine andere Anschlussnummer zuzuordnen.

Nächste Schritte

Nachdem Sie den Web-Client konfiguriert haben, können Sie Daten auf einem Knoten mit dem IBM Spectrum Protect Operations Center oder einem Browser sichern oder zurückschreiben bzw. archivieren oder abrufen.

Zugehörige Konzepte:

„Planungsoptionen“ auf Seite 340

„Web-Client-Optionen“ auf Seite 345

Zugehörige Tasks:

„Web-Client-Sitzung starten“ auf Seite 158

Zugehörige Verweise:

„Httpport“ auf Seite 465

„Passwordaccess“ auf Seite 525

Scheduler konfigurieren

Ihr IBM Spectrum Protect-Administrator kann den Client für die automatische Ausführung von Tasks konfigurieren. Damit geplante Ereignisse auf dem Client stattfinden können, müssen Sie den Client-Scheduler für die Kommunikation mit dem IBM Spectrum Protect-Server konfigurieren.

Informationen zu diesem Vorgang

So können Sie beispielsweise Dateien jeden Abend automatisch sichern oder einige Dateien jeden Freitag archivieren. Bei dieser Prozedur, die als zentrale Zeitplanung bezeichnet wird, arbeiten der Server und Ihr Clientknoten zusammen. Der Administrator ordnet Clients einem oder mehreren Zeitplänen zu, die zu der Maßnahmendomäne gehören, die in der Serverdatenbank verwaltet wird. Der IBM Spectrum Protect-Administrator definiert die zentrale Zeitplanung auf dem Server und Sie starten den Client-Scheduler auf Ihrer Workstation. Nach dem Starten des Client-Schedulers ist kein weiterer Eingriff erforderlich.

Mithilfe der Clientzeitplanung können Sie folgende Tasks ausführen:

- Informationen zu verfügbaren Zeitplänen anzeigen.
- Informationen zu geplanter Arbeit, die beendet ist, anzeigen.
- Planungsoptionen in der Datei `dsm.sys` ändern.

Die effektivste Möglichkeit zur Verwaltung des Client-Schedulers besteht in der Verwendung des Clientakzeptorservice. Sie können Informationen zu einem Vergleich zwischen der Verwendung des Clientakzeptors und traditioneller Scheduler-Services für die Verwaltung des Schedulers lesen. Außerdem erfahren Sie, wie der Client für die Verwaltung des Schedulers durch den Clientakzeptor konfiguriert wird.

Vergleich zwischen vom Clientakzeptor verwalteten Services und traditionellen Scheduler-Services

Sie können den IBM Spectrum Protect-Scheduler mit dem Clientakzeptorservice oder mit dem traditionellen Scheduler-Service verwalten. Dieser Abschnitt enthält einen Vergleich dieser Methoden.

Die folgende Tabelle zeigt die Unterschiede zwischen den vom Clientakzeptor verwalteten Services und den standardmäßigen traditionellen Scheduler-Services.

Tabelle 25. Vergleich zwischen vom Clientakzeptor verwalteten Services und traditionellen Scheduler-Services

Vom Clientakzeptor verwaltete Services	Traditionelle IBM Spectrum Protect-Scheduler-Services
Werden mithilfe der Option <code>managedservices schedule</code> definiert und mit Clientakzeptorservices gestartet. Der Clientakzeptordämon wird mit dem Befehl dsmcad gestartet.	Werden mit dem Befehl dsmc sched gestartet.
Der Clientakzeptorservice startet und stoppt den Schedulerprozess für jede geplante Aktion nach Bedarf.	Bleiben aktiv, selbst wenn die geplante Sicherung beendet ist.
Erfordern weniger Systemressourcen bei Inaktivität.	Erfordern einen höheren Verbrauch an Systemressourcen bei Inaktivität.
Clientoptionen und Überschreibungsoptionen auf dem IBM Spectrum Protect-Server werden jedes Mal aktualisiert, wenn die Clientakzeptorservices eine geplante Sicherung starten.	Clientoptionen und Überschreibungsoptionen auf dem IBM Spectrum Protect-Server werden erst nach dem Start von dsmc sched verarbeitet.
Können nicht bei Sicherungen mit <code>SESSIONINITIATION=SERVEROnly</code> verwendet werden.	Sie müssen den Schedulerprozess erneut starten, damit aktualisierte Clientoptionen wirksam werden. Wichtig: Wenn Sie den Client-Scheduler über die Befehlszeile ausführen, wird der Scheduler nicht als Hintergrundservice ausgeführt. Tipp: Starten Sie den traditionellen Scheduler regelmäßig, um Systemressourcen freizugeben, die zuvor von Systemaufrufen verwendet wurden.

Client für die Verwaltung des Schedulers durch den Clientakzeptorservice konfigurieren

Eine der effektivsten Möglichkeiten zur Verwaltung des Client-Schedulers besteht in der Verwendung des Clientakzeptorservice. Sie müssen den Client für die Verwaltung des Schedulers durch den Clientakzeptor konfigurieren.

Vorbereitende Schritte

- Wenn Sie Dateien für die Verschlüsselung einschließen, stellen Sie sicher, dass die Option **encryptkey** in der Optionsdatei auf `save` gesetzt ist. Diese Option wird durch Auswahl von **Kennwort für Verschlüsselungsschlüssel lokal speichern** auf der Registerkarte **Berechtigung** des Profileditors definiert. Wenn diese Option definiert ist, können unbeaufsichtigte geplante Services ausgeführt werden. Wenn der Verschlüsselungsschlüssel noch nicht gespeichert wurde, müssen Sie eine überwachte Sicherung von mindestens einer Datei ausführen, damit die Eingabeaufforderung für die Verschlüsselung angezeigt wird und Sie den Schlüssel speichern können.
- Sie können den Clientakzeptor nicht für die Planung verwenden, wenn die Option **sessioninitiation** auf `serveronly` gesetzt ist.

Informationen zu diesem Vorgang

Der Clientakzeptor dient als externer Zeitgeber für den Scheduler. Wenn der Scheduler gestartet wird, fragt er den Server nach dem nächsten geplanten Ereignis. Das Ereignis wird entweder sofort ausgeführt oder der Scheduler wird beendet. Der Clientakzeptor startet den Scheduler erneut, wenn der Zeitpunkt für die Ausführung des geplanten Ereignisses erreicht wird. Mit dieser Aktion wird die Anzahl Hintergrundprozesse auf Ihrer Workstation reduziert und Probleme in Bezug auf die Speicheraufbewahrungsdauer, die auftreten können, wenn der Scheduler ohne Verwaltung durch den Clientakzeptor ausgeführt wird, werden vermieden.

Der Clientakzeptorservice wird als auch Clientakzeptordämon (CAD) bezeichnet.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um den Clientakzeptor für die Verwaltung des Client-Schedulers zu verwenden:

1. Wählen Sie in der GUI des Clients für Sichern/Archivieren **Editieren** > **Vorgaben** aus.
2. Klicken Sie auf die Registerkarte **Web-Client**.
3. Klicken Sie im Feld für die Optionen verwalteter Services auf **Zeitplan**. Wenn der Clientakzeptor auch den Web-Client verwalten soll, klicken Sie auf die Option **Beide**.
4. Starten Sie den Clientakzeptordämon mit dem folgenden Befehl in der Befehlszeile:
`dsmcad`

Tipp:

- Sie können auch die Option **managedservices** in der Clientsystemoptionsdatei (`dsm.sys`) verwenden, um anzugeben, ob der Clientakzeptor den Scheduler verwaltet.
- Wenn der Clientakzeptor den Scheduler im Abfragemodus verwalten soll, ohne einen Empfangsport zu öffnen, verwenden Sie die Option **cadlistenonport** in der Datei `dsm.sys`.

Zugehörige Konzepte:

„Übersicht über die Konfiguration des Web-Clients“ auf Seite 67

„Geplante Befehle aktivieren oder inaktivieren“ auf Seite 302

„Planungsoptionen“ auf Seite 340

Zugehörige Tasks:

„Client-Scheduler-Prozess für die Ausführung als Hintergrundtask und den automatischen Start beim Systemstart definieren“ auf Seite 297

Zugehörige Verweise:

„Cadlistenonport“ auf Seite 372

„Managedservices“ auf Seite 502

„Sessioninitiation“ auf Seite 576

Client-Scheduler starten

Diese Task führt Sie durch die Schritte zum Planen von Ereignissen mithilfe der grafischen Benutzerschnittstelle und des Befehlszeilenclients.

Ereignisse mit dem Befehlszeilenclient planen

Diese Task führt Sie durch die Schritte zum Planen von Ereignissen über den Befehlszeilenclient.

Informationen zu diesem Vorgang

Sie müssen ein Systemadministrator sein, um den Client für Sichern/Archivieren für die Verwendung der Schnittstelle des Befehlszeilenclients zum Verarbeiten geplanter Ereignisse konfigurieren zu können. Die Befehlszeilentools müssen installiert sein, um diese Funktion zu aktivieren.

Anmerkung: Wenn Sie den Client-Scheduler über die Befehlszeile ausführen, wird der Scheduler nicht als Hintergrundservice ausgeführt.

Bevor Sie den Client-Scheduler über den Clientakzeptordämon starten können, müssen Sie die folgenden Schritte ausführen:

Vorgehensweise

1. Stellen Sie sicher, dass die Option `managedservices` in der Clientsystemoptionsdatei (`dsm.sys`) die Angabe `schedule` enthält.
2. Setzen Sie die Option `passwordaccess` in der Clientsystemoptionsdatei (`dsm.sys`) auf `generate`.

Ergebnisse

Wenn Sie Dateien für die Verschlüsselungsverarbeitung einschließen, stellen Sie sicher, dass Sie die Option **Kennwort für Verschlüsselungsschlüssel lokal speichern** im Fenster **Berechtigungsvorgaben** auswählen, sodass der Client-Scheduler geplante Services unbeaufsichtigt ausführen kann, ohne den Benutzer zur Eingabe des Verschlüsselungsschlüssels aufzufordern. Wenn der Verschlüsselungsschlüssel zuvor noch nicht gespeichert wurde, müssen Sie eine überwachte Sicherung von mindestens einer Datei ausführen, damit die Eingabeaufforderung für die Verschlüsselung angezeigt und der Schlüssel gespeichert wird.

Um den Client-Scheduler auf Ihrem Clientknoten zu starten und eine Verbindung zum Serverzeitplan herzustellen, müssen Sie wie folgt vorgehen:

1. Wechseln Sie in das Installationsverzeichnis des Clients für Sichern/Archivieren und geben Sie den folgenden Befehl ein:

```
dsmc schedule
```

Wenn Sie den Client-Scheduler starten, ist dieser kontinuierlich aktiv, bis Sie das Fenster schließen, den Prozess beenden oder sich vom System abmelden.

2. Wenn sich das Verzeichnis mit den ausführbaren Dateien des Clients nicht in Ihrer Umgebungsvariablen `PATH` befindet, wechseln Sie in das Installationsverzeichnis und geben Sie den folgenden Befehl ein:

```
./dsmc schedule
```

3. Damit der Befehl **schedule** im Hintergrund ausgeführt wird und der Client-Scheduler auch nach einer Abmeldung vom System aktiv bleibt, Folgendes eingeben:

```
nohup dsmc schedule 2> /dev/null &
```

Wenn das IBM Spectrum Protect-Kennwort für Ihre Workstation erforderlich ist und der Befehl **schedule** im Hintergrund ausgeführt werden soll, muss das Kennwort mit dem Befehl eingegeben werden.

Root: Soll der Client-Scheduler automatisch gestartet werden, stellen Sie sicher, dass die Option `passwordaccess` in `dsm.sys` auf `generate` gesetzt ist. Führen Sie anschließend die Prozedur für Ihr Betriebssystem aus:

Zum automatischen Starten jedes Client-Schedulers fügen Sie der Datei `/etc/inittab` einen Eintrag hinzu. In der Regel ist abhängig vom Betriebssystem und seiner Konfiguration die Ausführungsebene 2, 3, 4, 5 oder 6 zu verwenden. Details zu Ausführungsebenen können Sie der Dokumentation zu Ihrem Betriebssystem entnehmen.

Überprüfen Sie die Syntax für den Eintrag anhand der Dokumentation zu Ihrem Betriebssystem.

Hier einige Beispiele:

Für AIX fügen Sie der Datei `/etc/inittab` den folgenden Eintrag hinzu:

```
itsm:2:once:/usr/bin/dsmc sched > /dev/null 2>&1 # TSM scheduler
```

In diesem Beispiel ist die Ausführungsebene auf 2 gesetzt.

Für Solaris fügen Sie der Datei `/etc/inittab` den folgenden Eintrag hinzu:

```
itsm:23:once:/usr/bin/dsmc sched > /dev/null 2>&1 # TSM scheduler
```

In diesem Beispiel ist die Ausführungsebene auf 2 und 3 gesetzt.

Anmerkung: Die Umleitung nach `/dev/null` muss im Befehl angegeben werden.

Für Mac OS X:

Der Systemadministrator muss ein Kennwort generieren, sodass der Client das Kennwort in der Kennwortdatei (`TSM.sth`) speichern kann. Dies kann entweder mithilfe der IBM Spectrum Protect-Tools für Administratoren oder über die Befehlszeile erfolgen.

Ein Systemadministrator muss eine der folgenden Methoden verwenden, um dem Clientakzeptordämon beim Starten des Systems das Starten des Befehlszeilenclients im Planungsmodus für die Verarbeitung geplanter Ereignisse zu ermöglichen.

Methode 1 (bevorzugt)

- Verwenden Sie die Anwendung 'IBM Spectrum Protect-Tools für Administratoren' und die Anwendung zum Starten des Clientakzeptordämons. Dadurch wird der Clientakzeptordämon als Systemstartelement installiert, sodass er nach Systemwiederanläufen automatisch gestartet wird. Der Clientakzeptordämon wird zudem sofort gestartet; Sie müssen das System also nicht erneut starten, um geplante Ereignisse zu verarbeiten.

Methode 2

- Verwenden Sie das Shell-Skript in `"/Library/Application Support/tivoli/tsm/client/ba/bin"`, um den Clientakzeptordämon als Systemstartelement zu installieren. Der Name des Skripts lautet `StartCad.sh`.

Führen Sie die folgenden Schritte aus, um den Clientakzeptordämon manuell zu starten und zu überprüfen, ob er aktiv ist.

1. Geben Sie den folgenden Befehl ein, um zu überprüfen, ob der Clientakzeptordämon aktiv ist:

```
sudo ps -x | grep dsmcad
```

Ist der Clientakzeptordämon aktiv, hat einer der aufgelisteten Prozesse den Pfad `/usr/bin/dsmcad`.

2. Geben Sie den folgenden Befehl in ein Terminalfenster ein, um den Clientakzeptordämon manuell zu starten:

```
sudo /sbin/SystemStarter start dsmcad
```

Der Client-Scheduler kann beim Systemstart möglicherweise nicht ordnungsgemäß initialisiert werden, da TCP/IP nicht vollständig initialisiert ist. Sie müssen unter Umständen den Start des Scheduler-Service verzögern, damit für die Initialisierung von TCP/IP ausreichend Zeit verfügbar ist.

Der Client erkennt keine Änderungen, die an der Datei `dsm.opt` oder `dsm.sys` vorgenommen werden, während der Client-Scheduler aktiv ist. Werden diese Dateien geändert, während der Client-Scheduler aktiv ist, und sollen die neuen Werte sofort verwendet werden, muss der Client-Scheduler gestoppt und dann erneut gestartet werden. Wenn Sie beispielsweise die Option `incl excl` in Ihrer Datei `dsm.sys` ändern, sodass sie auf eine andere Einschluss-/Ausschlussoptionsdatei verweist, muss der Client-Scheduler gestoppt und erneut gestartet werden, bevor der Client die neue Datei verwendet.

Verwenden Sie zum manuellen Stoppen des Client-Schedulers den Befehl **kill**, falls der Client-Scheduler im Hintergrund ausgeführt wird, oder drücken Sie die Taste **q** bzw. die Tastenkombination **Strg+C**, falls er im Vordergrund ausgeführt wird. Um den Client-Scheduler erneut zu starten, geben Sie den Befehl **schedule** erneut ein.

Unabhängig von der Einstellung der Option `tapeprompt` in der Optionsdatei erfolgt während eines geplanten Ereignisses keine Aufforderung zum Laden von Bändern.

Zugehörige Tasks:

„Scheduler konfigurieren“ auf Seite 69

Zugehörige Verweise:

„Managedservices“ auf Seite 502

„Passwordaccess“ auf Seite 525

IBM Spectrum Protect-Client/Server-Übertragung über eine Firewall hinweg konfigurieren

In den meisten Fällen können die IBM Spectrum Protect-Server und -Clients über eine Firewall hinweg zusammenarbeiten.

Informationen zu diesem Vorgang

Alle Firewalls sind unterschiedlich; daher muss der Firewall-Administrator möglicherweise die Anweisungen für die verwendete Firewall-Software oder -Hardware konsultieren.

Es gibt zwei Methoden, um Client- und Serveroperationen durch eine Firewall zu aktivieren:

Methode 1:

Damit Clients über eine Firewall hinweg mit einem Server kommunizieren können, müssen folgende Anschlüsse in der Firewall durch den Firewall-Administrator geöffnet werden:

TCP/IP-Anschluss

Sollen der Client für Sichern/Archivieren, der Befehlszeilenverwal-

tungsclient und der Scheduler außerhalb einer Firewall ausgeführt werden, muss der Anschluss, der von der Serveroption **tcpport** angegeben wird (Standardwert 1500), vom Firewall-Administrator geöffnet werden. Dieser Anschluss wird mit der Option **tcpport** auf dem Client und Server definiert. Die Einstellung muss auf dem Client und Server dieselbe sein. Dies ermöglicht IBM Spectrum Protect-Schedulerkommunikation sowohl im Modus *Ausführung bei Sendeaufruf* als auch im Modus *gesteuerte Ausführung*, vom Clientakzeptor verwaltete Scheduler und regelmäßige Operationen des Clients für Sichern/Archivieren.

Anmerkung: Der Client kann den Anschluss, der durch die Option **tcpadminport** (auf dem Server) angegeben ist, nicht für eine Client-sitzung verwenden. Dieser Anschluss kann nur für Verwaltungssitzungen verwendet werden.

HTTP-Anschluss

Um der GUI des Clients für Sichern/Archivieren die Kommunikation mit den fernen Workstations über eine Firewall hinweg zu ermöglichen, muss der HTTP-Anschluss für die ferne Workstation geöffnet werden. Verwenden Sie die Option **httpport** in der Clientoptionsdatei der fernen Workstation, um diesen Anschluss anzugeben. Der standardmäßige HTTP-Anschluss ist 1581.

TCP/IP-Anschlüsse für die ferne Workstation

Die beiden TCP/IP-Anschlüsse für den fernen Workstation-Client müssen geöffnet werden. Verwenden Sie die Option **webports** in der Clientoptionsdatei der fernen Workstation, um diese Anschlüsse anzugeben. Werden keine Werte für die Option **webports** angegeben, bewirkt der Standardwert null (0), dass TCP/IP willkürlich zwei freie Anschlussnummern zuweist.

TCP/IP-Anschluss für Verwaltungssitzungen

Gibt eine separate TCP/IP-Anschlussnummer an, an der der Server Anforderungen für Verwaltungsclientsitzungen erwartet. Dies ermöglicht sichere Verwaltungssitzungen innerhalb eines privaten Netzes.

Methode 2:

Es ist unnötig, für den Client-Scheduler im Modus mit Bedienerführung *irgendwelche* Anschlüsse auf der Firewall zu öffnen. Wenn Sie die Option **sessioninitiation** auf *serveronly* setzen, versucht der Client nicht, Kontakt zum Server aufzunehmen. *Alle Sitzungen werden durch die Zeitplanung über Serversystemanfrage* an dem mit der Option **tcpclientport** auf dem Client definierten Anschluss eingeleitet. Die Option **sessioninitiation** beeinflusst nur das Verhalten des Client-Schedulers, der im Modus mit Bedienerführung ausgeführt wird.

Der IBM Spectrum Protect-Server muss für jeden Knoten den Parameter "SESSIONINITiation" in den Befehlen **register node** und **update node** definieren. Wenn der Server SESSIONINITiation=*clientorserver*, den Standardwert, angibt, kann der Client entscheiden, welche Methode verwendet werden soll. Wenn der Server SESSIONINITiation=*serveronly* angibt, werden alle Sitzungen vom Server eingeleitet.

Damit eine Client-Scheduler-Konfiguration bei Verwendung dieser Methode funktionsfähig ist, müssen die folgenden Parameter mit SESSIONINITiation=*serveronly* **UND** SESSIONSECURITY=*transitional* festgelegt werden.

Anmerkung:

1. Wird *sessioninitiation* auf *serveronly* gesetzt, muss der Wert für die Clientoption *tcpclientaddress* mit dem Wert für die Option *HLAddress* im Serverbefehl **update node** oder **register node** übereinstimmen. Der Wert für die Clientoption *tcpclientport* muss mit dem Wert für die Option *LLAddress* im Serverbefehl **update node** oder **register node** übereinstimmen.
2. Wenn Sie die Option *sessioninitiation* auf *serveronly* setzen, versuchen der Befehlszeilenclient und die GUI des Clients für Sichern/Archivieren mit Ausnahme der vom Clientakzeptor verwalteten Scheduler weiterhin, Sitzungen einzuleiten; sie werden jedoch vom IBM Spectrum Protect-Server für Knoten blockiert, für die die Option *sessioninitiation* auf *serveronly* gesetzt ist.
3. Wenn der Scheduler zum ersten Mal auf einer Client-Workstation konfiguriert wird, kann sich der Scheduler-Service unter Umständen nicht beim Server authentifizieren, wenn der Server den Client-Scheduler kontaktiert, um einen Zeitplan auszuführen. Dies kann geschehen, wenn *passwordaccess* auf *generate* gesetzt ist, der IBM Spectrum Protect-Server sich hinter einer Firewall befindet und das verschlüsselte Kennwort nicht lokal gespeichert werden kann, bevor der Scheduler gestartet wird. Um dieses Problem zu beheben, müssen Sie den Scheduler von der Befehlszeile aus ausführen (*dsmc schedule*), warten, bis eine geplante Operation gestartet wird, und das Kennwort für Ihren Knoten eingeben, wenn Sie dazu aufgefordert werden.
4. Der Client kann keine Eingabeaufforderung für das Kennwort für den Verschlüsselungsschlüssel im Schedulermodus anzeigen. Wenn Sie die IBM Spectrum Protect-Datenverschlüsselung verwenden, müssen Sie einmal eine interaktive Erstsicherung ausführen, um den Verschlüsselungsschlüssel zu definieren, indem Sie die TCP/IP-Verbindung von der Client-Workstation zur Server-Workstation öffnen. Weitere Informationen zum Einrichten dieser Übertragung finden Sie unter **Methode 1**. Nachdem der Verschlüsselungsschlüssel definiert wurde, können Sie vom Server eingeleitete Sitzungen verwenden, um die Dateien mithilfe der Verschlüsselung zu sichern.

Wenn Sie die Option *sessioninitiation* auf *client* setzen, leitet der Client Sitzungen mit dem Server ein (**Methode 1**), indem er über den TCP/IP-Anschluss kommuniziert, der durch die Serveroption *tcpport* definiert ist. Dies ist der Standardwert. Mit der Zeitplanung über Serversystemanfrage kann der Client dazu aufgefordert werden, eine Verbindung zum Server herzustellen.

Bei Verwendung des Clients für Sichern/Archivieren über eine Firewall hinweg im *Modus mit Bedienerführung* muss der IBM Spectrum Protect-Server den Kontakt zum Client herstellen. Dazu muss unter Umständen Software auf dem IBM Spectrum Protect-Server installiert werden, damit die Anforderung über die Firewall geleitet werden kann. Diese Software leitet die Serveranforderung über einen Socks-Anschluss auf der Firewall. Diese Methode wird als *Socksifizierung eines Systems* bezeichnet. Proxys werden nicht unterstützt, da sie nur bestimmte Arten von Übertragungsprotokollen (HTTP, FTP, GOPHER) weiterleiten. IBM Spectrum Protect-Übertragungen werden nicht durch Proxys weitergeleitet. Es ist wichtig zu wissen, dass der Client nach entsprechender Aufforderung eine neue Verbindung zum IBM Spectrum Protect-Server herstellt. Dies bedeutet, dass die oben beschriebene Firewall-Konfiguration die geeigneten Einstellungen aufweisen muss.

Zugehörige Tasks:

| „Scheduler konfigurieren“ auf Seite 69

| **Zugehörige Verweise:**

| „Sessioninitiation“ auf Seite 576

| „Tcpadminport“ auf Seite 609

| „Tcpport“ auf Seite 614

| „Webports“ auf Seite 680

IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren

Secure Sockets Layer (SSL) ermöglicht eine sichere Kommunikation auf SSL-Basis nach Industriestandard zwischen dem IBM Spectrum Protect-Client und -Server.

Informationen zu diesem Vorgang

Die folgenden Clientkomponenten unterstützen SSL:

- Befehlszeilenclient
- Verwaltungsbefehlszeilenclient
- Client-GUI
- Client-API

Nur abgehende Client/Server-Verbindungen unterstützen SSL. Ein Client der Version 8.1.2, der mit einer Server einer früheren Version kommuniziert, unterstützt SSL. Ein Client der Version 8.1.2, der mit einem Server der Version 8.1.2 kommuniziert, muss SSL verwenden. Eingehende Verbindungen (beispielsweise Clientakzeptor, vom Server eingeleitete Zeitplanverbindungen) unterstützen SSL nicht. Die Kommunikation zwischen Clients unterstützt SSL. Die Web-GUI unterstützt SSL nicht. Die Web-GUI wird bei der Kommunikation mit einem Server der Version 8.1.2 nicht mehr unterstützt.

Jeder IBM Spectrum Protect-Server, der für SSL aktiviert ist, muss über ein eindeutiges Zertifikat verfügen. Das Zertifikat kann einen der folgenden Typen aufweisen:

- Ein von IBM Spectrum Protect selbst signiertes Zertifikat.
- Ein von einer Zertifizierungsstelle (Certificate Authority - CA) ausgestelltes Zertifikat. Die Zertifizierungsstelle kann ein Unternehmen wie VeriSign oder Thawte oder eine interne Zertifizierungsstelle innerhalb Ihres Unternehmens sein.

Führen Sie die folgenden Schritte aus, um die SSL-Übertragung mit einem selbst signierten Zertifikat zu aktivieren:

1. Besorgen Sie sich das selbst signierte Zertifikat des IBM Spectrum Protect-Servers (cert256.arm). Verwenden Sie die Zertifikatsdatei cert.arm, wenn der Server nicht für die Verwendung von Transport Layer Security (TLS) 1.2 konfiguriert ist. Verwenden Sie andernfalls die Datei cert256.arm. Die Clientzertifikatsdatei muss mit der vom Server verwendeten Zertifikatsdatei identisch sein.
2. Konfigurieren Sie die Clients. Damit SSL verwendet werden kann, muss jeder Client das selbst signierte Serverzertifikat importieren.
Importieren Sie das Zertifikat mithilfe des Dienstprogramms dsmcert.
3. Geht bei einem Ausfall des IBM Spectrum Protect-Servers das Zertifikat verloren, wird automatisch ein neues Zertifikat vom Server generiert. Jeder Client muss das neue Zertifikat abrufen und importieren.

Für Schnellzugriffspfaddetails für die Kommunikation zwischen einem Client der Version 8.1.2 und einem Server der Version 8.1.2 können Sie die Option `SSLACCEPTCERTFROMSERV` verwenden, um ein selbst signiertes Zertifikat automatisch zu akzeptieren. Ausführliche Informationen finden Sie in „Konfiguration mithilfe der Standardsicherheitseinstellungen (Schnellzugriffspfad)“ auf Seite 145.

Führen Sie die folgenden Schritte aus, um die SSL-Übertragung mit einem von einer Zertifizierungsstelle signierten Zertifikat zu aktivieren:

1. Besorgen Sie sich das CA-Stammzertifikat.
2. Konfigurieren Sie die Clients. Damit SSL verwendet werden kann, muss jeder Client das selbst signierte Serverzertifikat importieren.

Importieren Sie das Zertifikat mithilfe des Dienstprogramms `dsmcert`.

Tipp: Nachdem Sie diesen Schritt ausgeführt haben, muss der Client das Stammzertifikat nicht erneut importieren, wenn der Server ein neues Zertifikat erhält, das von derselben CA signiert ist.

3. Wenn Sie den Client für Sichern/Archivieren im Rahmen der Wiederherstellung nach einem Katastrophenfall wiederherstellen, müssen Sie das SSL-Zertifikat erneut auf dem Server installieren. Wenn das Zertifikat nicht mehr vorhanden ist, müssen Sie ein neues Zertifikat anfordern. Sie müssen den Client nicht rekonfigurieren, wenn das neue Zertifikat von einer CA signiert wurde.

Als Nächstes müssen Sie das Serverzertifikat oder das CA-Stammzertifikat importieren.

Bei Verwendung eines selbst signierten Zertifikats

Jeder IBM Spectrum Protect-Server generiert ein eigenes Zertifikat. Der festgelegte Dateiname des Zertifikats ist entweder `cert.arm` oder `cert256.arm`. Die Zertifikatsdatei wird auf der Server-Workstation im Serverinstanzverzeichnis gespeichert (z. B. `/opt/tivoli/tsm/server/bin/cert256.arm`). Falls die Zertifikatsdatei nicht vorhanden ist und Sie die Serveroption **SSLTCPPORT** oder **SSLTCPADMINPORT** angeben, wird die Zertifikatsdatei erstellt, wenn Sie den Server mit diesen Optionen erneut starten. IBM Spectrum Protect-Server der Version 6.3 (und höher) generieren Dateien namens `cert256.arm` und `cert.arm`. IBM Spectrum Protect-Server mit einer älteren Version als 6.3 generieren ausschließlich Zertifikatsdateien namens `cert.arm`. Sie müssen das Zertifikat auswählen, das als Standardwert auf dem Server festgelegt ist.

Führen Sie die folgenden Schritte aus, um die SSL-Verbindung zu einem Server einzurichten:

1. Besorgen Sie sich das Zertifikat beim Serveradministrator.
2. Importieren Sie das Zertifikat mit dem folgenden Befehl in die Schlüsseldatenbank des Clients:

```
dsmcert -add -server <Servername> -file <Pfad_zu_cert256.arm>
```

Bei Verwendung eines Zertifikats von einer Zertifizierungsstelle

Wenn das Zertifikat von einer Zertifizierungsstelle (Certificate Authority - CA) wie VeriSign oder Thawte ausgestellt wurde, ist der Client für SSL bereit und Sie können die folgenden Schritte überspringen.

Die Liste der vorinstallierten Stammzertifikate externer Zertifizierungsstellen finden Sie in „Stammzertifikate von Zertifizierungsstellen“ auf Seite 82. Wenn das Zertifikat nicht von einer der anerkannten Zertifizierungsstellen ausgestellt wurde, führen Sie die folgenden Schritte aus:

1. Besorgen Sie sich das Stammzertifikat der Zertifizierungsstelle, die das Zertifikat signiert hat.
2. Importieren Sie das Zertifikat mit dem folgenden Befehl in die Schlüsseldatenbank des Clients:

```
dsmcert -add -server <Servername> -file <Pfad_zu_cert256.arm>
```

Wichtig:

1. Die Schlüsseldatenbank wird mit einem automatisch generierten Pseudokennwort verschlüsselt. Das Kennwort wird automatisch in der Stashdatei (dsmcert.sth) gespeichert. Die Stashdatei wird vom Client für Sichern/Archivieren verwendet, um das Kennwort für die Schlüsseldatenbank abzurufen.
2. Der Schlüsseldatenbankdatei des Clients können mehrere Serverzertifikate hinzugefügt werden, sodass der Client eine Verbindung zu verschiedenen Servern herstellen kann. Ebenso können der Schlüsseldatenbank des Clients mehrere CA-Stammzertifikate hinzugefügt werden.
3. Wenn Sie die vorhergehenden Befehle nicht im Verzeichnis des Clients für Sichern/Archivieren ausführen, müssen Sie dsmcert.kdb und dsmcert.sth in dieses Verzeichnis kopieren.
4. Standardmäßig ist der Root Eigner der lokalen Schlüsseldatenbankdateien und nur er verfügt über Berechtigungen. Andere Benutzer können diese Dateien nicht lesen. Wenn Sie planen, den Client als Benutzer ohne Rootberechtigung auszuführen, müssen Sie die Berechtigungen aktualisieren. Führen Sie beispielsweise den folgenden Befehl aus, um allen Benutzern und Gruppen Lesezugriff zu erteilen:

```
# chmod go+r dsmcert.*
```
5. Aus Leistungsgründen sollten Sie SSL nur bei Bedarf für Sitzungen verwenden. Ein Client der Version 8.1.2, der mit einem Server der Version 8.1.2 kommuniziert, muss SSL verwenden. SSL No (der Standardwert) gibt an, dass keine Verschlüsselung verwendet wird, wenn Daten zwischen dem Client und einem Server einer Version vor Version 8.1.2 übertragen werden. Wenn der Client die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt, gibt der Standardwert No an, dass Objektdaten nicht verschlüsselt werden. Alle anderen Informationen werden verschlüsselt, wenn der Client mit dem Server kommuniziert. Wenn der Client die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt, gibt der Wert Yes an, dass SSL zum Verschlüsseln aller Informationen, einschließlich Objektdaten, verwendet wird, wenn der Client mit dem Server kommuniziert. Sie könnten dem IBM Spectrum Protect-Serversystem für die höheren Anforderungen zusätzliche Prozessorressourcen hinzufügen.
6. Damit ein Client eine Verbindung zu einem Server herstellen kann, der Transport Layer Security (TLS) Version 1.2 verwendet, muss das Zertifikat den Signaturalgorithmus SHA-1 oder einen strengeren Algorithmus aufweisen. Falls Sie ein selbst signiertes Zertifikat verwenden, müssen Sie das Zertifikat cert256.arm verwenden. Ihr IBM Spectrum Protect-Administrator muss möglicherweise das Standardzertifikat auf dem IBM Spectrum Protect-Server ändern. Details enthält der Abschnitt über die Serveroption SSLTLS12.

Weitere ausführliche Informationen für einen Client der Version 8.1.2, der mit einem Server der Version 8.1.1 oder früheren Stufen der Version 8 bzw. Version 7.1.7 und früheren Stufen kommuniziert

Nachdem das Serverzertifikat der Clientschlüsseldatenbank hinzugefügt wurde, fügen Sie die Option SSL Yes der Clientoptionsdatei hinzu und aktualisieren den Wert der Option TCPPOPT. Es ist wichtig zu verstehen, dass

der Server normalerweise auf einem anderen Anschluss für SSL-Verbindungen eingerichtet wird. In anderen Worten: Auf dem Server werden zwei Anschlüsse geöffnet:

1. Ein Anschluss akzeptiert normale Clientverbindungen ohne SSL.
2. Ein anderer Anschluss akzeptiert nur SSL-Verbindungen.

Sie können mit einem SSL-fähigen Client keine Verbindung zu einem Nicht-SSL-Anschluss herstellen, und umgekehrt gilt dies ebenso.

Ist der Wert von **tcppport** falsch, kann der Client keine Verbindung zum Server herstellen. Geben Sie in der Option **tcppport** die richtige Anschlussnummer an.

Wenn Sicherheitsprotokolle inaktiviert werden sollen, die nicht so sicher wie TLS 1.2 sind, fügen Sie der Clientoptionsdatei die Option **SSLDISABLELEGACYtls yes** hinzu oder wählen Sie in der Java-GUI das Kontrollkästchen **TLS 1.2 oder höher erforderlich** auf der Registerkarte **Übertragung** des Profileditors aus. Wenn TLS 1.2 oder höher als erforderlich angegeben wird, können Attacken durch Schadprogramme besser verhindert werden.

Zugehörige Verweise:

„Ssl“ auf Seite 598

„Sslfipsmode“ auf Seite 601

Symbolischen Link für den Zugriff auf die neueste GSKit-Bibliothek erstellen

Sie können einen symbolischen Link erstellen, um von dem Verzeichnis, in dem die frühere Version von GSKit installiert ist, auf die Position zu verweisen, an der sich die neuesten GSKit-Bibliotheken auf dem System befinden.

Vorbereitende Schritte

- Für einen IBM Spectrum Protect-Client der Version 8.1.2 und höheren Stufen sowie Version 7.1.8 und höheren Stufen der Version 7 ist GSKit-Version 8.0.50.78 erforderlich.
- Für einen IBM Spectrum Protect-Client der Version 8.1.1 und früheren Stufen der Version 8 sowie Version 7.1.7 und früheren Stufen ist eine frühere GSKit-Version als 8.0.50.78 erforderlich.

Informationen zu diesem Vorgang

Wenn Sie Db2 for Linux, UNIX, and Windows unter UNIX und Linux installieren, werden auch lokale GSKit-Bibliotheken installiert. Diese Bibliotheken sind in `<Db2-Installationspfad>/lib64/gskit_db2` oder `<Db2-Installationspfad>/lib32/gskit_db2` gespeichert. Unter Windows ist die Standardposition `C:\Programme\ibm\gsk8`.

Während der Installation anderer IBM Produkte, wie beispielsweise IBM Spectrum Protect, wird unter Umständen eine weitere Kopie der GSKit-Bibliotheken installiert. Abhängig von dem Produkt kann es sich bei diesen Bibliotheken um lokale GSKit-Bibliotheken oder globale GSKit-Bibliotheken handeln. Wenn Db2 for Linux, UNIX, and Windows und ein anderes IBM Produkt, das GSKit-Bibliotheken umfasst, auf demselben System installiert werden, kann es zu Interoperabilitätsproblemen kommen. Diese Interoperabilitätsprobleme können auftreten, da GSKit nur

Bibliotheken aus einer einzigen GSKit-Quelle in einem einzelnen Prozess zulässt. Die Interoperabilitätsprobleme können zu unvorhersehbarem Verhalten und Laufzeitfehlern führen.

Um sicherzustellen, dass eine einzige Quelle für GSKit-Bibliotheken verwendet wird, kann das Konzept symbolischer Links verwendet werden. Während einer Erstinstallation von Db2 for Linux, UNIX, and Windows erstellt das Installationsprogramm einen symbolischen Link `<Db2-Installationspfad>/lib64/gskit` oder `<Db2-Installationspfad>/lib32/gskit` zu `<Db2-Installationspfad>/lib64/gskit_db2` oder `<Db2-Installationspfad>/lib32/gskit_db2`. Diese symbolischen Links sind die Standardpositionen, aus denen die GSKit-Bibliotheken geladen werden. Für Produkte, deren Produktpaket Db2 for Linux, UNIX, and Windows umfasst, und den symbolischen Link vom Standardverzeichnis in das Bibliotheksverzeichnis einer anderen Kopie von GSKit ändern, muss sichergestellt werden, dass das neu installierte GSKit dieselbe oder eine höhere Version hat. Diese Einschränkung gilt unabhängig davon, ob es sich um globale oder lokale Bibliotheken handelt. Während eines Upgrades oder Updates von Db2 for Linux, UNIX, and Windows wird der symbolische Link beibehalten. Wenn die neu installierte Kopie über einen symbolischen Link zur Standardposition verfügt, wird der symbolische Link, der der älteren Installationskopie zugeordnet ist, beibehalten. Wenn die neu installierte Kopie über keinen symbolischen Link zur Standardposition verfügt, wird der symbolische Link, der der neueren Installationskopie zugeordnet ist, beibehalten.

Es bestehen bestimmte Einschränkungen, da sich der symbolische Link `<Db2-Installationspfad>/lib64/gskit` oder `<Db2-Installationspfad>/lib32/gskit` in dem Pfad der Installationskopie von Db2 for Linux, UNIX, and Windows befindet. Wenn beispielsweise zwei oder mehr Instanzen für eine Db2-Kopie erstellt werden, haben Änderungen an dem symbolischen Link Auswirkungen auf alle Instanzen.

Sie können auch ein Domino-Server-GSKit auf ähnliche Weise ändern. Ein Domino-Server verfügt über nicht über einen GSKit-Ordner, aber über die Ordner C und N sowie eine Bibliothek `libgsk8iccs_64.so`. Sie können zunächst Softlinks für diese Ordner und Dateien erstellen, um auf die entsprechenden Ordner im GSKit-Paket zu verweisen, in denen der IBM Spectrum Protect-Client für Sichern/Archivieren der Version 8.1.2 installiert ist; gehen Sie dazu wie folgt vor:

- `ln -s /usr/local/ibm/gsk8_64/lib64/C /opt/ibm/lotus/notes/90010/zlinux`
- `ln -s /usr/local/ibm/gsk8_64/lib64/N /opt/ibm/lotus/notes/90010/zlinux`
- `ln -s /usr/local/ibm/gsk8_64/lib64/libgsk8iccs_64.so /opt/ibm/lotus/notes/90010/zlinux`

Ändern Sie im nächsten Schritt das Kennwort des DPD-Knotens in `domdsmc CHANGEADSM Pwd tv1054_domnote2 tv1054_domnote2 tv1054_domnote2`. Führen Sie abschließend `domdsmc query adsm` aus.

Vorgehensweise

1. Erstellen Sie einen symbolischen Link unter Windows, wenn Sie über Administratorberechtigungen verfügen. Benennen Sie die Db2-Kopie von GSKit im Verzeichnis `lib64`, das sich an der Standardposition `C:\Programme\ibm\gsk8` befindet, um. Starten Sie eine DOS-Shell, navigieren Sie zu der Position von Db2-GSKit und benennen Sie das Verzeichnis wie folgt um:

```
cd C:\Programme\ibm\gsk8
rename lib64 lib64-db2
```

2. Erstellen Sie einen symbolischen Link an der Position der Db2-Kopie von GSKit und verweisen Sie auf die Position der TSM-Kopie von GSKit, indem Sie in der DOS-Shell die folgenden Befehle ausführen. Navigieren Sie zu der Position der Db2-Kopie von GSKit und erstellen Sie dann wie folgt den symbolischen Link:

```
cd C:\Programme\ibm\gsk8
```

```
mklink /d lib64 "c:\Programme\Common Files\Tivoli\TSM\api64\gsk8\lib64"
```

3. Starten Sie Db2 erneut, damit die Änderungen wirksam werden. Beim Start lädt Db2 GSKit aus der neuen Position, die auf die IBM Spectrum Protect-Kopie von GSKit verweist. Geben Sie in der Db2-Eingabeaufforderung die folgenden Befehle ein:

```
db2stop
```

```
db2start
```

Stammzertifikate von Zertifizierungsstellen

Der Client für Sichern/Archivieren verfügt über eine Liste von Stammzertifikaten für eine Reihe bekannter Zertifizierungsstellen.

Die folgende Liste enthält die Stammzertifikate für eine Reihe bekannter Zertifizierungsstellen, die mit dem Client geliefert werden:

- Entrust.net Global Secure Server Certification Authority
- Entrust.net Global Client Certification Authority
- Entrust.net Client Certification Authority
- Entrust.net Certification Authority (2048)
- Entrust.net Secure Server Certification Authority
- VeriSign Class 3 Public Primary Certification Authority
- VeriSign Class 2 Public Primary Certification Authority
- VeriSign Class 1 Public Primary Certification Authority
- VeriSign Class 4 Public Primary Certification Authority - G2
- VeriSign Class 3 Public Primary Certification Authority - G2
- VeriSign Class 2 Public Primary Certification Authority - G2
- VeriSign Class 1 Public Primary Certification Authority - G2
- VeriSign Class 4 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 2 Public Primary Certification Authority - G3
- VeriSign Class 1 Public Primary Certification Authority - G3
- Thawte Personal Premium CA
- Thawte Personal Freemail CA
- Thawte Personal Basic CA
- Thawte Premium Server CA
- Thawte Server CA
- RSA Secure Server Certification Authority

Wenn Sie Zertifikate verwenden wollen, die von einer anderen Zertifizierungsstelle ausgegeben wurden, müssen Sie das Stammzertifikat dieser Zertifizierungsstelle im Rahmen der Clientkonfiguration auf allen Clients installieren.

System für die journalbasierte Sicherung konfigurieren

Bevor Sie journalbasierte Sicherungen ausführen können, müssen Sie den Journaldämon (Linux) oder den Journalsteuerkomponentenservice (Windows) installieren und konfigurieren.

Konfiguration des Journaldämons

Die journalbasierte Sicherung wird durch die Installation und Konfiguration des IBM Spectrum Protect-Journaldämons ermöglicht.

Konfigurieren Sie den Journaldämon, indem Sie die Konfigurationsmusterdatei für den Journaldämon (`tsmjbbd.ini.smp`) editieren und unter dem Namen `tsmjbbd.ini` speichern. Beide Dateien sollten sich im Standardinstallationsverzeichnis befinden.

Starten Sie nach der Konfiguration der Datei `tsmjbbd.ini` den Journaldämon, indem Sie die ausführbare Datei **tsmjbbd** starten.

Führen Sie die Scriptdatei `jbbinittab` aus, um der Datei `/etc/inittab` einen Eintrag hinzuzufügen, damit unter AIX der Journaldämon nach dem Neustart Ihres Systems gestartet wird. Die ausführbare Datei `tsmjbbd` und die Scriptdatei `jbbinittab` sollten sich im Standardinstallationsverzeichnis befinden.

Damit der Journaldämon unter AIX gestoppt wird, geben Sie den Befehl `kill nnnn` aus (`nnnn` ist die Prozess-ID von **tsmjbbd**). Bevor der Journaldämonprozess (**tsmjbbd**) beendet wird, wird die Dateipfadkernelerweiterung benachrichtigt, das Puffern von Dateiänderungen zu stoppen.

Wichtig: Verwenden Sie nicht den Befehl `kill -9 nnnn`, weil der Befehl `kill -9` den Prozess sofort und ohne eine Benachrichtigung, dass das Puffern von Dateiänderungen gestoppt werden soll, beendet.

Unter Linux erstellt das Installationsprogramm den Service `tsmjbbd` an der Position `/etc/init.d`. Führen Sie zum Steuern des Service den folgenden Befehl als Root aus. Mit diesem Befehl können Sie den Service stoppen, starten, erneut starten oder seinen Status überprüfen:



Wenn das Betriebssystem Linux den Initialisierungsservice `systemd` ausführt, führen Sie die folgenden Schritte aus, um den Journaldämon zu starten:

1. Kopieren Sie die bereitgestellte `systemd`-Einheitendatei `/opt/tivoli/tsm/client/ba/bin/tsmjbbd.service` in das Verzeichnis `/etc/systemd/system/`.
2. Führen Sie den folgenden Befehl aus, um die `systemd`-Einheitenliste zu aktualisieren:
`systemctl daemon-reload`
3. Führen Sie den folgenden Befehl aus, um den Journaldämon zur Systembootzeit zu starten:
`systemctl enable tsmjbbd.service`
4. Führen Sie den folgenden Befehl aus, um den Journaldämon zu starten:
`systemctl start tsmjbbd.service`

Anmerkung:

1. Netzdateisysteme und auslagerbare Dateisysteme werden nicht unterstützt.
2. Tägliche journalbasierte Sicherungen sollten durch regelmäßige vollständige Teilsicherungen ergänzt werden. Die Ausführung progressiver vollständiger Teilsicherungen kann mehr Zeit in Anspruch nehmen als eine journalbasierte Sicherung. Berücksichtigen Sie dies bei der Terminierung dieser Sicherungen, indem Sie die Teilsicherungen beispielsweise für Zeiten mit geringer Systemauslastung planen. Setzen Sie diese Sicherungsverfahren in einem ausgewogenen Verhältnis ein, das sich an Ihren Geschäftsanforderungen orientiert. Beispielsweise könnten Sie für jede Nacht eine journalbasierte Sicherung sowie zusätzlich eine vollständige progressive Teilsicherung pro Woche planen.
3. Bei der journalbasierten Sicherung wird die Dateipfadkernelerweiterung für die Überwachung der Dateisystemänderungen verwendet. Um die Leistung der journalbasierten Sicherungen zu verbessern, werden Verzeichnisse, die keine Benutzerdateien enthalten, nicht auf Änderungen überwacht und nicht in journalbasierte Sicherungen einbezogen. Die folgende Liste enthält die Verzeichnisse, die auf AIX- und Linux-Systemen bei journalbasierten Sicherungen nicht berücksichtigt werden. Änderungen an diesen Verzeichnissen werden verarbeitet, wenn Sie unter Verwendung des Befehls **incremental** mit der Option **-nojournal** regelmäßige vollständige Teilsicherungen ausführen.

AIX	Linux
/bin	/bin
/dev	/boot
/etc	/dev
/lib	/etc
/usr/bin	/lib
/usr/lib	/proc
/usr/share	/sbin
	/sys
	/usr/bin
	/usr/lib
	/usr/share
	/var

Die Konfigurationsdatei des Journaldämons wird regelmäßig auf Aktualisierungen der Liste der Journaled File Systems überprüft. Dateisysteme können zur Liste der überwachten Dateisysteme hinzugefügt oder daraus entfernt werden, ohne dass der Journaldämon gestoppt werden muss.

Achtung: Wenn Sie ein vom Journaldämon überwacht Dateisystem abhängen, wird die Journaldatenbank für dieses Dateisystem gelöscht. Damit die Datenbank erhalten bleibt, legen Sie `PreserveDbOnExit=1` in der Zeilengruppe mit den Einstellungen für Dateisysteme mit Journalaufzeichnung an. Diese Einstellung hat zur Folge, dass die Journaldatenbank erhalten bleibt, wenn das Dateisystem abgehängt wird; außerdem wird sichergestellt, dass die Journaldatenbank gültig ist, wenn das Dateisystem wieder angehängt wird. Weitere Informationen finden Sie in „Zeilengruppe JournaledFileSystemSettings“ auf Seite 86.

Die Syntax für Zeilengruppen und Zeilengruppeneinstellungen ist wie folgt:

Syntax für Zeilengruppen:

[Zeilengruppenname]

Syntax für Zeilengruppeneinstellungen:

Zeilengruppeneinstellung=Wert

Anmerkung:

1. Sie können Kommentare in der Datei angeben, indem Sie die Zeile mit einem Semikolon beginnen.
2. Bei Namen von Zeilengruppen und Werten muss die Groß-/Kleinschreibung nicht beachtet werden muss.
3. Numerische Werte können als Hexadezimalwerte angegeben werden, indem dem Wert die Zeichen 0x vorangestellt werden; andernfalls wird der Wert als Dezimalwert interpretiert.
4. Es besteht keine Korrelation zwischen diesen Einstellungen für Dateisysteme mit Journalaufzeichnung und Einstellungen in der Clientoptionsdatei. Beim Journaldämon handelt es sich um einen unabhängigen Prozess, der keine Optionen in der Clientoptionsdatei verarbeitet.

Zeilengruppe JournalSettings

Einstellungen unter dieser Zeilengruppe sind global und gelten für den gesamten Journaldämon.

Die Zeilengruppe JournalSettings hat folgende Syntax:

Syntax für die Zeilengruppe JournalSettings:

[JournalSettings]

Syntax für Zeilengruppeneinstellungen:

JournalSettings=*Wert*

Sie können folgende Werte für JournalSettings angeben:

ErrorLog

Gibt die Protokolldatei an, in die die vom Journaldämon generierten, ausführlichen Nachrichten geschrieben werden. Der Standardwert ist jbberror.log im Verzeichnis der ausführbare Datei des Dämons. Zum Beispiel:

ErrorLog=/logs/jbberror.log

JournalDir

Verzeichnis, in das Journaldatenbankdateien geschrieben werden und in dem sie gespeichert sind.

Ist der angegebene Pfad ein absoluter Pfadname (wenn er z. B. mit einem Begrenzer dir beginnt), ist dies das verwendete Verzeichnis. Ist der angegebene Pfad ein relativer Verzeichnisname, wird dieser Pfad an jeden Dateisystemnamen angehängt, und es wird der daraus resultierende Pfadname verwendet.

Standardwert ist ein Verzeichnis mit dem Namen .tSm_JoUrNaL (wird innerhalb jedes Dateisystems verwendet, für das eine Journalführung erfolgt).

Der Vorteil des Ansiedelns der Journaldatenbank auf dem Dateisystem, das überwacht wird, ist das Verbleiben der Datenbank beim Dateisystem. Der Nachteil liegt darin, dass die Aktualisierungen für die Datenbank verarbeitet und gelöscht werden müssen.

Wichtig: Übertragen Sie die Datenbank in ein Dateisystem, das kein Journalized File System ist, sofern dieses Dateisystem nicht in einer Clusterumgebung gemeinsam genutzt wird.

Diese Einstellung gilt für alle Journaled File Systems; sie kann jedoch durch eine Überschreibungszeilengruppe für jedes Journaled File System überschrieben werden.

Zeilengruppe JournalExcludeList

Die Liste der Exclude-Anweisungen filtert Änderungen und verhindert, dass manche Änderungen in der Journaldatenbank aufgezeichnet werden.

Änderungen an Objekten, die mit den Anweisungen in dieser Zeilengruppe übereinstimmen, werden ignoriert und nicht in der Journaldatenbank aufgezeichnet.

Anmerkung:

1. Das Ausschließen von Dateien aus dem Journal hat keine Bedeutung für diejenigen Dateien, die vom Sicherungscient ausgeschlossen werden, außer dass verhindert wird, dass während einer journalbasierten Sicherung die Dateien zur Verarbeitung an den Sicherungscient gesendet werden. Eine Datei, die nicht aus dem Journal ausgeschlossen ist, sollte dennoch vom Client für Sichern/Archivieren ausgeschlossen werden, wenn es eine übereinstimmende Exclude-Anweisung in der Clientoptionsdatei gibt.
2. Der Journaldämon bietet nur eine Teilmenge der Funktion INCLUDE/EXCLUDE, die vom Client für Sichern/Archivieren zur Verfügung gestellt wird. Der Journaldämon unterstützt keine Anweisungen INCLUDE und auch nicht die Option *exclude.dir*.

Es besteht keine Korrelation zwischen der Ausschlussliste des Journals und der Ausschlussliste des Clients für Sichern/Archivieren.

Die folgenden Metazeichen für die Mustererkennung werden unterstützt:

- % Stimmt mit genau einem einzigen Zeichen überein.
- * Entspricht null oder mehr Zeichen.
- %EnvVar%
Erweitert die Umgebungsvariable.

Nachfolgend steht ein Beispiel für die Syntax einer Exclude-Anweisung:

```
[JournalExcludeList]
*.jbb.jbbdb
*.jbbInc.jbbdb
```

Zeilengruppe JournaledFileSystemSettings

Einstellungen unter dieser Zeilengruppe gelten für jedes angegebene Journaled File System, sofern sie nicht für einzelne Dateisysteme in einer Überschreibungszeilengruppe überschrieben sind.

Dateisysteme, die Sie in der Zeilengruppe 'JournalFileSystems.Extended' angeben, überschreiben alle Dateisysteme, die Sie möglicherweise zuvor in der Zeilengruppe 'JournaledFileSystemSettings' in der Liste der Journaled File Systems angegeben haben. Alle anderen Optionen, die Sie in der Zeilengruppe 'JournaledFileSystemsSettings' angegeben haben, bleiben erhalten.

Die Syntax für die Zeilengruppe 'JournaledFileSystemSettings' ist nachfolgend dargestellt:

Syntax für die Zeilengruppe JournaledFileSystemSettings:
[JournaledFileSystemSettings]

Syntax für Zeilengruppeneinstellungen:
JournaledFileSystemSetting=Wert

Sie können folgende Werte für *JournaledFileSystemSettings* angeben:

JournaledFileSystems

Gibt eine Liste der aufzuzeichnenden Dateisysteme an (die einzelnen Einträge werden durch Leerzeichen voneinander getrennt). Es werden vollständige Dateisystemspezifikationen und virtuelle Windows-Zusammenführungen unterstützt. Es gibt keinen Standardwert. Sie müssen mindestens ein Journaled File System angeben, damit der Journaldämon ausgeführt wird. Journaled File Systems können online hinzugefügt oder entfernt werden, ohne dass der Dämon erneut gestartet werden muss. Zum Beispiel:

```
JournaledFileSystems=/home /other
```

Wichtig: Das Journal wählt Objektnamen streng auf der Basis einer Zeichenfolgeübereinstimmung aus. Die Auswirkungen auf den Benutzer liegen darin, dass er größte Sorgfalt walten lassen muss, wenn er Dateisysteme für die Journalführung auswählt. Beispiel: Angenommen, Sie haben ein Dateisystem /jbb und ein anderes Dateisystem namens /jbb/mnt1. Wenn Sie das Journal anweisen, nur /jbb zu überwachen, entsprechen auch alle Änderungen für /jbb/mnt1 dieser Zeichenfolge und werden in die Datenbank eingegeben. Wenn Sie jedoch eine Sicherung auf dem Client durchführen, wird dieser den Namen auf der Basis der Dateisysteme syntaktisch analysieren, erkennen, dass das Journal dieses Dateisystem nicht überwacht und anschließend dem Journal mitteilen, die Dateien /jbb/mnt1 aus der Datenbank zu entfernen. Die Lösung ist, entweder beide zu überwachen oder die Liste JournalExcludeList zu verwenden. Dasselbe gilt für die Optionen der virtuellen Mountpunkte. Sie müssen mit dieser Liste konsistent sein. Wenn Sie beispielsweise /home/student1 als virtuellen Mountpunkt in Ihrer Optionsdatei dsm.sys angeben und /home unter Journalführung stellen wollen, müssen Sie JournaledFileSystems=/home /home/student1 angeben. In diesem Fall werden zwei separate Datenbanken erstellt.

JournalDbSize

Gibt die maximale Größe der Journaldatenbank an. Die Größe der Journaldatenbank wird in Byte angegeben. Der Wert Null (0) gibt an, dass die Datenbankgröße nur von der Kapazität des Dateisystems, das die Journaldatenbank enthält, begrenzt wird. Der Standardwert ist 0 (unbegrenzt). Zum Beispiel:

```
JournalDbSize=0x10000000
```

NotifyBufferSize, DirNotifyBufferSize

Geben Sie Benachrichtigung über Änderungen der Puffergrößen für ein Journaled File System an. Ein großer Umfang an Änderungsaktivitäten auf einem Journaled File System erfordert unter Umständen, dass diese vergrößert werden. Der Standardwert ist 0x00020000 (128 k) für Dateien und 0x00010000 (64 k) für Verzeichnisse.

```
NotifyBufferSize=0x00200000
```

Einstellung PreserveDbOnExit

Diese Einstellung ermöglicht, dass ein Journal gültig bleibt, wenn ein Journaled File System in den Status 'offline' und danach wieder in den Status 'online' versetzt wird. Dies ist hilfreich, um das Journal beim Systemwarmstart und bei der Ressourcenversetzung beizubehalten.

Diese Einstellung ermöglicht, dass bei einer journalbasierten Sicherung die Verarbeitung fortgesetzt wird, wenn der Dämon erneut gestartet wird (oder das Dateisystem wieder in den Status 'online' versetzt wird), ohne eine vollständige Teilsicherung ausführen zu müssen.

Anmerkung: Jede Änderungsaktivität, die auftritt, während der Journaldämon nicht aktiv ist (oder während das Dateisystem offline ist), wird nicht im Journal aufgezeichnet.

Der Wert 1 gibt an, dass die Datenbank des Journaled File System nicht gelöscht wird, wenn das Journaled File System in den Status 'offline' versetzt wird. Die Datenbank hat immer noch Gültigkeit, wenn das Journaled File System wieder in den Status 'online' versetzt wird. Dieser Wert sollte mit Vorsicht verwendet werden, da jede Änderungsaktivität für das Dateisystem, die auftritt, während das Journaled File System offline ist, nicht in der Journaldatenbank widergespiegelt wird. Mit der Standardeinstellung 0 wird die Journaldatenbank des Journaled File System gelöscht.

Anmerkung: Das Journal bleibt nur erhalten, wenn ein Journaled File System normal 'offline' gesetzt wird oder 'offline' gesetzt wird, wenn die Ressource nicht mehr verfügbar ist und Sie die Einstellung `deferFsMonStart` angeben. Wird ein Dateisystem aufgrund eines Fehlers wie beispielsweise eines Benachrichtigungspufferüberlaufs 'offline' gesetzt, wird das Journal gelöscht.

Anmerkung: Setzen Sie `preserveDBonExit` nur, wenn Sie sicherzustellen können, dass der Journalservice kontrolliert beendet wird. Unter eine "kontrollierte Beendigung" fällt auch das Stoppen des Journalservice, um das System erneut zu starten, die Übernahme einer Clusterressource oder das Versetzen einer Clusterressource. Die Journaldatenbank kann beschädigt werden, wenn die Beendigung nicht kontrolliert erfolgt. Führen Sie daher die folgenden Schritte aus, wenn der Journalservice nicht kontrolliert beendet wurde oder wenn die Journaldatenbank durch andere Ursachen nicht kontrolliert offline gesetzt wurde.

1. Stoppen Sie den Journalservice (falls er aktiv ist).
2. Löschen Sie die beschädigte Journaldatenbank.
3. Starten Sie den Journalservice erneut.
4. Führen Sie eine Teilsicherung aus.

Nachfolgend steht ein Beispiel, bei dem die Journaldatenbank beim Verlassen nicht gelöscht wird:

```
preserveDBonExit=1
```

Einstellung `deferFSMonStart`

Diese Einstellung verzögert in folgenden Fällen den Versuch, mit der Überwachung eines Dateisystems zu beginnen:

- Wenn das angegebene Journaled File System nicht gültig oder nicht verfügbar ist.
- Das Journalverzeichnis für das angegebene Journaled File System ist nicht im Zugriff oder kann nicht erstellt werden.

Die Überprüfung der Ressourcen findet in den Intervallen statt, die Sie über die Einstellung `deferRetryInterval` angeben.

Der Wert 1 gibt an, dass die Einstellung aktiviert ist. Der Wert 0 gibt an, dass die Einstellung inaktiviert ist. Standardwert ist 0.

Einstellung *deferRetryInterval*

Diese Einstellung gibt das Zeitintervall in Sekunden an, nach dem verzögerte Dateisysteme mit aktivierter Einstellung *deferRetryInterval* auf ihre Verfügbarkeit geprüft und in den Status 'online' versetzt werden. Der Standardwert ist 5 Sekunden.

Einstellung *logFSErrors*

Der Wert 1 besagt, dass alle Fehler protokolliert werden sollen, die beim Zugriff auf ein Journaled File System oder Journalverzeichnis festgestellt wurden. Der Wert Null besagt, dass das Protokollieren von Fehlern, die beim Überprüfen verzögerter Dateisysteme und Journalverzeichnisse festgestellt wurden, unterdrückt wird. Dies wird normalerweise zusammen mit der Einstellung *deferFSMonStart* verwendet, um zu verhindern, dass sehr viele Nachrichten Dateisystem nicht verfügbar in die Protokolle geschrieben werden, wenn ein Journaled File System verzögert in den Status 'online' versetzt wird. Der Standardwert ist 1 (alle Fehler protokollieren).

Zugehörige Konzepte:

„Zeilengruppen überschreiben“ auf Seite 90

„Zeilengruppe 'JournaledFileSystems.Extended'“

Zeilengruppe 'JournaledFileSystems.Extended':

Die Zeilengruppe 'JournaledFileSystems.Extended' überschreibt alle Dateisysteme, die in der Zeilengruppe 'JournaledFileSystems' enthalten sind. Außerdem hebt sie die von der Zeilengruppe 'JournaledFileSystems' auferlegte Begrenzung auf 1023 Zeichen auf.

Falls Sie in die Zeilengruppe 'JournaledFileSystems' Dateisysteme einschließen, sind in dieser Zeilengruppe maximal 1023 Zeichen zulässig. Bei umfangreichen Konfigurationen mit vielen Dateisystemen reicht die Begrenzung auf 1023 Zeichen nicht aus, um alle Dateisysteme anzugeben. Wenn Sie mehr als 1023 Zeichen benötigen, um alle Dateisysteme angeben zu können, die Sie in journalbasierte Sicherungen einschließen wollen, geben Sie die Dateisysteme in der Zeilengruppe 'JournaledFileSystems.Extended' an. Für diese erweiterte Zeilengruppe ist die Beschränkung auf 1023 Zeichen nicht gültig. Werte in der Zeilengruppe 'JournaledFileSystems.Extended' überschreiben alle Werte, die in der anderen Zeilengruppe angegeben sind. Falls ein Dateisystem sowohl in der Zeilengruppe 'JournaledFileSystems' als auch in der Zeilengruppe 'JournaledFileSystems.Extended' angegeben ist, wird das Dateisystem in der Zeilengruppe 'JournaledFileSystems' ignoriert.

Die Syntax für die Zeilengruppe 'JournaledFileSystems.Extended' hat das Format einer einfachen Liste. Damit die von Ihnen gewünschten Dateisysteme bei den journalbasierten Sicherungen eingeschlossen werden, editieren Sie die Konfigurationsdatei des Journaldämons (ihr Standardname ist `tmsjbbd.ini`).

Syntax für die Zeilengruppe *JournaledFileSystems.Extended*:

[*JournaledFileSystems.Extended*]

Syntax für Zeilengruppeneinstellungen:

```
/Dateisystem_1  
/Dateisystem_2  
.  
.  
/Dateisystem_n
```

Nehmen Sie in die Liste alle Dateisysteme auf, die in der journalbasierten Sicherung eingeschlossen sein sollen.

Zeilengruppen überschreiben

Jede beliebige Einstellung in der Zeilengruppe **JournaledFileSystemSettings** kann für ein bestimmtes Journaled File System überschrieben werden, indem eine Überschreibungszeilengruppe erstellt wird.

HookFileName

Damit das Journal mit der Überwachung eines Dateisystems beginnt, muss es den Namen einer vorhandenen Datei in diesem Dateisystem kennen. Diese Einstellung gibt eine vorhandene Datei an. Der Zugriff auf diese Datei wird dann als Test verwendet, um zu sehen, ob dieses Dateisystem online ist. (Die Systemdefinition 'angehängt' kann nicht verwendet werden, da wir die Verwendung virtueller Mountpunkte im Client für Sichern/Archivieren zulassen. Dies bedeutet, dass das System des Clients für Sichern/Archivieren ein Verzeichnis als (virtuelles) Dateisystem behandeln kann).

Deshalb muss, wenn dieses Dateisystem angehängt und abgehängt werden kann, ein Eintrag für **HookFileName** zur Verfügung gestellt werden.

Wird kein Eintrag für **HookFileName** eingegeben, versucht der Journaldämon, eine temporäre Datei im höchsten Verzeichnis zu erstellen, sie für den Beginn der Überwachung zu verwenden und sie anschließend zu löschen.

Nachfolgend steht die Syntax für die Zeilengruppe **JournaledFileSystemSettings**:

Syntax für die Zeilengruppe JournaledFileSystemSettings:

[JournaledFileSystemSettings.fs]

Syntax für Zeilengruppeneinstellungen:

JournaledFileSystemSetting=neuer Wert

Der Name der Überschreibungszeilengruppe für /home wäre beispielsweise:

```
JournaledFileSystemSettings./home
HookFileName=/home/doNotDeleteThisFile
```

Clientseitige Datendeduplizierung

Die *Datendeduplizierung* ist eine Methode zur Reduzierung des Speicherbedarfs, indem redundante Daten entfernt werden.

Übersicht

Zwei Datendeduplizierungstypen sind verfügbar: *clientseitige Datendeduplizierung* und *serverseitige Datendeduplizierung*.

Als *clientseitige Datendeduplizierung* wird ein Datendeduplizierungsverfahren bezeichnet, das der Client für Sichern/Archivieren verwendet, um bei der Sicherungs- und Archivierungsverarbeitung redundante Daten zu entfernen, bevor die Daten an den IBM Spectrum Protect-Server übertragen werden. Durch die clientseitige Datendeduplizierung kann das Datenvolumen reduziert werden, das über ein lokales Netz gesendet wird.

Unter *serverseitiger Datendeduplizierung* versteht man ein Datendeduplizierungsverfahren, das der Server durchführt. Der IBM Spectrum Protect-Administrator kann die zu verwendende Position für die Datendeduplizierung (Client oder Server) mit dem Parameter **DEDUP** im Serverbefehl **REGISTER NODE** oder **UPDATE NODE** angeben.

Erweiterungen

Mit der clientseitigen Deduplizierung von Daten haben Sie folgende Möglichkeiten:

- Bestimmte Dateien auf einem Client von der Deduplizierung von Daten ausschließen.
- Einen Cache für die Deduplizierung von Daten aktivieren, der den Datenaustausch im Netz zwischen dem Client und dem Server reduziert. Der Cache enthält Bereiche, die in vorherigen Teilsicherungsoperationen an den Server gesendet wurden. Anstatt den Server nach dem Vorhandensein eines Bereichs abzufragen, fragt der Client seinen Cache ab.

Eine Größe und Position für einen Client-Cache angeben. Wird eine Inkonsistenz zwischen dem Server und dem lokalen Cache festgestellt, wird der lokale Cache entfernt und erneut gefüllt.

Anmerkung: Für Anwendungen, die die IBM Spectrum Protect-API verwenden, darf der Datendeduplizierungscache wegen möglicher Sicherheitsfehler nicht verwendet werden, die verursacht werden, wenn der Cache nicht mit dem IBM Spectrum Protect-Server synchron ist. Wenn mehrere, gleichzeitig ablaufende Sitzungen des Clients für Sichern/Archivieren konfiguriert sind, muss für jede Sitzung ein separater Cache konfiguriert werden.

- Sowohl die clientseitige Deduplizierung von Daten als auch die Komprimierung aktivieren, um das vom Server gespeicherte Datenvolumen zu reduzieren. Jeder Bereich wird komprimiert, bevor er an den Server gesendet wird. Der Kompromiss liegt zwischen Speichereinsparungen und der Verarbeitungsleistung, die zum Komprimieren der Clientdaten erforderlich ist. Im Allgemeinen gilt: Wenn Sie Daten auf dem Clientsystem komprimieren und deduplizieren, ist etwa zweimal so viel Verarbeitungsleistung wie für die Deduplizierung von Daten allein erforderlich.

Der Server kann mit deduplizierten, komprimierten Daten arbeiten. Außerdem können Clients für Sichern/Archivieren vor Version 6.2 deduplizierte, komprimierte Daten zurückschreiben.

Bei der clientseitigen Datendeduplizierung wird der folgende Prozess verwendet:

- Der Client erstellt Bereiche. *Bereiche* sind Abschnitte von Dateien, die mit anderen Dateibereichen verglichen werden, um Duplikate festzustellen.
- Der Client und der Server arbeiten zusammen, um doppelte Bereiche zu identifizieren. Der Client sendet Bereiche, die nicht doppelt sind, an den Server.
- Nachfolgende Deduplizierungsoperationen für Clientdaten erstellen neue Bereiche. Einige oder alle dieser Bereiche können mit den Bereichen übereinstimmen, die in vorherigen Deduplizierungsoperationen für Daten erstellt und an den Server gesendet wurden. Übereinstimmende Bereiche werden nicht erneut an den Server gesendet.

Vorteile

Die clientseitige Deduplizierung von Daten bietet mehrere Vorteile:

- Sie kann das über das lokale Netz (LAN) gesendete Datenvolumen reduzieren.
- Die zum Identifizieren doppelter Daten erforderliche Verarbeitungsleistung wird vom Server auf Clientknoten verlagert. Die serverseitige Deduplizierung von Daten ist für Speicherpools, die für die Deduplizierung aktiviert sind, immer aktiviert. Dateien, die sich in den Speicherpools befinden, die für die Deduplizierung aktiviert sind, und die vom Client dedupliziert wurden, erfordern jedoch keine zusätzliche Verarbeitung.

- Die zum Entfernen doppelter Daten auf dem Server erforderliche Verarbeitungsleistung wird eliminiert. Dadurch werden Speichereinsparungen auf dem Server sofort wirksam.

Die clientseitige Deduplizierung von Daten hat einen möglichen Nachteil. Der Server verfügt erst dann über vollständige Kopien von Clientdateien, *wenn* Sie die primären Speicherpools, die die clientseitigen Bereiche enthalten, in einem nicht deduplizierten Kopierspeicherpool sichern. (*Bereiche* sind Teile einer Datei, die während des Prozesses für die Deduplizierung von Daten erstellt werden.) Während der Speicherpoolsicherung in einem nicht deduplizierten Speicherpool werden clientseitige Bereiche in aneinandergrenzenden Dateien neu erstellt.

Standardmäßig müssen primäre Speicherpools mit sequenziellem Zugriff, die für die Deduplizierung von Daten definiert sind, in nicht deduplizierten Kopierspeicherpools gesichert werden, bevor sie zurückgefordert und doppelte Daten entfernt werden können. Mit dem Standardwert wird sichergestellt, dass der Server immer über Kopien vollständiger Dateien in einem primären Speicherpool oder einem Kopierspeicherpool verfügt.

Wichtig: Um das Datenvolumen noch weiter zu reduzieren, können Sie gleichzeitig die clientseitige Datendeduplizierung und die Komprimierung aktivieren. Jeder Bereich wird komprimiert, bevor er an den Server gesendet wird. Durch Komprimierung wird Speicherbereich eingespart, jedoch die Verarbeitungszeit auf der Client-Workstation verlängert.

In einem für die Datendeduplizierung aktivierten Speicherpool (Dateipool) wird nur eine einzige Instanz eines Datenbereichs aufbewahrt. Andere Instanzen desselben Datenbereichs werden durch einen Zeiger auf die aufbewahrte Instanz ersetzt.

Ist die clientseitige Datendeduplizierung aktiviert und verfügt der Server über keinen weiteren Speicherbereich im Zielpool, wobei ein nächster Pool definiert ist, stoppt der Server die Transaktion. Der Client für Sichern/Archivieren wiederholt die Transaktion ohne clientseitige Datendeduplizierung. Zur Behebung des Problems muss der IBM Spectrum Protect-Administrator dem ursprünglichen Dateipool weitere Arbeitsdatenträger hinzufügen oder die Operation ohne Aktivierung der Deduplizierung wiederholen.

Zur Verwendung der clientseitigen Datendeduplizierung muss der IBM Spectrum Protect-Server Version 6.2 oder höher haben.

Voraussetzungen

Bei der Konfiguration der clientseitigen Datendeduplizierung müssen die folgenden Voraussetzungen erfüllt sein:

- Der Client und Server müssen die Version 6.2.0 oder eine höhere Version haben. Es sollte immer die letzte Wartungsversion verwendet werden.
- Wenn ein Client eine Datei sichert oder archiviert, werden die Daten in den primären Speicherpool geschrieben, der durch die Kopiengruppe der Verwaltungsklasse angegeben wird, die an die Daten gebunden ist. Zum Deduplizieren der Clientdaten muss der primäre Speicherpool ein Plattenspeicherpool mit sequenziellem Zugriff (FILE) oder ein Containerspeicherpool sein, der für die Datendeduplizierung aktiviert ist.
- Für die Option DEDUPLICATION auf dem Client muss YES definiert sein. Sie können die Option DEDUPLICATION in der Clientoptionsdatei, im Profileditor der GUI des Clients für Sichern/Archivieren oder in der Clientoptionsgruppe auf dem

IBM Spectrum Protect-Server definieren. Verwenden Sie den Befehl **DEFINE CLIENTOPT**, um die Option **DEDUPLICATION** in einer Clientoptionsgruppe zu definieren. Um zu verhindern, dass der Client den Wert in der Clientoptionsgruppe überschreibt, geben Sie **FORCE=YES** an.

- Die clientseitige Deduplizierung von Daten muss auf dem Server aktiviert sein. Um die clientseitige Deduplizierung von Daten zu aktivieren, verwenden Sie den Parameter **DEDUPLICATION** im Serverbefehl **REGISTER NODE** oder **UPDATE NODE**. Setzen Sie den Wert des Parameters auf **CLIENTORSERVER**.
- Stellen Sie sicher, dass Dateien auf dem Client nicht von der clientseitigen Deduplizierung von Daten ausgeschlossen sind. Standardmäßig sind alle Dateien eingeschlossen. Sie können wahlweise bestimmte Dateien mit der Clientoption **exclude.dedup** von der clientseitigen Datendeduplizierung ausschließen.
- Dateien auf dem Client dürfen nicht verschlüsselt sein. Verschlüsselte Dateien und Dateien aus verschlüsselten Dateisystemen können nicht dedupliziert werden.
- Dateien müssen größer als 2 KB und Transaktionen unter dem mit der Option **CLIENTDEDUPTXNLIMIT** angegebenen Wert liegen. Dateien mit einer Größe von 2 KB oder weniger werden nicht dedupliziert.

Der Server kann die maximale Transaktionsgröße für die Datendeduplizierung durch Definieren der Option **CLIENTDEDUPTXNLIMIT** auf dem Server begrenzen. Weitere Informationen zu dieser Option finden Sie in der Dokumentation zum IBM Spectrum Protect-Server.

Die folgenden Operationen haben Vorrang vor der clientseitigen Datendeduplizierung:

- LAN-unabhängige Datenversetzung
- Simultane Schreiboperationen
- Datenverschlüsselung

Wichtig: Planen oder aktivieren Sie keine dieser Operationen während der clientseitigen Datendeduplizierung. Wird eine dieser Operationen während der clientseitigen Datendeduplizierung ausgeführt, wird die clientseitige Datendeduplizierung inaktiviert und es wird eine Nachricht in das Fehlerprotokoll geschrieben.

Die Einstellung auf dem Server legt letztendlich fest, ob die clientseitige Datendeduplizierung aktiviert ist. Siehe Tabelle 26.

Tabelle 26. Datendeduplizierungseinstellungen: Client und Server

Wert der Clientoption DEDUPLICATION	Einstellung auf dem Server	Position für die Datendeduplizierung
Yes	Entweder auf dem Server oder auf dem Client	Client
Yes	Nur auf dem Server	Server
No	Entweder auf dem Server oder auf dem Client	Server
No	Nur auf dem Server	Server

Verschlüsselte Dateien

Der IBM Spectrum Protect-Server und der Client für Sichern/Archivieren können keine verschlüsselten Dateien deduplizieren. Wird während der Datendeduplizie-

rungsverarbeitung eine verschlüsselte Datei entdeckt, wird die Datei nicht dedupliziert und eine Nachricht wird protokolliert.

Tipp: Sie müssen verschlüsselte Dateien und Dateien, die für die clientseitige Deduplizierung von Daten ausgewählt werden können, nicht separat verarbeiten. Beide Typen von Dateien können in derselben Operation verarbeitet werden. Sie werden jedoch in verschiedenen Transaktionen an den Server gesendet.

Als Sicherheitsvorkehrung können Sie einen oder mehrere der folgenden Schritte ausführen:

- Aktivieren Sie die Speichereinheitenverschlüsselung zusammen mit der clientseitigen Deduplizierung von Daten.
- Verwenden Sie die clientseitige Deduplizierung von Daten nur für Knoten, die sicher sind.
- Sind Sie sich bezüglich der Netzsicherheit nicht sicher, aktivieren Sie Secure Sockets Layer (SSL).
- Sollen bestimmte Objekte (beispielsweise Imageobjekte) nicht von der clientseitigen Deduplizierung von Daten verarbeitet werden, können Sie sie auf dem Client ausschließen. Wird ein Objekt von der clientseitigen Deduplizierung von Daten ausgeschlossen und an einen Speicherpool gesendet, der für die Deduplizierung von Daten definiert ist, wird das Objekt auf dem Server dedupliziert.
- Verwenden Sie den Befehl **SET DEDUPVERIFICATIONLEVEL**, um mögliche Sicherheitsattacken auf den Server während der clientseitigen Deduplizierung von Daten festzustellen. Mit diesem Befehl können Sie einen Prozentsatz von Clientbereichen angeben, die vom Server geprüft werden sollen. Wenn der Server eine mögliche Sicherheitsattacke feststellt, wird eine Nachricht angezeigt.

Zugehörige Tasks:

„Client für die Datendeduplizierung konfigurieren“

Zugehörige Verweise:

„Deduplication“ auf Seite 394

„Exclude-Optionen“ auf Seite 438

„Dedupcachepath“ auf Seite 393

„Dedupcachesize“ auf Seite 394

„Enablededupcache“ auf Seite 426

„Ieobjtype“ auf Seite 467

Client für die Datendeduplizierung konfigurieren

Konfigurieren Sie den Client so, dass Sie die Datendeduplizierung beim Sichern und Archivieren Ihrer Dateien verwenden können.

Vorbereitende Schritte

Stellen Sie vor dem Konfigurieren des Clients für die Datendeduplizierung sicher, dass die Voraussetzungen erfüllt sind, die in „Clientseitige Datendeduplizierung“ auf Seite 90 aufgelistet sind:

- Der Server muss den Client mit dem Parameter **DEDUP=CLIENTORSERVER** im Befehl **REGISTER NODE** oder **UPDATE NODE** für die clientseitige Datendeduplizierung aktivieren.
- Der Zielspeicherpool für die Daten muss ein Speicherpool sein, der für die Datendeduplizierung aktiviert ist.

- Stellen Sie sicher, dass Ihre Dateien an die korrekte Verwaltungsklasse gebunden sind.
- Die Dateien müssen größer als 2 KB sein.

Eine Datei kann von der Verarbeitung für die clientseitige Datendeduplizierung ausgeschlossen sein. Standardmäßig sind alle Dateien eingeschlossen. Weitere Informationen finden Sie in der Beschreibung der Option `exclude.dedup`.

Der Server kann die maximale Transaktionsgröße für die Datendeduplizierung durch Definieren der Option `CLIENTDEDUPTXNLIMIT` auf dem Server begrenzen.

Vorgehensweise

Verwenden Sie zur Aktivierung der Datendeduplizierung auf dem Client eine der folgenden Methoden:

Option	Bezeichnung
Clientoptionsdatei bearbeiten	<ul style="list-style-type: none"> • Fügen Sie die Option <code>deduplication yes</code> der Datei <code>dsm.sys</code> hinzu.
Profileditor	<ol style="list-style-type: none"> 1. Klicken Sie im IBM Spectrum Protect-Fenster auf Editieren > Clientvorgaben. 2. Klicken Sie auf Deduplizierung. 3. Wählen Sie das Kontrollkästchen Deduplizierung aktivieren aus. 4. Klicken Sie auf OK, um Ihre ausgewählten Einträge zu sichern und den Profileditor zu schließen.

Ergebnisse

Nachdem Sie den Client für die Datendeduplizierung konfiguriert haben, starten Sie eine Sicherungs- oder Archivierungsoperation. Wenn die Operation beendet ist, zeigt der Sicherungs- oder Archivierungsbericht das Datenvolumen an, das in dieser Operation dedupliziert wurde, sowie die Anzahl der von der clientseitigen Datendeduplizierung verarbeiteten Dateien.

Wenn nicht genügend Plattenspeicherplatz für die Sicherungs- oder Archivierungsoperation zur Verfügung steht, können Sie die clientseitige Datendeduplizierung ohne lokalen Datendeduplizierungscache aktivieren. Gehen Sie dabei wie folgt vor:

1. Fügen Sie die Option `deduplication yes` der Clientoptionsdatei hinzu.
 - Fügen Sie die Option `deduplication yes` der Datei `dsm.sys` hinzu. Sie können diese Option auch in der GUI definieren.
2. Inaktivieren Sie den lokalen Datendeduplizierungscache. Führen Sie hierfür einen der folgenden Schritte aus:
 - Fügen Sie die Option `ENABLEDEDUPCACHE NO` der Datei `dsm.sys` hinzu.
 Sie können diese Option auch im Profileditor des Clients für Sichern/Archivieren definieren, indem Sie das Kontrollkästchen **Deduplizierungscache aktivieren** abwählen.

Beispiel

Im folgenden Beispiel wird der Befehl `'query session'` verwendet, um die Datentypen anzuzeigen, die für die Datendeduplizierung verarbeitet wurden.

```
Protect> q sess
IBM Spectrum Protect-Serververbindungsinformationen

Servername.....: SERVER1
Servertyp.....: Windows
Schutz der Archivaufbewahrung: "Nein"
Serverversion.....: Ver. 6, Rel. 2, Stu. 0.0
Datum des letzten Zugriffs...: 25.08.2009 13:38:18
Sicherungsdateien löschen....: "Nein"
Archivierungsdateien löschen.: "Ja"
Deduplizierung.....: "Client oder Server"

Knotenname.....: AVI
Benutzername.....:
```

Im folgenden Beispiel wird der Befehl 'query management class' verwendet, um die Datentypen anzuzeigen, die für die Datendeduplizierung verarbeitet wurden.

```
Protect> q mgmt -det
Domänenname : DEDUP
Aktivierte Maßnahmengruppe : DEDUP
Aktivierungsdatum/-zeit : 24.08.2009 07:26:09
Standardverwaltungs-klasse : DEDUP
Aufbewahrungszeitraum für Sicherung : 30 Tag(e)
Aufbewahrungszeitraum für Archivierung: 365 Tag(e)
```

```
Verw.-Klasse: DEDUP
Beschreibung: dedup - Standardwerte
Speicherverwaltungsverfahren: Keine
Auto-Umlagerung bei Nichtbenutzung: 0
Sicherung vor Umlagerung erforderlich: JA
Ziel für umgelagerte Dateien: SPACEMGPOOL
Kopiengruppe
Kopiengruppenname.....: STANDARD
Kopienart.....: Sichern
Kopienhäufigkeit.....: 0 Tag(e)
Versionen bestehender Daten: 2 Version(en)
Versionen gelöschter Daten: 1 Version(en)
Extraversionen aufbewahren: 30 Tag(e)
Einzigste Version aufbewahren: 60 Tag(e)
Kopiennummerierung.....: Gemeinsam statisch
Kopienmodus.....: Geändert
Kopienziel.....: AVIFILEPOOL
LAN-unabhängiges Ziel..: NEIN
Daten deduplizieren.....: JA
```

```
Kopiengruppenname.....: STANDARD
Kopienart.....: Archivieren
Kopienhäufigkeit.....: Cmd
Version aufbewahren....: 365 Tag(e)
Kopiennummerierung.....: Gemeinsam statisch
Kopienmodus.....: Absolut
Aufbewahrungsstart.....: Erstellen
Mindestaufbewahrung....: 65534 Tag(e)
Kopienziel.....: FILEPOOL
LAN-unabhängiges Ziel..: NEIN
Daten deduplizieren.....: JA
```

ANS1900I Rückkehrcode ist 0.

Zugehörige Konzepte:

„Clientseitige Datendeduplizierung“ auf Seite 90

Zugehörige Verweise:

„Deduplication“ auf Seite 394

„Enablededupcache“ auf Seite 426

„Exclude-Optionen“ auf Seite 438

➡ Option CLIENTDEDUPTXNLIMIT

➡ Befehl REGISTER NODE

➡ Befehl UPDATE NODE

Dateien bei der Datendeduplizierung ausschließen

Sie können eine Datei bei der Datendeduplizierung während der Sicherungs- oder Archivierungsverarbeitung ausschließen.

Informationen zu diesem Vorgang

Sie können nur Dateien bei der Deduplizierung von Archivierungsdaten ausschließen. Sie können Dateien und Images (soweit zutreffend) bei der Deduplizierung von Sicherungsdaten ausschließen.

Vorgehensweise

Sollen bestimmte Dateien bei der clientseitigen Datendeduplizierung nicht verarbeitet werden, können Sie diese über die GUI bei der Datendeduplizierungsverarbeitung ausschließen:

1. Klicken Sie auf **Editieren > Clientvorgaben**.
2. Klicken Sie auf die Registerkarte **Einschluss/Ausschluss**.
3. Klicken Sie auf **Hinzufügen**, um das Fenster **Include/Exclude-Optionen definieren** zu öffnen.
4. Wählen Sie eine Kategorie für die Verarbeitung aus.
 - Um eine Datei bei der Datendeduplizierung während der Archivierungsverarbeitung auszuschließen, wählen Sie **Archivieren** in der Liste **Kategorie** aus.
 - Um eine Datei bei der Datendeduplizierung während der Sicherungsverarbeitung auszuschließen, wählen Sie **Sichern** in der Liste **Kategorie** aus.
5. Wählen Sie **Exclude.Dedup** in der Liste **Typ** aus.
6. Wählen Sie einen Eintrag in der Liste **Objekttyp** aus.
 - Für die Archivierungsverarbeitung ist nur der Objekttyp **Datei** verfügbar.
 - Für die Sicherungsverarbeitung wählen Sie einen der folgenden Objekttypen aus:
 - **Datei**
 - **Image**
7. Geben Sie eine Datei oder ein Muster im Feld **Datei oder Muster** an. Sie können Platzhalterzeichen verwenden. Wenn Sie die Datei oder das Muster nicht eingeben wollen, klicken Sie auf **Durchsuchen**, um ein Auswahlfenster zu öffnen und eine Datei auszuwählen. Für angehängte Dateibereiche können Sie den Verzeichnismountpunkt im Auswahlfenster auswählen.
8. Klicken Sie auf **OK**, um das Fenster 'Include/Exclude-Optionen definieren' zu schließen. Die Ausschlussoptionen, die Sie definiert haben, befinden sich in einer Exclude-Anweisung unten im Listenfeld für Anweisungen auf der Registerkarte **Vorgaben für Einschluss/Ausschluss**.
9. Klicken Sie auf **OK**, um Ihre ausgewählten Einträge zu sichern und den Profilditor zu schließen.

Nächste Schritte

Sie können auch Dateien von der Datendeduplizierungsverarbeitung ausschließen, indem Sie die Datei `dsm.sys` editieren:

1. Fügen Sie die Option `deduplication yes` hinzu.
2. Die Dateien in einem Verzeichnis von der Datendeduplizierung ausschließen. Sollen beispielsweise die Dateien im Verzeichnis `/Users/Administrator/Documents/Taxes/` ausgeschlossen werden, fügen Sie die folgende Anweisung hinzu: `EXCLUDE.dedup /Users/Administrator/Documents/Taxes/.../*`
3. Clientseitige Datendeduplizierung für die Imagesicherung eines Dateisystems ausschließen. Soll beispielsweise das Dateisystem `/home` ausgeschlossen werden, fügen Sie die folgende Anweisung hinzu: `EXCLUDE.DEDUP /home/*/*`
`IEOBJTYPE=Image`

Wichtig: Wird ein Objekt an einen Datendeduplizierungspool gesendet, wird die Datendeduplizierung auf dem Server ausgeführt, selbst wenn das Objekt von der clientseitigen Datendeduplizierung ausgeschlossen ist.

Zugehörige Konzepte:

„Clientseitige Datendeduplizierung“ auf Seite 90

Zugehörige Verweise:

„Deduplication“ auf Seite 394

„Enablededupcache“ auf Seite 426

„Exclude-Optionen“ auf Seite 438

Konfiguration und Verwendung der automatisierten Clientübernahme

Wenn der IBM Spectrum Protect-Server nicht verfügbar ist, kann eine automatische Übernahme des Clients für Sichern/Archivieren auf einem Sekundärserver zum Zweck der Datenwiederherstellung stattfinden. Sie können in der Konfiguration des Clients die automatisierte Übernahme angeben oder eine Übernahme des Clients unterbinden. Außerdem können Sie den Replikationsstatus Ihrer Daten auf dem Sekundärserver bestimmen, bevor Sie die replizierten Daten zurückschreiben oder abrufen.

Zugehörige Tasks:

„Daten während einer Übernahme zurückschreiben oder abrufen“ auf Seite 257

Automatisierte Clientübernahme - Übersicht

Bei einem Ausfall auf dem IBM Spectrum Protect-Server kann eine automatische Übernahme des Clients für Sichern/Archivieren auf einem Sekundärserver zum Zweck der Datenwiederherstellung stattfinden.

Der IBM Spectrum Protect-Server, zu dem der Client während der normalen Produktionsprozesse eine Verbindung herstellt, wird als *Primärserver* bezeichnet. Wenn der Primärserver und die Clientknoten für die Knotenreplikation konfiguriert sind, wird dieser Server auch als *Quellenreplikationsserver* bezeichnet.

Die Clientdaten auf dem Quellenreplikationsserver können auf einem anderen IBM Spectrum Protect-Server, dem *Zielreplikationsserver*, repliziert werden. Dieser Server wird auch als *Sekundärserver* bezeichnet, auf dem eine automatische Übernahme des Clients stattfindet, wenn der Primärserver ausfällt.

Damit eine automatische Übernahme des Clients auf dem Sekundärserver stattfinden kann, müssen dem Client die Verbindungsinformationen für diesen Server zur

Verfügung gestellt werden. Während des Normalbetriebs werden die Verbindungsinformationen für den Sekundärserver im Verlauf des Anmeldeprozesses automatisch vom Primärserver an den Client gesendet. Die Daten des Sekundärservers werden automatisch in der Clientoptionsdatei gespeichert. Es ist kein manueller Eingriff des Benutzers erforderlich, um die Daten für diesen Server hinzuzufügen.

Der Client versucht bei jeder Anmeldung am Server eine Verbindung zum Primärserver herzustellen. Wenn der Primärserver nicht verfügbar ist, findet automatisch eine Übernahme des Clients auf dem Sekundärserver statt und zwar gemäß den Informationen zum Sekundärserver in der Clientoptionsdatei.

In diesem Übernahmemodus können Sie alle replizierten Clientdaten zurückschreiben oder abrufen. Wenn der Primärserver wieder online ist, wird der Client bei seinem nächsten Start automatisch wieder auf den Primärserver zurückgesetzt.

Der folgende Beispieltext zeigt die Verbindungsinformationen des Sekundärservers, die an den Client gesendet und in der Clientsystemoptionsdatei (dsm.sys) gespeichert werden:

```
*** Diese Optionen sollten nicht manuell geändert werden
REPLSERVERNAME          TARGET
REPLTCPSERVERADDRESS 192.0.2.9
REPLTCPSPORT          1501
REPLSSLPORT           1502
REPLSERVERGUID         60.4a.c3.e1.85.ba.11.e2.af.ce.00.0c.29.2f.07.d3

MYREPLICATIONServer TARGET
*** Ende der automatisch aktualisierten Optionen
```

Voraussetzungen für die automatisierte Clientübernahme

Bevor Sie den Client für die automatisierte Clientübernahme konfigurieren oder verwenden, müssen der Client für Sichern/Archivieren und der IBM Spectrum Protect-Server mehrere Voraussetzungen erfüllen.

Stellen Sie sicher, dass der Client die folgenden Voraussetzungen für die automatisierte Clientübernahme erfüllt:

- Auf dem Primärserver, dem Sekundärserver und dem Client für Sichern/Archivieren muss IBM Spectrum Protect Version 7.1 oder eine höhere Version ausgeführt werden.
- Der Primärserver und der Sekundärserver müssen für die Knotenreplikation konfiguriert sein.
- Der Clientknoten muss mithilfe des Serverbefehls REGISTER NODE REPLSTATE=ENABLED oder UPDATE NODE REPLSTATE=ENABLED für die Knotenreplikation auf dem Quellenreplikationsserver konfiguriert sein.
- Die automatisierte Clientübernahme ist auf dem Client standardmäßig aktiviert. Ist jedoch die Option usereplicationfailover no in der Clientoptionsdatei angegeben, geben Sie entweder hier den Wert yes an oder entfernen Sie die Option.
- Die Clientoptionsdatei muss gültige Verbindungsinformationen für den Sekundärserver enthalten. Während des Normalbetriebs werden diese Informationen automatisch vom Primärserver an den Client gesendet.
- Um die vom Primärserver gesendeten Verbindungsinformationen des Sekundärservers speichern zu können, benötigt der Client Schreibzugriff auf die Datei dsm.opt (Windows-Clients) bzw. die Datei dsm.sys (AIX-, Linux-, Mac OS X- und Oracle Solaris-Clients). Wenn der Client keinen Schreibzugriff auf diese Dateien hat, werden die Informationen des Sekundärservers nicht in der Clientoptionsdatei gespeichert und ein Fehler wird im Fehlerprotokoll hinzugefügt.

- Benutzer ohne Rootberechtigung können die Standardposition für die Knotenreplikationstabelle nicht verwenden. Sie müssen die Option **nrtablepath** in die Datei `dsm.sys` einfügen, um eine andere Position anzugeben. Weitere Informationen finden Sie in „Nrtablepath“ auf Seite 520.
- Bevor die Verbindungsinformationen des Sekundärservers an die Optionsdatei gesendet werden, müssen die folgenden Prozesse stattfinden:
 - Der Client muss mindestens einmal auf dem Quellenreplikationsserver gesichert werden.
 - Der Clientknoten muss mindestens einmal auf dem Zielreplikationsserver repliziert werden.
- Die Übernahme erfolgt für Clientknoten, die mit der Unterstützung für den Clientknoten-Proxy gesichert werden, wenn sowohl der Ziel- als auch der Agentenknoten für die Replikation auf dem Zielreplikationsserver konfiguriert ist. Wenn der Zielknoten explizit repliziert wird, wird auch der Agentenknoten zusammen mit der Proxy-Beziehung implizit auf dem Zielreplikationsserver repliziert.
 Beispiel: Node_B wird mit dem folgenden Befehl die Berechtigung zur Ausführung von Clientoperationen im Namen von Node_A erteilt:
`grant proxynode target=Node_A agent=Node_B`

Ist für beide Knoten die Replikation mit der Option `replstate=enabled` in der Knotendefinition konfiguriert, werden auch Node_B und die Proxy-Beziehung repliziert, wenn Node_A repliziert wird.

Einschränkungen für die automatisierte Clientübernahme

Der folgende Abschnitt enthält Informationen, die den Prozess der automatisierten Clientübernahme und die damit verbundenen Einschränkungen erläutern.

Für die automatisierte Clientübernahme gelten die folgenden Einschränkungen:

- Wenn sich der Client im Übernahmemodus befindet, können Sie keine Funktionen verwenden, für die eine Datenspeicherung auf dem Sekundärserver erforderlich ist (z. B. Sicherungs- oder Archivierungsoperationen). Sie können lediglich Datenwiederherstellungsfunktionen verwenden, z. B. Zurückschreibungs-, Abruf- oder Abfrageoperationen. Sie können auch Clientoptionen bearbeiten und das Kennwort des IBM Spectrum Protect-Clients ändern.
- Zeitpläne werden nicht auf dem Sekundärserver repliziert. Daher werden keine Zeitpläne ausgeführt, während der Primärserver nicht verfügbar ist.
- Nachdem der Client eine Verbindung zum Sekundärserver im Übernahmemodus hergestellt hat, versucht er erst wieder bei der nächsten Erstanmeldung am Server eine Verbindung zum Primärserver herzustellen. Der Client unternimmt nur dann einen Übernahmeversuch auf dem Sekundärserver, wenn die einleitende Verbindung zum Primärserver fehlschlägt. Die einleitende Verbindung ist die erste Verbindung, die der Client zum Server herstellt.

Wenn der Primärserver während einer Clientoperation ausfällt, findet keine Übernahme des Clients auf dem Sekundärserver statt und die Operation schlägt fehl. Sie müssen den Client erneut starten, damit eine Übernahme auf dem Sekundärserver stattfinden kann, und dann die Clientoperation wiederholen.

Zurückschreibungsoperationen, die unterbrochen werden, wenn der Primärserver ausfällt, können nach der Übernahme des Clients nicht erneut gestartet werden. Sie müssen nach der Übernahme des Clients auf dem Sekundärserver die gesamte Zurückschreibungsoperation erneut ausführen.

- Wird das IBM Spectrum Protect-Kennwort vor der Replikation des Clientknotens geändert, wird es zwischen dem Primärserver und dem Sekundärserver nicht synchronisiert. Wenn während dieser Zeit eine Übernahme stattfindet, müssen

Sie das Kennwort auf dem Sekundärserver und auf dem Client manuell zurücksetzen. Wenn der Primärserver wieder online ist, muss das Kennwort zurückgesetzt werden, damit der Client eine Verbindung zum Primärserver herstellen kann.

Wird das Kennwort zurückgesetzt, während eine Verbindung des Clients zum Sekundärserver besteht, muss das Kennwort auf dem Primärserver zurückgesetzt werden, bevor sich der Client am Primärserver anmelden kann. Diese Einschränkung gilt, wenn für die Option **passwordaccess** der Wert **generate** definiert ist oder wenn das Kennwort manuell zurückgesetzt wird.

- Wenn Sie Clientdaten gesichert oder archiviert haben, der Primärserver jedoch ausfällt, bevor er den Clientknoten repliziert, werden die neuesten Sicherungs- bzw. Archivierungsdaten nicht auf dem Sekundärserver repliziert. Der Replikationsstatus des Dateibereichs ist nicht aktuell. Wenn Sie versuchen, die Daten im Übernahmefunktionsmodus zurückzuschreiben oder abzurufen, während der Replikationsstatus nicht aktuell ist, wird in einer Nachricht angezeigt, dass die Daten, die Sie wiederherstellen wollen, nicht auf dem neuesten Stand sind. Sie können mit der Wiederherstellung fortfahren oder warten, bis der Primärserver wieder online ist.
- Wenn auf dem Quellenreplikationsserver eine Benutzer-ID mit Administrator- und Clienteignerberechtigung vorhanden ist und der Name der Benutzer-ID mit dem Namen des Clientknotens identisch ist, wird die Benutzer-ID mit Administratorberechtigung während des Knotenreplikationsprozesses auf dem Server repliziert. Ist eine solche Benutzer-ID auf dem Quellenreplikationsserver nicht vorhanden, wird während des Replikationsprozesses diese Administratordefinition auf dem Zielreplikationsserver nicht erstellt.

Sind dem Knoten andere Benutzer-IDs mit Administratorberechtigung zugeordnet, muss der IBM Spectrum Protect-Administrator die Benutzer-IDs mit Administratorberechtigung auf dem Zielreplikationsserver manuell konfigurieren. Andernfalls kann der Benutzer mit Verwaltungsaufgaben keine Verbindung zum Zielreplikationsserver (Sekundärserver) mit dem Web-Client herstellen.

- Wenn Sie eine Datei von IBM Spectrum Protect zurückschreiben und das Dateisystem von IBM Spectrum Protect for Space Management verwaltet wird, dürfen Sie die Datei nicht als Stubdatei zurückschreiben. Sie müssen die vollständige Datei zurückschreiben. Verwenden Sie die Option `restoremigstate=no`, um die vollständige Datei zurückzuschreiben. Wenn Sie die Datei als Stubdatei vom Zielsystem zurückschreiben, kann dies folgende Konsequenzen haben:
 - Sie können die Datei nicht mithilfe des IBM Spectrum Protect for Space Management-Clients vom IBM Spectrum Protect-Quellensystem zurückrufen.
 - Die Datei verfällt durch den für den IBM Spectrum Protect-Quellensystem ausgeführten IBM Spectrum Protect for Space Management-Abgleichsprozess. Wenn die Datei durch einen Abgleichsprozess verfällt, können Sie die vollständige Datei mithilfe des Clients für Sichern/Archivieren und der Option `restoremigstate=no` zurückschreiben.

Übernahmefunktionalität der IBM Spectrum Protect-Komponenten

IBM Spectrum Protect-Komponenten und -Produkte verwenden den Client für Sichern/Archivieren oder die API für die Sicherung von Daten auf dem IBM Spectrum Protect-Primärserver. Wenn der Primärserver ausfällt, kann eine Übernahme einiger dieser Produkte und Komponenten auf dem Sekundärserver erfolgen, während andere Komponenten nicht übernahmefähig sind.

Weitere Informationen zur Übernahmefunktionalität der IBM Spectrum Protect-Komponenten und -Produkte finden Sie in Technote 1649484.

Zugehörige Tasks:

„Status replizierter Clientdaten bestimmen“ auf Seite 104

Client für automatisierte Übernahme konfigurieren

Sie können durch eine manuelle Konfiguration festlegen, dass eine automatische Übernahme des Clients auf dem Sekundärserver stattfindet.

Vorbereitende Schritte

Vor der Konfiguration:

- Stellen Sie sicher, dass der Clientknoten an der Knotenreplikation auf dem Primärserver beteiligt ist.

Anmerkung: Wenn der Replikationsserver Version 8.1.1 oder früher hat und SSL aktiviert ist, müssen Sie das SSL-Zertifikat manuell mit dem folgenden Befehl auf dem Client installieren: `gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "TSM server STSM01 self-signed key" -file <Zertifikatsdatei> -format ascii` Dabei ist <Zertifikatsdatei> der Pfad zu dem zugehörigen Zertifikat.

- Stellen Sie sicher, dass der Client die Voraussetzungen für die automatisierte Clientübernahme erfüllt.
- Verwenden Sie diese Prozedur nur, wenn die Verbindungsinformationen für den Sekundärserver nicht aktuell oder in der Clientoptionsdatei nicht vorhanden sind.

Informationen zu diesem Vorgang

Eine manuelle Konfiguration des Clients für die automatisierte Übernahme ist in folgenden Situationen denkbar:

- Die Konfiguration des Sekundärservers wurde geändert und der Primärserver fällt aus, bevor sich der Client beim Server anmeldet. Wenn Sie die Verbindungsinformationen manuell hinzufügen, ist eine Übernahme des Clients auf dem Sekundärserver möglich.
- Die Verbindungsinformationen des Sekundärservers in der Clientoptionsdatei wurden versehentlich ganz oder teilweise gelöscht.

Tipp: Anstelle einer manuellen Konfiguration der Clientoptionsdatei können Sie den Befehl `dsmc q session` ausführen, wobei Sie zur Anmeldung beim Primärserver aufgefordert werden. Die Verbindungsinformationen für den Sekundärserver werden automatisch an die Clientoptionsdatei gesendet.

Vorgehensweise

Gehen Sie wie folgt vor, um den Client manuell für die automatisierte Übernahme zu konfigurieren:

1. Stellen Sie sicher, dass die automatisierte Clientübernahme für den Client aktiviert ist, indem Sie dafür sorgen, dass die Option `usereplicationfailover` entweder in der Clientoptionsdatei nicht vorhanden oder auf `yes` gesetzt ist. Die automatisierte Clientübernahme ist auf dem Client standardmäßig aktiviert, daher ist die Option `usereplicationfailover` in der Clientoptionsdatei nicht erforderlich.
2. Bitten Sie den Administrator des IBM Spectrum Protect-Servers um Auskunft über die Verbindungsinformationen des Sekundärservers und fügen Sie diese

Informationen am Anfang der Clientoptionsdatei ein. Gruppieren Sie die Anweisungen in einer Zeilengruppe unter der Anweisung **replservername**.

Fügen Sie beispielsweise die folgenden Anweisungen in die Datei dsm.sys ein:

```
REPLSERVERNAME      TARGET
REPLTCPSERVERADDRESS 192.0.2.9
REPLTCPSPORT        1501
REPLSSLPORT         1502
REPLSERVERGUID      60.4a.c3.e1.85.ba.11.e2.af.ce.00.0c.29.2f.07.d3
```

```
Servename      server_a
COMMMethod      TCPip
TCPPort         1500
TCPServeraddress server_hostname1.example.com
PASSWORDAccess  prompt
MYREPLICATIONServer TARGET
```

- Benutzer ohne Rootberechtigung müssen eine Position für die Knotenreplikationstabelle angeben, indem die Option **nrtblepath** zur Datei dsm.sys hinzugefügt wird. Der Client für Sichern/Archivieren verwendet diese Tabelle für die Speicherung von Informationen zu jeder Sicherungs- oder Archivierungsoperation auf dem IBM Spectrum Protect-Server.

Sie müssen eine Position angeben, für die Ihre Benutzer-ID Schreibzugriff hat.
Beispiel:

```
nrtblepath /Volumes/nrtbl
```

Einschränkung: Geben Sie nicht das Stammverzeichnis (/) als Position der Knotenreplikationstabelle an.

- Speichern und schließen Sie die Clientoptionsdatei.
- Starten Sie die GUI des Clients für Sichern/Archivieren erneut oder melden Sie sich über die Befehlszeilenschnittstelle beim IBM Spectrum Protect-Server an. Der Client ist mit dem Sekundärserver verbunden.

Beispiel

Nachdem Sie die automatisierte Clientübernahme auf dem Client konfiguriert haben und der Client versucht, sich beim Server anzumelden, wird die folgende Beispielbefehlsausgabe angezeigt:

```
IBM Spectrum Protect
Befehlszeilenschnittstelle des Clients für Sichern/Archivieren
  Clientversion 8, Release 1, Stufe 0.0
  Clientdatum/-zeit: 16.12.2016 12:05:35
(c) Copyright IBM Corporation und andere 1990, 2016. Alle Rechte vorbehalten.

Knotenname: MY_NODE_NAME
ANS2106I Verbindung zum primären IBM Spectrum Protect-Server 192.0.2.1 ist
fehlgeschlagen.

ANS2107I Es wird versucht, eine Verbindung zum sekundären Server TARGET
unter 192.0.2.9 : 1501 herzustellen.

Knotenname: MY_NODE_NAME
Sitzung hergestellt mit Server TARGET: Windows
  Serverversion 8, Release 1, Stufe 0.0
  Serverdatum/-zeit: 16.12.2016 12:05:35  Letzter Zugriff: 15.12.2016 09:55:56

Sitzung im Übernahmemodus auf dem sekundären Server aufgebaut
ANS2108I Verbindung zum sekundären Server TARGET hergestellt.
```

Nächste Schritte

Sie können alle replizierten Daten im Übernahmemodus zurückschreiben oder abrufen.

Zugehörige Konzepte:

„Automatisierte Clientübernahme - Übersicht“ auf Seite 98

Zugehörige Tasks:

„Daten während einer Übernahme zurückschreiben oder abrufen“ auf Seite 257

Zugehörige Verweise:

„Forcefailover“ auf Seite 460

„Myreplicationserver“ auf Seite 513

„Nrtablepath“ auf Seite 520

„Replserverguid“ auf Seite 548

„Replservername“ auf Seite 550

„Replsslport“ auf Seite 552

„Repltcpport“ auf Seite 554

„Repltcpserveraddress“ auf Seite 555

„Usereplicationfailover“ auf Seite 626

Status replizierter Clientdaten bestimmen

Bevor Sie Clientdaten vom Sekundärserver zurückschreiben oder abrufen, können Sie prüfen, ob die neueste Sicherung des Clients auf dem Sekundärserver repliziert wurde.

Informationen zu diesem Vorgang

Sie können den Status replizierter Clientdaten abrufen, um festzustellen, ob die neueste Clientsicherung auf dem Sekundärserver repliziert wurde.

Wenn die Zeitmarke der neuesten Sicherungsoperation auf dem Client mit der Zeitmarke der Sicherung auf dem Sekundärserver übereinstimmt, ist der Replikationsstatus aktuell.

Wenn die Zeitmarke der neuesten Sicherungsoperation von der Zeitmarke der Sicherung auf dem Sekundärserver abweicht, ist der Replikationsstatus nicht aktuell. Diese Situation kann eintreten, wenn Sie den Client zwar gesichert haben, der Primärserver aber vor dem Replizieren des Clientknotens ausfällt.

Vorgehensweise

Geben Sie den folgenden Befehl in die Eingabeaufforderung ein, um den Status der replizierten Clientdaten zu bestimmen:

```
dsmc query filespace -detail
```

Die folgende Beispielausgabe zeigt, dass die Zeitmarken auf dem Server und auf dem Client übereinstimmen und dass daher der Replikationsstatus aktuell ist:

Nr.	Datum ltzt	Teilsich.	Typ	FSID	Unicode	Replikation	Dateibereichsname
1	00.00.0000	00:00:00	HFS		9	Yes	Current /
<div> <div>Letztes Speicherdatum</div> <div>Server</div> <div>Lokal</div> </div>							
Sicherungsdaten:				22.04.2013	19:39:17	22.04.2013	19:39:17
Archivierungsdaten:				Kein Datum verfügbar		Kein Datum verfügbar	

Die folgende Beispielausgabe zeigt, dass die Zeitmarken auf dem Server und auf dem Client nicht übereinstimmen und dass daher der Replikationsstatus nicht aktuell ist:

Nr.	Datum ltzt	Teilsich.	Typ	FSID	Unicode	Replikation	Dateibereichsname
1	00.00.0000	00:00:00	HFS		9	Yes	Not Current /
<div> <div>Letztes Speicherdatum</div> <div>Server</div> <div>Lokal</div> </div>							
Sicherungsdaten:				22.04.2013	19:39:17	24.04.2013	19:35:41
Archivierungsdaten:				Kein Datum verfügbar		Kein Datum verfügbar	

Nächste Schritte

Wenn Sie versuchen, die Daten im Übernahmemodus zurückzuschreiben, während der Replikationsstatus nicht aktuell ist, wird in einer Nachricht angezeigt, dass die Daten, die Sie zurückschreiben wollen, nicht auf dem neuesten Stand sind. Sie können mit der Zurückschreibung fortfahren oder warten, bis der Primärserver wieder online ist.

Zugehörige Tasks:

„Daten während einer Übernahme zurückschreiben oder abrufen“ auf Seite 257

Zugehörige Verweise:

„Nrtablepath“ auf Seite 520

Automatisierte Clientübernahme verhindern

Sie können in der Konfiguration des Clients festlegen, dass die automatisierte Clientübernahme auf dem Sekundärserver verhindert werden soll.

Informationen zu diesem Vorgang

Sie können die automatisierte Clientübernahme verhindern, z. B., wenn Sie wissen, dass die Daten auf dem Clientknoten vor dem Ausfall des Primärservers nicht auf dem Sekundärserver repliziert wurden. In diesem Fall wollen Sie verhindern, dass replizierte Daten vom Sekundärserver wiederhergestellt werden, die möglicherweise veraltet sind.

Vorgehensweise

Um eine Übernahme des Clientknotens auf dem Sekundärserver zu verhindern, fügen Sie die folgende Anweisung in die Clientoptionsdatei ein:

```
usereplicationfailover no
```

Diese Einstellung setzt die Konfiguration außer Kraft, die der IBM Spectrum Protect-Serveradministrator auf dem Primärserver angibt.

Ergebnisse

Es findet keine automatische Übernahme des Clientknotens auf dem Sekundärserver statt, wenn er den nächsten Versuch unternimmt, eine Verbindung zum inaktiven Primärserver herzustellen.

Zugehörige Tasks:

„Status replizierter Clientdaten bestimmen“ auf Seite 104

Zugehörige Verweise:

„Usereplicationfailover“ auf Seite 626

Clientübernahme erzwingen

Es kann eine sofortige Übernahme des Clients auf dem Sekundärserver stattfinden, auch wenn der Primärserver betriebsbereit ist. Sie können mit diesem Verfahren beispielsweise prüfen, ob eine Übernahme des Clients auf dem erwarteten Sekundärserver stattfindet.

Vorgehensweise

Gehen Sie wie folgt vor, um eine sofortige Übernahme des Clients auf dem Sekundärserver zu erzwingen:

1. Fügen Sie die Option **forcefailover yes** in die Clientsystemoptionsdatei (dsm.sys) ein.
2. Stellen Sie eine Verbindung zum Sekundärserver her, indem Sie die GUI des Clients für Sichern/Archivieren erneut starten oder indem Sie eine Befehlsitzung mit dem Befehl **dsmc** starten.
3. Optional: Sie können eine Verbindung zum Sekundärserver auch herstellen, indem Sie die Option **-forcefailover=yes** in einem Befehl angeben, anstatt die Optionsdatei zu aktualisieren. Beispiel:
`dsmc q sess -forcefailover=yes`

Nächste Schritte

Sie können mit einer der folgenden Methoden überprüfen, ob eine Verbindung zum Sekundärserver besteht:

- Überprüfen Sie das Feld **Informationen zum sekundären Server** im Fenster **Verbindungsinformationen** in der GUI des Clients für Sichern/Archivieren.
- Überprüfen Sie die Befehlsausgabe, wenn Sie eine Befehlsitzung starten. Der Status des Sekundärservers wird in der Ausgabe angezeigt.

Zugehörige Verweise:

„Forcefailover“ auf Seite 460

Client für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Daten konfigurieren

Bevor Sie Tivoli Storage Manager FastBack-Clientdaten sichern oder archivieren können, müssen Sie Konfigurationstasks ausführen.

Stellen Sie zunächst sicher, dass der Client für Sichern/Archivieren konfiguriert und der Tivoli Storage Manager FastBack-Client installiert wurde.

Installieren Sie den FastBack-Client anhand der Informationen in Tivoli Storage Manager FastBack.

Führen Sie nach der Installation des FastBack-Clients die folgenden Tasks aus:

1. Registrieren Sie einen Knoten für jeden FastBack-Client, auf dem Daten gesichert und archiviert werden. Der Knotenname muss der kurze Hostname des FastBack-Clients sein.

Dies ist eine einmalige Konfiguration, die für jeden FastBack-Client, dessen Datenträger gesichert oder archiviert werden müssen, einmal ausgeführt wird.

Dieser Registrierungsschritt muss nur dann manuell ausgeführt werden, wenn der Client für Sichern/Archivieren als eigenständige Anwendung verwendet wird.

Das Administration Center führt diese Knotenregistrierung automatisch aus, wenn der Benutzer über das Administration Center Zeitpläne für die Archivierung oder Sicherung von FastBack-Daten erstellt. Ab Version 7.1 ist die Komponente 'Administration Center' nicht mehr in Tivoli Storage Manager- oder IBM Spectrum Protect-Verteilungen enthalten.

FastBack-Benutzer, die über ein Administration Center aus einem früheren Server-Release verfügen, können damit weiterhin FastBack-Zeitpläne erstellen und ändern. Wenn noch kein Administration Center installiert ist, können Sie die Vorgängerversion von <ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/admincenter/v6r3/> herunterladen. Wenn kein Administration Center installiert ist, müssen Sie FastBack-Zeitpläne auf dem IBM Spectrum Protect-Server erstellen und ändern. Informationen zur Erstellung von Zeitplänen auf dem Server finden Sie in der Dokumentation für den IBM Spectrum Protect-Server.

2. Erteilen Sie mit dem Serverbefehl **GRANT PROXY** Ihrem aktuellen Knoten des Clients für Sichern/Archivieren Proxy-Berechtigung auf jedem Knoten, der den in Schritt 1 erstellten FastBack-Client darstellt. Der FastBack-Knoten muss das Ziel und der aktuelle Clientknoten der Proxy sein.

Dies ist eine einmalige Konfiguration, die vom Administration Center ausgeführt wird, wenn die Sicherung oder Archivierung vom Administration Center eingeleitet wird.

3. Führen Sie den Befehl **set password** aus, um die Berechtigungsnachweise der FastBack-Repositorys zu speichern, zu denen der Client für Sichern/Archivieren eine Verbindung herstellt. Führen Sie den Befehl `set password -type=fastback` einmal für jedes Repository aus, zu dem der Client für Sichern/Archivieren voraussichtlich eine Verbindung herstellt.

Die gespeicherten Berechtigungsnachweise sind von den folgenden Konfigurationen abhängig:

- Client für Sichern/Archivieren auf dem FastBack-Server
- Client für Sichern/Archivieren auf dem FastBack Disaster Recovery Hub
- Client für Sichern/Archivieren auf einer dedizierten Proxy-Workstation

Informationen zur Integration von IBM Spectrum Protect und Tivoli Storage Manager FastBack finden Sie in Tivoli Storage Manager FastBack und IBM Spectrum Protect integrieren.

Zugehörige Konzepte:

„Installationsvoraussetzungen für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Clientdaten“ auf Seite 10

Zugehörige Verweise:

„Set Password“ auf Seite 820

Konfiguration und Verwendung der Clusterumgebung

Der Begriff *Cluster* hat in unterschiedlichen Umgebungen unterschiedliche Bedeutungen. Er kann Folgendes bedeuten: hoch verfügbar, hohe Leistung, Lastausgleich, Grid-Computing oder eine Kombination all dieser Begriffe.

Es sind derzeit mehrere Clusteringprodukte für UNIX und Linux verfügbar, und in diesem Abschnitt werden diejenigen Aspekte einer Clusteringumgebung definiert, die vorhanden sein müssen, damit diese Sicherungsmethodik korrekt funktioniert. Ein Basisverständnis über die Funktionsweise Ihrer Clustersoftware wird benötigt. Aktivitäten in Bezug auf Clustersoftware wie z. B. die Entwicklung von Anwendungsstart- und -stoppscripts werden in diesem Abschnitt nicht beschrieben.

Eine Clusterumgebung bezieht sich auf eine UNIX- oder Linux-Umgebung, die folgende Merkmale aufweist:

- Platten werden von physischen Workstations gemeinsam genutzt, entweder auf exklusive Weise (zu jedem Zeitpunkt hat nur ein Host Zugriff auf die logische Platte) oder gleichzeitig.
- Platten werden dem Host als lokale Festplatten und nicht als Netzressourcen angezeigt.

Wichtig: Hängen Sie die Dateisysteme lokal an das System an und nicht über ein LAN-gestütztes Dateifreigabeprotokoll wie z. B. Network File System (NFS).

- Mountpunkte lokaler Festplatten sind auf jedem physischen Host in der Umgebung identisch (wenn das Dateisystem `/group1_disk1` von NodeA zu NodeB fehlschlägt, wird es auf NodeB als `/group1_disk1` angehängt).

Übersicht über Clusterumgebungen

Clusterumgebungen können in vielen unterschiedlichen Konfigurationen definiert werden. In diesem Abschnitt werden die gängigsten Clusterkonfigurationen beschrieben.

Aktiv/Aktiv: Pool-Clusterressourcen

In einer Konfiguration Aktiv/Aktiv verwaltet jeder Knoten aktiv mindestens eine Ressource und wird als Sicherung für eine oder mehrere Ressourcen im Cluster konfiguriert. Aktiv/Aktiv ist die häufigste Form einer Clusterumgebung.

Aktiv/Passiv: Fehlertolerant

In einer Konfiguration Aktiv/Passiv verwaltet ein Knoten aktiv die Ressource.

Der andere Knoten wird nur verwendet, wenn es beim Primärknoten zu einem Fehler kommt und die Ressource eine Übernahme benötigt. Ein Cluster Aktiv/Passiv ist ein Subtyp eines Clusters Aktiv/Aktiv.

Gleichzeitiger Zugriff

In einer gleichzeitig ablaufenden Konfiguration verwalten mehrere Knoten eine Ressource. Wenn ein Fehler auftritt, wird die Ressource von den anderen Knoten weiter verwaltet.

Client für Sichern/Archivieren in einer Clusterumgebung konfigurieren

Der Client für Sichern/Archivieren ist so konzipiert, dass er die Sicherung von Clusterlaufwerken verwaltet, indem er den Client für Sichern/Archivieren in den Kontext der Ressourcengruppen des Clusters stellt.

Informationen zu diesem Vorgang

Dies hat den Vorteil, dass Daten von lokalen Ressourcen gesichert werden können (im Gegensatz zum Zugriff auf die Daten über das Netz), um die Leistung der Sicherungsoperation zu maximieren und die Sicherungsdaten in Bezug auf die Ressourcengruppe zu verwalten. Deshalb kann der Client für Sichern/Archivieren Daten immer auf Clusterressourcen sichern, als ob die Daten lokale Daten wären, und die Leistung beim Sichern maximieren. Dadurch wird sichergestellt, dass kritische Daten über Systemausfälle hinweg gesichert werden.

Beispiel: Eine Clusterumgebung Aktiv/Aktiv hat drei physische Hosts im Cluster mit den Namen NodeA, NodeB und NodeC.

Die Knoten verfügen über folgende Qualitäten:

- NodeA ist Eigner der Clusterressource mit den Dateisystemen /A1 und /A2
- NodeB ist Eigner der Clusterressource mit den Dateisystemen /B1 und /B2
- NodeC ist Eigner der Clusterressource mit den Dateisystemen /C1 und /C2

Anmerkung: NodeA hat möglicherweise noch zwei Datenträger, /fs1 und /fs2, die keine Clusterdatenträger sind und gesichert werden müssen.

Um die beste Sicherungsleistung zu erzielen, möchten Sie unter Umständen, dass alle Knoten im Cluster die Sicherungen der in ihrem Besitz befindlichen gemeinsam genutzten Dateisysteme ausführen. Wenn eine Knotenübernahme auftritt, werden die Sicherungstasks des fehlgeschlagenen Knotens auf den Knoten verschoben, auf dem die Übernahme auftrat. Beispiel: Wenn NodeA fehlschlägt und von NodeB übernommen wird, wird die Sicherung von /A1 und /A2 auf NodeB verschoben.

Nachfolgend die Voraussetzungen, die erfüllt sein müssen, bevor der Client für Sichern/Archivieren für das Sichern von Cluster- und Nicht-Clusterdatenträgern konfiguriert werden kann:

- Für jede Ressourcengruppe, die geschützt werden soll, muss ein separater Schedulerprozess des Clients für Sichern/Archivieren ausgeführt werden. Unter normalen Bedingungen hätte jeder Knoten zwei Schedulerprozesse: einen für die Clusterressourcen und einen für die lokalen Dateisysteme. Nach einer Störung werden zusätzliche Schedulerprozesse auf einem Knoten gestartet, damit die Ressourcen, die von einem anderen Knoten verschoben wurden, geschützt werden.
- Die Kennwortdateien des Clients für Sichern/Archivieren müssen auf Clusterplatten gespeichert werden, damit das generierte Kennwort des Clients für Sichern/Archivieren dem Übernahmeknoten nach einer Störung zur Verfügung steht.
- Die Dateisysteme, die als Teil einer Ressourcengruppe geschützt werden sollen, werden mithilfe der Option domain des Clients für Sichern/Archivieren definiert. Die Option domain wird in der Datei dsm.sys angegeben, die ebenfalls auf einer Clusterplatte gespeichert werden sollte, damit der Übernahmeknoten auf sie zugreifen kann.

Führen Sie die folgenden Schritte aus, um den Client für Sichern/Archivieren in einer Clusterumgebung zu konfigurieren.

Vorgehensweise

1. Registrieren Sie die Knotendefinitionen des Clients für Sichern/Archivieren beim IBM Spectrum Protect-Server. Alle Knoten im Cluster müssen auf dem

IBM Spectrum Protect-Server definiert sein. Wenn Sie mehrere Clusterressourcen in einer Clusterumgebung definieren, für die die Übernahme unabhängig voneinander erfolgt, muss für jede Ressourcengruppe ein eindeutiger Knotenname definiert werden. Für das oben stehende Beispiel einer Drei-Wege-Clusterkonfiguration Aktiv/Aktiv müssen Sie wie folgt drei Knoten (einen pro Ressource) definieren: (1) Protect: IBM>register node nodeA nodeApw domain=standard, (2) Protect: IBM>register node nodeB nodeBpw domain=standard, (3) Protect: IBM>register node nodeC nodeCpw domain=standard.

2. Konfigurieren Sie die Systemoptionsdatei des Clients für Sichern/Archivieren. Jeder Knoten im Cluster muss für jede Clusterressourcengruppe separate Serverzeilengruppen haben, damit er in jeder entsprechenden Datei dsm.sys gesichert werden kann. Sie müssen sicherstellen, dass die Serverzeilengruppen in den Systemoptionsdateien auf jedem Knoten identisch sind. Als Alternative können Sie die Datei dsm.sys auf eine gemeinsam genutzte Clusterlokation stellen. Die Serverzeilengruppe, die für die Sicherung von Datenträgern mit Clustern definiert werden, müssen folgende speziellen Merkmale aufweisen:

- Die Option nodename muss sich auf den Namen des Clientknotens beziehen, der auf dem IBM Spectrum Protect-Server registriert ist. Ist der Clientknotenname nicht definiert, nimmt der Knotenname standardmäßig den Wert des Hostnamens des Knoten an, was möglicherweise zu einem Konflikt mit anderen Knotennamen führt, die für dasselbe Clientsystem verwendet werden.

Wichtig: Verwenden Sie die Option nodename, um den Clientknoten explizit zu definieren.

- Für die Option tcpclientaddress muss die Service-IP-Adresse des Clusterknotens angegeben werden.
 - Für die Option passworddir muss ein Verzeichnis auf den gemeinsam genutzten Datenträgern angegeben werden, die Bestandteil der Clusterressourcengruppe sind.
 - Die Optionen errorlogname und schedlogname müssen sich auf Dateien auf den gemeinsam genutzten Datenträgern beziehen, die Bestandteil der Clusterressourcengruppe sind, um eine einzelne, kontinuierliche Protokolldatei aufrecht zu erhalten.
 - Alle Include/Exclude-Anweisungen müssen sich auf Dateien auf den gemeinsam genutzten Datenträgern beziehen, die Bestandteil der Clusterressourcengruppe sind.
 - Wenn Sie die Option inclexcl verwenden, muss sich diese auf einen Dateipfad auf den gemeinsam genutzten Datenträgern beziehen, die Bestandteil der Clusterressourcengruppe sind.
 - Die Zeilengruppenamen, die mit der Option servername identifiziert werden, müssen auf allen Systemen identisch sein.
3. Andere Optionen des Clients für Sichern/Archivieren können nach Bedarf definiert werden. Im folgenden Beispiel müssen alle drei Knoten, NodeA, NodeB und NodeC, die folgenden drei Serverzeilengruppen in ihrer Datei dsm.sys aufweisen:

```
Servername      server1_nodeA
nodename        NodeA
commmethod      tcpip
tcpport         1500
tcpserveraddress server1.example.com
tcpclientaddress nodeA.example.com
passwordaccess  generate
passworddir     /A1/tsm/pwd
```

```

managedservices    schedule
schedlogname       /A1/tsm/dsmsched.log
errorlogname       /A1/tsm/errorlog.log

```

```

Servername         server1_nodeB
nodename           NodeB
commmethod         tcpip
tcpport            1500
tcpserveraddress   server1.example.com
tcpclientaddress   nodeB.example.com
passwordaccess     generate
passworddir        /B1/tsm/pwd
managedservices    schedule
schedlogname       /B1/tsm/dsmsched.log
errorlogname       /B1/tsm/errorlog.log

```

```

Servername         server1_nodeC
nodename           NodeC
commmethod         tcpip
tcpport            1500
tcpserveraddress   server1.example.com
tcpclientaddress   nodeC.example.com
passwordaccess     generate
passworddir        /C1/tsm/pwd
managedservices    schedule
schedlogname       /C1/tsm/dsmsched.log
errorlogname       /C1/tsm/errorlog.log

```

4. Konfigurieren Sie die Benutzeroptionsdatei des Clients für Sichern/Archivieren. Die Optionsdatei (dsm.opt) muss auf den gemeinsam genutzten Datenträgern in der Clusterressourcengruppe stehen. Definieren Sie die Umgebungsvariable DSM_CONFIG so, dass sie sich auf diese Datei bezieht. Stellen Sie sicher, dass die Datei dsm.opt folgende Einstellungen enthält:
 - Der Wert für die Option servername muss der Serverzeilengruppe in der Datei dsm.sys entsprechen, die Parameter für die Sicherung von Clusterdatenträgern enthält.
 - Definieren Sie die Clusterdateisysteme so, dass sie mit der Option domain gesichert werden.

Anmerkung: Stellen Sie sicher, dass Sie die Option 'domain' in der Datei dsm.opt definieren oder geben Sie die Option im Zeitplan oder in der Befehlszeile des Clients für Sichern/Archivieren an. Dadurch werden Clusteroperationen auf Clusterressourcen und Nicht-Clusteroperationen auf Nicht-Clusterressourcen beschränkt.

Im Beispiel definieren die Knoten NodeA, NodeB und NodeC ihre entsprechende Datei dsm.opt und die Umgebungsvariable DSM_CONFIG wie folgt:

NodeA:

- 1) Die Datei /A1/tsm/dsm.opt definieren:

```

servername server1_nodeA
domain      /A1 /A2

```

- 2) Folgenden Befehl ausgeben oder in Ihr Benutzerprofil einschließen:

```
export DSM_CONFIG=/A1/tsm/dsm.opt
```

NodeB:

- 1) Die Datei /B1/tsm/dsm.opt definieren:

```

servername server1_nodeB
domain      /B1 /B2

```

2) Folgenden Befehl ausgeben oder in Ihr Benutzerprofil einschließen:

```
export DSM_CONFIG=/B1/tsm/dsm.opt
```

NodeC:

1) Die Datei /C1/tsm/dsm.opt definieren:

```
servername server1_nodeC  
domain      /C1 /C2
```

2) Folgenden Befehl ausgeben oder in Ihr Benutzerprofil einschließen:

```
export DSM_CONFIG=/C1/tsm/dsm.opt
```

5. Definieren Sie die Zeitplandefinitionen für jede Clusterressourcengruppe. Nachdem die Basiseinrichtung abgeschlossen ist, definieren Sie die automatischen Zeitpläne für das Sichern von Clusterressourcen, um die Sicherungsanforderungen zu erfüllen. Die Prozedur illustriert die Zeiteinrichtung durch Verwendung des integrierten IBM Spectrum Protect-Scheduler. Wenn Sie einen von einem Lieferanten erworbenen Scheduler verwenden, schlagen Sie in der vom Schedulerlieferanten zur Verfügung gestellten Dokumentation nach.

- Definieren Sie einen Zeitplan in der Maßnahmendomäne, in der Clusterknoten definiert sind. Stellen Sie sicher, dass das Startfenster des Zeitplans groß genug ist, um im Fall einer Störung und eines Zurücksetzungsereignisses den Zeitplan auf dem Übernahmeknoten erneut starten zu können. Dies bedeutet, dass die Dauer des Zeitplans so definiert werden muss, dass sie länger ist als die Zeit, die benötigt wird, um die Sicherung der Clusterdaten für diesen Knoten unter normalen Bedingungen zu beenden.

Wenn der erneute Verbindungsaufbau innerhalb des Startfensters für das betreffende Ereignis gelingt, wird der geplante Befehl erneut gestartet. Die geplante Teilsicherung prüft dann erneut die Dateien, die vor der Übernahme an den Server gesendet wurden. Die Sicherung wird an der Stelle fortgesetzt, an der sie vor der Übernahme gestoppt wurde.

Im folgenden Beispiel wird der Zeitplan `clus_backup` in der Standarddomäne so definiert, dass die Sicherung um 00:30 Uhr täglich gestartet wird, wobei die Dauer auf zwei Stunden festgesetzt ist (dies ist die normale Sicherungszeit für die Daten eines einzelnen Knotens).

```
Protect: IBM>define schedule standard clus_backup action=incr  
starttime=00:30 startdate=TODAY Duration=2
```

- Ordnen Sie den Zeitplan wie folgt allen Knoten des Clients für Sichern/Archivieren zu, die für das Sichern von Clusterressourcen definiert sind: (1)
Protect: IBM>define association standard clus_backup nodeA, (2)
Protect: IBM>define association standard clus_backup nodeB, (3)
Protect: IBM>define association standard clus_backup nodeC.

6. Definieren Sie den Scheduler-Service für Sichern. Auf jedem Clientknoten muss für jede Ressource, für deren Sicherung der Knoten unter normalen Bedingungen verantwortlich ist, ein Scheduler-Service konfiguriert werden. Die Umgebungsvariable `DSM_CONFIG` für jeden Ressourcenscheduler-Service muss so definiert werden, dass sie auf die entsprechende Datei `dsm.opt` für diese Ressource verweist. Für die Beispielkonfiguration müssen folgende Shell-Skripts erstellt werden, damit die `dsmcad`-Prozesse nach Bedarf von jedem beliebigen Knoten im Cluster gestartet werden können.

```
NodeA: /A1/tsm/startsched  
#!/bin/ksh  
export DSM_CONFIG=/A1/tsm/dsm.opt  
dsmcad
```

```

NodeB: /B1/tsm/startsched
#!/bin/ksh
export DSM_CONFIG=/B1/tsm/dsm.opt
dsmcad
NodeC: /C1/tsm/startsched
#!/bin/ksh
export DSM_CONFIG=/C1/tsm/dsm.opt
dsmcad

```

7. Definieren Sie den Client für Sichern/Archivieren für die Clusteranwendung. Damit die Sicherung der fehlgeschlagenen Ressource nach einer Übernahmebedingung fortgesetzt werden kann, muss der IBM Spectrum Protect-Scheduler-Service (für jeden Cluster-Clientknoten) als Ressource für die Clusteranwendung definiert werden, um an der Übernahmeverarbeitung teilzuhaben. Dies ist erforderlich, damit die Sicherung der fehlgeschlagenen Ressourcen von dem Knoten, der die Ressource übernimmt, fortgesetzt werden kann. Eine gegenteilige Aktion würde zu einer unvollständigen Sicherung der fehlgeschlagenen Ressource führen. Die Beispielskripts in Schritt 5 können den Clusterressourcen zugeordnet werden, um sicherzustellen, dass sie auf Knoten im Cluster gestartet werden, während die Plattenressourcen, die geschützt werden, von einem Knoten zum anderen verschoben werden. Die tatsächlichen Schritte, die erforderlich sind, um den Scheduler-Service als Clusterressource zu installieren, hängen von der spezifischen Cluster-Software ab. Die Dokumentation zu Ihrer Clusteranwendung enthält weitere Informationen.

8. Stellen Sie sicher, dass das Kennwort für jeden Knoten korrekt generiert und an der mit der Option `passworddir` angegebenen Position in den Cache gestellt wurde. Dies können Sie prüfen, indem Sie folgende Schritte ausführen:

- a. Prüfen Sie, ob jeder Knoten ohne Aufforderung zur Kennworteingabe eine Verbindung zum IBM Spectrum Protect-Server herstellen kann. Hierfür führen Sie die Befehlszeilenschnittstelle des Clients für Sichern/Archivieren aus und geben auf jedem Knoten den folgenden Befehl ein:

```
#dsmc query session
```

Wenn Sie zur Eingabe Ihres Kennworts aufgefordert werden, geben Sie das Kennwort ein, um den Befehl erfolgreich auszuführen, und wiederholen den Befehl. Das zweite Mal sollte der Befehl ohne Eingabeaufforderung für das Kennwort ausgeführt werden. Wenn Sie zur Kennworteingabe aufgefordert werden, überprüfen Sie Ihre Konfiguration.

- b. Prüfen Sie, ob die anderen Knoten im Cluster Sitzungen mit dem IBM Spectrum Protect-Server wegen des in einer Übernahmeverarbeitung befindlichen Knotens starten können. Dies kann durchgeführt werden, indem dieselben Befehle, wie im Schritt oben beschrieben, auf den Sicherungsknoten ausgeführt werden. Beispiel: Um zu prüfen, ob NodeB und NodeC bei einem Übernahmeereignis eine Sitzung als NodeA starten können, ohne dass zur Eingabe des Kennworts aufgefordert wird, führen Sie folgende Befehle auf NodeB und NodeC aus.

```
#export DSM_CONFIG=/A1/tsm/dsm.opt
#dsmc query session
```

Die Eingabeaufforderung für das Kennwort wird jetzt möglicherweise angezeigt, aber dies ist unwahrscheinlich. Wenn Sie zur Eingabe aufgefordert werden, war das Kennwort in der gemeinsam genutzten Lokation nicht richtig gespeichert. Überprüfen Sie die Einstellung der Option `passworddir`, die für NodeA verwendet wird, und folgen Sie den Konfigurationsschritten erneut.

- c. Stellen Sie sicher, dass die Zeitpläne von jedem Knoten korrekt ausgeführt werden. Sie können einen Zeitplan auslösen, indem Sie die Startzeit des Zeitplans auf Jetzt setzen. Denken Sie daran, die Startzeit nach Abschluss des Tests wieder zurückzusetzen.

Protect: IBM>update sched standard clus_backup starttime=now

- d. Die Übernahme und Rückübertragung zwischen nodeA und nodeB ist immer noch gültig, während nodeA die Sicherung ausführt und sich im Startfenster des Zeitplans befindet. Überprüfen Sie, ob die Teilsicherung nach Übernahme und Rückübertragung weiterhin ausgeführt und erfolgreich beendet wird.
- e. Geben Sie den folgenden Befehl aus, damit das Kennwort eines Knotens (nodeA) abläuft. Stellen Sie sicher, dass die Sicherung unter normalen Clusteroperationen ebenso wie die Übernahme und Rückübertragung normal weiterläuft:

Protect: IBM>update node nodeA forcep=yes

9. Konfigurieren Sie den Client für Sichern/Archivieren, sodass lokale Ressourcen gesichert werden.

- a. Definieren Sie Clientknoten auf dem IBM Spectrum Protect-Server. Lokale Ressourcen sollten nie mit Knotennamen gesichert oder archiviert werden, die für das Sichern von Clusterdaten definiert sind. Werden lokale Datenträger gesichert, die nicht als Clusterressourcen definiert sind, müssen für die Datenträger im Cluster und die Datenträger, die nicht zum Cluster gehören, separate Knotennamen (und separate Clientinstanzen) verwendet werden.

Im folgenden Beispiel setzen wir voraus, dass nur NodeA über die zu sichernden lokalen Dateisysteme /fs1 und /fs2 verfügt. Zum Verwalten der lokalen Ressourcen registrieren Sie den Knoten NodeA_local auf dem IBM Spectrum Protect-Server: Protect: IBM>register node nodeA_local nodeA_localpw domain=standard.

- b. Fügen Sie in der Systemoptionsdatei dsm.sys auf jedem Knoten eine separate Zeilengruppe hinzu, die lokale Ressourcen mit den folgenden besonderen Merkmalen sichern muss:

- Der Wert der Option tcpclientaddress muss der Name oder die IP-Adresse des lokalen Hosts sein. Dabei handelt es sich um die IP-Adresse, die für den primären Datenverkehr zu und von einem Knoten verwendet wird.
- Wenn der Client nicht zu einem Cluster gehörende Datenträger sichert und zurückschreibt, ohne mit dem Cluster verbunden zu sein, muss der Wert der Option tcpclientaddress die Boot-IP-Adresse sein. Diese IP-Adresse wird zum Starten des Systems (Knoten) verwendet, bevor die Verbindung zum Cluster hergestellt wird:

Beispielzeilengruppe für NodeA_local:

Servername	server1_nodeA_local
nodename	nodeA_local
commethod	tcpip
tcpport	1500
tcpserveraddress	server1.example.com
tcpclientaddress	nodeA_host.example.com
passwordaccess	generate
managedservices	schedule

- c. Definieren Sie die Benutzeroptionsdatei dsm.opt in einem Pfad, der sich auf einer Ressource ohne Cluster befindet.

- Der Wert für die Option `servername` muss der Serverzeilengruppe in der Datei `dsm.sys` entsprechen, die Parameter für die Sicherung von Datenträgern ohne Cluster definiert.
- Verwenden Sie die Option `domain`, um die zu sichernden Dateisysteme ohne Cluster zu definieren.

Anmerkung: Stellen Sie sicher, dass Sie die Option 'domain' in der Datei `dsm.opt` definieren oder geben Sie die Option im Zeitplan oder in der Befehlszeile des Clients für Sichern/Archivieren an, um die Sicherungs-/Archivierungsoperationen auf Datenträger ohne Clustering zu beschränken.

Im folgenden Beispiel verwendet nodeA die folgende Datei `/home/admin/dsm.opt` und richtet die Umgebung `DSM_CONFIG` so ein, dass sie auf `/home/admin/A1.dsm.opt` verweist.

Inhalt von `/home/admin/A1.dsm.opt`

```
servername ibm_nodeA_local
domain     /fs1 /fs2
```

```
export DSM_CONFIG=/home/admin/A1.dsm.opt
```

- d. Definieren Sie einen Zeitplan und richten Sie ihn so ein, dass er die Teilsicherung für Dateisysteme außerhalb des Clusters ausführt.

```
Protect: IBM>define schedule standard local_backup action=incr
starttime=00:30 startdate=TODAY Duration=2
```

Ordnen Sie den Zeitplan allen Knoten des Clients für Sichern/Archivieren zu, die für das Sichern von Ressourcen außerhalb des Clusters definiert sind.

```
Protect: IBM>define association standard nodeA_local
```

10. Schreiben Sie die Gruppendateisystemdaten zurück. Alle Datenträger in einer Clusterressource werden unter dem Zielknoten gesichert, der für diese Clusterressource definiert ist. Wenn Sie die Daten, die auf einem Clusterdatenträger resident sind, zurückschreiben müssen, können Sie sie von dem Clientknoten zurückschreiben, der zum Zeitpunkt der Zurückschreibung Eigner der Clusterressource ist. Der Client für Sichern/Archivieren muss dieselbe Benutzeroptionsdatei (`dsm.opt`) verwenden, die während der Sicherung verwendet wurde, um die Daten zurückzuschreiben. Es sind keine zusätzlichen Installationsvoraussetzungen erforderlich, um Daten auf Clusterdatenträgern zurückzuschreiben.
11. Schreiben Sie die Daten des lokalen Dateisystems zurück. Die Datenträger ohne Cluster werden unter der separaten Knotennamenkonfiguration für Operationen ohne Cluster gesichert. Zum Zurückschreiben dieser Daten muss der Client für Sichern/Archivieren dieselbe Benutzeroptionsdatei (`dsm.opt`) verwenden, die während der Sicherung verwendet wurde. Definieren Sie in dem Beispiel die Umgebungsvariable `DSM_CONFIG` so, dass sie auf `/home/admin/A1.dsm.opt` verweist, bevor Sie eine Clientzurückschreibung für den lokalen Knoten `nodeA_local` ausführen.

Zugehörige Konzepte:

Kapitel 5, „Daten zurückschreiben“, auf Seite 247

Web-Client-Zugriff in einer Clusterumgebung aktivieren

Wenn während einer Übernahmebedingung IBM Spectrum Protect-Web-Client-Zugriff erforderlich ist, müssen Sie den Web-Clientakzeptordämon, der dem Cluster zugeordnet ist, so konfigurieren, dass für ihn zusammen mit der Clusterressource eine Übernahme erfolgt.

Vorbereitende Schritte

Ab IBM Spectrum Protect Version 8.1.2 können Sie nicht mehr die Web-Client-GUI verwenden, um eine Verbindung zum IBM Spectrum Protect-Server der Version 8.1.2 oder höher herzustellen. Weitere Informationen enthält der Abschnitt „Web-Client in der neuen Sicherheitsumgebung verwenden“ auf Seite 158.

Informationen zu diesem Vorgang

Nachdem Sie die im Abschnitt *Client für Sichern/Archivieren in einer Clusterumgebung konfigurieren* beschriebenen Konfigurationsschritte ausgeführt haben, müssen Sie die nachfolgend beschriebenen zusätzlichen Schritte ausführen, um die Konfiguration des Web-Client-Zugriffs abzuschließen:

Vorgehensweise

1. Konfigurieren Sie den Clientakzeptordämon so, dass er den Web-Client und den Scheduler verwaltet. In der Konfiguration des Clientakzeptordämons sollte festgelegt werden, dass er sowohl Scheduler als auch den Web-Client-Zugriff verwaltet. Auf diese Weise wird die Anzahl Dämonen verkleinert, die als Clusteranwendungen konfiguriert werden müssen, und die Konfiguration und Verwaltung dadurch vereinfacht. Wenn eine Übernahme erfolgt, startet der Clientakzeptor auf dem Knoten, der die Übernahme handhabt.
2. Aktualisieren Sie die Option `managedservices` in der Systemoptionsdatei `dsm.sys` auf jedem Knoten für jede Serverzeilengruppe, wie unten für NodeA gezeigt:

Servername	server1_NodeA
nodename	NodeA
commmethod	tcpip
tcpp	1500
tcps	server1.example.com
tcpclientaddress	nodeA.example.com
passwordaccess	generate
passworddir	/A1/tsm/pwd
schedlogn	/A1/tsm/dsmsched.log
errorlogname	/A1/tsm/errorlog.log
managedservices	webclient schedule

3. Konfigurieren Sie den Clientakzeptordämon für die Verwendung eines bekannten HTTP-Anschlusses. Standardmäßig verwendet der Clientakzeptordämon für den Web-Client-Zugriff HTTP-Anschluss 1581, sofern verfügbar. Wenn dieser Anschluss nicht verfügbar ist, sucht der Clientakzeptor den ersten verfügbaren Anschluss ab 1581. Bei einer Übernahmefunktion einer Clusterkonfiguration Aktiv/Aktiv führt das Hostsystem eines Übernahmekusters wahrscheinlich mehrere Instanzen des Clientakzeptors aus. Wenn die Standardeinstellungen für den HTTP-Anschluss verwendet werden, verwendet der Übernahmeknoten einen beliebigen verfügbaren Anschluss für den Clientakzeptor, für den eine Übernahme erfolgt, da der Standardanschluss wahrscheinlich durch die aktuellen Clientakzeptorprozesse des Übernahmehosts belegt ist. Dies führt zu Problemen für den Web-Client, der dem Clientakzeptor, für den die Übernahme erfolgt ist, zugeordnet ist, da der neue HTTP-Anschluss den Web-Client-Benutzern nicht bekannt ist. Sie können gegebenenfalls die Option `httpport` verwenden, um für jede Ressource die Anschlüsse für den Web-Client-Zugriff anzugeben. Dadurch ist es möglich, dass Sie stets denselben Anschluss verwenden, wenn Sie eine Verbindung von einem Web-Browser aus herstellen, unabhängig vom Knoten, der die Clusterressource bedient. Fügen Sie wie folgt auf jedem Knoten für jede Serverzeilengruppe die Option `httpport` in der Systeme-

moptionsdatei (dsm.sys) hinzu und stellen Sie dabei sicher, dass in jeder Zeilen-
gruppe ein eindeutiger Wert verwendet wird:

```
Servername      server1_NodeA
nodename        NodeA
commmethod      tcpip
tcpp            1500
tcps            server1.example.com
tcpclientadres  nodeA.example.com
passwordaccess  generate
passworddir     /A1/tsm/pwd
managedservices webclient schedule
schedlogn       /A1/tsm/dsmsched.log
errorlogname    /A1/tsm/errorlog.log
httpport        1510

Servername      server1_NodeB
nodename        NodeB
commmethod      tcpip
tcpp            1500
tcps            server1.example.com
tcpclientadres  nodeB.example.com
passwordaccess  generate
passworddir     /B1/tsm/pwd
managedservices webclient schedule
schedlogn       /B1/tsm/dsmsched.log
errorlogname    /B1/tsm/errorlog.log
httpport        1511

Servername      server1_NodeC
nodename        NodeC
commmethod      tcpip
tcpp            1500
tcps            server1.example.com
tcpclientadres  nodeC.example.com
passwordaccess  generate
passworddir     /C1/tsm/pwd
managedservices webclient schedule
schedlogn       /C1/tsm/dsmsched.log
errorlogname    /C1/tsm/errorlog.log
httpport        1512
```

Traditionelle AIXIBM PowerHA SystemMirror-Konfigurationen migrieren

Wenn Sie den Client für Sichern/Archivieren gegenwärtig in einer IBM PowerHA
SystemMirror-Umgebung mit der Option clusternode verwenden, müssen Sie Ihre
aktuellen Konfigurationen aktualisieren. Die Option clusternode wird nicht mehr
unterstützt.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um Ihre aktuellen Konfigurationen zu aktua-
lisieren:

Vorgehensweise

1. Aktualisieren Sie die Systemoptionsdatei des Clients für Sichern/Archivieren.
Wie bei der Option clusternode muss jeder Knoten im Cluster auch weiterhin
für jede Clusterressourcengruppe separate Serverzeilengruppen haben, damit er
in jeder entsprechenden Datei dsm.sys gesichert werden kann. Die bestehende
Datei dsm.sys für NodeA wird möglicherweise wie folgt angezeigt:

Servername	server1_nodeA
commethod	tcpip
tcpp	1500
tcps	server1.example.com
tcpclientaddress	nodeA.example.com
passwordaccess	generate
passworddir	/A1
clusternode	yes
manageservices	schedule
schedlogn	/A1/dsmsched.log
errorlogname	/A1/errorlog.log

2. Beachten Sie, dass in diesem Beispiel keine Option `nodename` verwendet wird. Nehmen Sie die folgenden Änderungen an der bestehenden Datei `dsm.sys` für NodeA vor.
 - Entfernen Sie die Option `clusternode`.
 - Geben Sie, falls nicht bereits geschehen, eine Option `nodename` an.
3. Die neue Datei `dsm.sys` für NodeA sollte wie folgt erscheinen:

Servername	server1_nodeA
commethod	tcpip
nodename	myclus (myclus ist der vorhandene Clustername)
tcpp	1500
tcps	server1.example.com
tcpclientaddress	nodeA.example.com
passwordaccess	generate
passworddir	/A1
manageservices	schedule
schedlogn	/A1/dsmsched.log
errorlogname	/A1/errorlog.log

4. Registrieren Sie die Knoten des Clients für Sichern/Archivieren beim IBM Spectrum Protect-Server. Wenn die neuen Knoten des Clients für Sichern/Archivieren im ersten Schritt hinzugefügt werden, um den aktuellen Standardwert des Clusterknotennamens zu ersetzen, registrieren Sie diese Knoten auf dem IBM Spectrum Protect-Server.
5. Aktualisieren Sie die Zeitplandefinitionen. Wenn im vorherigen Schritt neue Knoten des Clients für Sichern/Archivieren hinzugefügt wurden, stellen Sie sicher, dass die Sicherungszeitplandefinitionen, die vorher zum Sichern der Daten dieses Knotens verwendet wurden, jetzt den neuen Clientknotennamen zugeordnet werden.
6. Prüfen Sie die Konfiguration. Weitere Informationen finden Sie in „Client für Sichern/Archivieren in einer Clusterumgebung konfigurieren“ auf Seite 108.

Hinweise zur AIX-Konfiguration vor Ausführung von momentaufnahmebasierten Dateisicherungen und -archivierungen

Wenn Sie Ihren IBM Spectrum Protect-AIX-Client für die Ausführung von momentaufnahmebasierten Dateisicherungen und -archivierungen konfigurieren, sind einige Hinweise zu beachten.

- Stellen Sie sicher, dass die Datenträgergruppe, die das Dateisystem enthält, von dem eine Momentaufnahme erstellt werden soll, ausreichenden Plattenspeicherplatz aufweist, damit externe JFS2-Momentaufnahmen für das Dateisystem erstellt werden können.
- Der Client verwendet eine Standardgröße von 100 Prozent der Dateisystemgröße für die Momentaufnahmegröße. Dieser Wert wurde als geeignetster Wert für Dateisysteme mit ruhiger mittlerer Dateisystemaktivität gefunden. Wenn Sie auf der Grundlage Ihrer Erfahrung mit Ihrer eigenen Dateisystemaktivität glauben,

diesen Wert verringern zu müssen, können Sie mit der Option `snapshotcachesize` diesen Wert durch Feinabstimmung optimieren.

- Aktivieren Sie keine internen Momentaufnahmen, wenn Sie neue JFS2-Dateisysteme unter AIX 6.1 oder höher für alle Dateisysteme erstellen, die von IBM Spectrum Protect verwaltet werden. Der Client verwendet externe Momentaufnahmen und JFS2 ermöglicht nicht die gleichzeitige Erstellung externer und interner Momentaufnahmen für dasselbe Dateisystem.

Zugehörige Verweise:

„`Snapshotcachesize`“ auf Seite 590

NetApp und IBM Spectrum Protect für Teilsicherungen unter Verwendung der Momentaufnahmedifferenz konfigurieren

Sie müssen die Verbindungsinformationen für den NetApp-Dateiserver konfigurieren, damit der Befehl für eine Teilsicherung unter Verwendung der Momentaufnahmedifferenz auf dem Client für Sichern/Archivieren ausgeführt werden kann. Außerdem müssen Sie mit dem Befehl **set password** den Hostnamen des Dateiservers sowie das Kennwort und den Benutzernamen für den Zugriff auf den Dateiserver angeben.

Vorgehensweise

1. Gehen Sie wie folgt vor, um eine Konsolsitzung auf dem NetApp-Dateiserver aufzubauen und einen neuen Benutzer auf dem Dateiserver zu definieren:
 - a. Fügen Sie die Benutzer-ID einer Gruppe hinzu, die eine Benutzeranmeldung auf dem Dateiserver mit HTTP und die Ausführung von API-Befehlen gestattet.
 - b. Geben Sie auf dem Dateiserver den folgenden Befehl ein, um die Benutzer-ID aufzulisten und die Einstellungen zu überprüfen und ob die Ausgabe ähnlich ist:

```
useradmin user list snapdiff-Benutzer
```

```
Name: snapdiff-Benutzer
Info:
Rid: 131077
Groups: snapdiff-Gruppe
Full Name:
```

Für 7-Mode-NetApp-Dateiserver:

```
Allowed Capabilities: login-http-admin,api-*
```

Bei Clustered Data ONTAP-NetApp-Dateiservern ist als einzige Berechtigung `ontapapi` mit der Rolle `admin` erforderlich.

- c. Ist für die Option **security.password.firstlogin.enable** für die Benutzer-ID auf dem NetApp-Server `on` definiert, stellen Sie sicher, dass alle Gruppen über die Leistungsmerkmale **login-telnet** und **cli-password*** verfügen.

Tipp: Wenn die Option **security.password.firstlogin.enable** aktiviert ist, wird die Benutzer-ID bei der Erstellung auf `expired` gesetzt. Der Benutzer kann keine Befehle ausführen (auch keine Momentaufnahmedifferenzteilsicherung), bis sein Kennwort geändert wird. Benutzer in Gruppen, die nicht über diese Funktionalität verfügen, können sich nicht beim Speichersystem anmelden. Informationen zur Definition einer Benutzer-ID und eines Kennworts auf dem NetApp-Dateiserver finden Sie in der NetApp-Dokumentation.

2. Konfigurieren Sie den integrierten NetApp Data ONTAP-HTTP-Server, um Verwaltungssitzungen über Fernzugriff für den NetApp-Dateiserver zu ermöglichen.
 - a. Wenn eine normale HTTP-Verbindung für Momentaufnahmedifferenzsicherungen verwendet werden soll, aktivieren Sie die Option **httpd.admin.enable** auf dem NetApp-Dateiserver.
 - b. Wenn eine sichere HTTPS-Verbindung für Momentaufnahmedifferenzsicherungen verwendet werden soll (durch Angabe der Option **-snapdiffhttps**), aktivieren Sie die Option **httpd.admin.ssl.enable** auf dem NetApp-Dateiserver.
 - c. Testen Sie auf dem IBM Spectrum Protect-Clientknoten die Verbindung zwischen dem IBM Spectrum Protect-Client-Computer und dem NetApp ONTAP-Server, um sicherzustellen, dass die Verbindung zum NetApp-Server nicht durch Firewalls oder andere NetApp-Konfigurationsoptionen verhindert wird.

Tipp: Informationen zum Testen der Verbindung finden Sie in der NetApp ONTAP-Dokumentation.

3. Exportieren Sie die NetApp-Datenträger und ziehen Sie die folgenden Einstellungen in Betracht:

Tipp: Ausführliche Informationen zum Exportieren der NetApp-Datenträger für die Verwendung in Linux-Hosts finden Sie in der NetApp-Dokumentation.

- Ordnen Sie die NetApp-Datenträger mit einem NFS-Mount zu.
- Stellen Sie sicher, dass die NetApp-Datenträger über die UNIX-Sicherheitseinstellung verfügen.

4. Definieren Sie die Benutzer-ID und das Kennwort auf dem Client für Sichern/Archivieren für die in Schritt 1 auf Seite 119 erstellte Benutzer-ID, indem Sie die folgenden Schritte ausführen:

- a. Melden Sie sich mit der Rootbenutzer-ID an.
- b. Geben Sie den folgenden Befehl in die Befehlszeile des Clients für Sichern/Archivieren ein:

```
dsmc set password -type=filer eigener_Dateiserver snapdiff-Benutzer neues_Kennwort
```

Ersetzen Sie folgende Werte:

eigener_Dateiserver

Dieser Wert ist der vollständig qualifizierte Hostname Ihres NetApp-Dateiservers.

snapdiff-Benutzer

Dieser Wert ist die in Schritt 1 auf Seite 119 erstellte Benutzer-ID.

neues_Kennwort

Dieser Wert ist das Kennwort für die in Schritt 1 auf Seite 119 erstellte Benutzer-ID.

Zugehörige Tasks:

„Clustered Data ONTAP NetApp-Dateiserverdatenträger schützen“ auf Seite 121

Zugehörige Verweise:

„Snapdiff“ auf Seite 581

„Snapdiffhttps“ auf Seite 588

„Createnewbase“ auf Seite 383

Clustered Data ONTAP NetApp-Dateiserverdatenträger schützen

Sie können eine Momentaufnahmedifferenzteilsicherung eines Datenträgers auf einem NetApp-Dateiserver erstellen, der zu einer Clustered Data ONTAP-Konfiguration gehört (C-Mode-Dateiserver).

Vorbereitende Schritte

- Führen Sie die Prozedur in „NetApp und IBM Spectrum Protect für Teilsicherungen unter Verwendung der Momentaufnahmedifferenz konfigurieren“ auf Seite 119 aus.
- Stellen Sie sicher, dass die Clustered Data ONTAP-Umgebung korrekt vom Administrator der NetApp Storage Virtual Machine konfiguriert wurde.

Einschränkung: Die IBM Spectrum Protect-Unterstützung für Momentaufnahmedifferenzteilsicherungen von Clustered Data ONTAP-Datenträgern gilt nur bei NetApp ONTAP 8.2.1 und höheren Versionen.

Informationen zu diesem Vorgang

In einer Clustered Data ONTAP-Umgebung enthalten Storage Virtual Machines (die auch als Daten-vServer bezeichnet werden) Datenträger, die vom Client für Sichern/Archivieren geschützt werden können.

Eine Storage Virtual Machine besteht aus einem einzelnen infiniten Datenträger (Infinite Volume) oder einem oder mehreren flexiblen Datenträgern (FlexVol Volumes). Der Zugriff auf Datenträger erfolgt über Fernzugriff mithilfe der Dateifreigabe (CIFS unter Windows-Betriebssystemen, NFS unter Linux-Betriebssystemen).

Die Storage Virtual Machines werden vom Cluster-Management-Dateiserver verwaltet, dem physischen Dateiserver (C-Mode-Dateiserver), auf dem sich die Storage Virtual Machines befinden. Der Sicherungsclient ist auf der fernen Maschine installiert, die auf die Datenträger zugreift.

Der Client für Sichern/Archivieren muss mit Berechtigungsnachweisen für die NetApp-C-Mode-Dateiserver konfiguriert werden, auf die für Sicherungsoperationen zugegriffen wird.

Voraussetzungen:

- Für diese Prozedur sind die folgenden Informationen erforderlich:
 - Der Hostname oder die IP-Adresse des Cluster-Management-Dateiservers.
 - Der Hostname oder die IP-Adresse der Storage Virtual Machine.
 - Der Name der Storage Virtual Machine.
 - Die Berechtigungsnachweise des Cluster-Management-Dateiservers (Benutzername und Kennwort).
- Dem Benutzer des Cluster-Management-Dateiservers, der vom Client konfiguriert wird, muss die Berechtigung `ontapapi` mit der Rolle `admin` zugeordnet sein. Die Berechtigung `ontapapi` ermöglicht keinen interaktiven Zugriff auf den Dateiserver mithilfe von Methoden wie `telnet`, `ssh` oder `http/https`. Für die Ausführung von Momentaufnahmedifferenzteilsicherungen sind keine weiteren Benutzerberechtigungen erforderlich.

Vorgehensweise

Führen Sie die folgenden Schritte auf der fernen Maschine aus, auf der der Client für Sichern/Archivieren installiert ist:

1. Konfigurieren Sie den Client für Sichern/Archivieren mit den Berechtigungsnachweisen des Cluster-Management-Dateiservers. Verwenden Sie den Befehl **dsmc set password**, um die Berechtigungsnachweise des Management-Dateiservers, der der Storage Virtual Machine zugeordnet ist, zu speichern. Geben Sie beispielsweise den folgenden Befehl ein:

```
dsmc set password -type=filer Hostname_des_Management-Dateiservers  
Name_des_Benutzers_des_Management-Dateiservers Kennwort_des_Management-Dateiservers
```

Dabei gilt:

Hostname_des_Management-Dateiservers

Der Hostname oder die IP-Adresse des Cluster-Management-Dateiservers.

Name_des_Benutzers_des_Management-Dateiservers

Der Name des Benutzers des Cluster-Management-Dateiservers.

Kennwort_des_Management-Dateiservers

Das Kennwort für den Benutzer des Management-Dateiservers.

Tipp: Das Kennwort des Cluster-Management-Dateiservers wird verschlüsselt, wenn es vom Client für Sichern/Archivieren gespeichert wird.

2. Ordnen Sie jede Storage Virtual Machine mithilfe des Befehls **dsmc set netappsvm** dem Management-Dateiserver zu. Geben Sie z. B. den folgenden Befehl ein:

```
dsmc set netappsvm Hostname_der_Storage_Virtual_Machine  
Hostname_des_Management-Dateiservers Name_der_Storage_Virtual_Machine
```

Dabei gilt:

Hostname_der_Storage_Virtual_Machine

Der Hostname oder die IP-Adresse der Storage Virtual Machine, die zur Bereitstellung von Datenträgern verwendet wird, die gesichert werden sollen.

Hostname_des_Management-Dateiservers

Der Hostname oder die IP-Adresse des Cluster-Management-Dateiservers.

Name_der_Storage_Virtual_Machine

Der Name der Storage Virtual Machine.

Anmerkung: Der Hostname oder die IP-Adresse der Storage Virtual Machine, die zur Bereitstellung von Datenträgern verwendet wird, muss mit der Angabe in den Befehlen **dsmc set** konsistent sein. Wenn beispielsweise die Datenträger über die IP-Adresse einer Storage Virtual Machine bereitgestellt werden, muss die IP-Adresse (nicht der Hostname) in den Befehlen **dsmc set** verwendet werden. Andernfalls schlägt die Clientauthentifizierung mit dem Cluster-Management-Dateiserver fehl.

Sie müssen den Befehl **dsmc set netappsvm** nur einmal für jede Storage Virtual Machine angeben. Wenn die Storage Virtual Machine auf einen anderen Cluster-Management-Dateiserver versetzt wird, müssen Sie den Hostnamen des zugehörigen Cluster-Management-Dateiservers mithilfe des Befehls aktualisieren.

3. Stellen Sie die ferne Storage Virtual Machine auf einem lokalen Dateisystem bereit. Geben Sie beispielsweise den folgenden Befehl für jede Storage Virtual Machine ein:

```
mount Hostname_der_Storage_Virtual_Machine/tmp/fs1
```

Dabei gilt:

Hostname_der_Storage_Virtual_Machine

Der Hostname oder die IP-Adresse der Storage Virtual Machine.

/tmp/fs1

Ein Beispiel eines Dateisystems, in dem der Datenträger der Storage Virtual Machine bereitgestellt werden soll.

4. Starten Sie eine progressive vollständige Teilsicherung eines flexiblen oder infiniten Datenträgers.

Der HTTP-Zugriff auf den NetApp-Dateiserver ist standardmäßig nicht aktiviert. Wenn Sie Ihren Dateiserver nicht so konfiguriert haben, dass der Zugriff unter Verwendung von HTTP zulässig ist, verwenden Sie die Option `snappdiffhttps` des Clients für Sichern/Archivieren, um den Zugriff auf den Cluster-Management-Server mit dem Protokoll HTTPS zu ermöglichen.

Geben Sie beispielsweise auf Linux-Clients den folgenden Befehl ein:

```
dsmc incr /tmp/fs1 -snappdiff -snappdiffhttps
```

Tipp: Sie müssen die progressive vollständige Teilsicherung nur einmal ausführen. Nachdem diese Sicherung erfolgreich abgeschlossen wurde, führen in zukünftigen Sicherungsoperationen Differenzsicherungen aus.

5. Starten Sie eine Momentaufnahmedifferenzsicherung des flexiblen oder infiniten Datenträgers.

Geben Sie beispielsweise auf Linux-Clients den folgenden Befehl ein:

```
dsmc incr /tmp/fs1 -snappdiff -snappdiffhttps
```

Beispiel

Ein Benutzer des Clients für Sichern/Archivieren möchte eine Momentaufnahmedifferenzteilsicherung der Datenträger auf einem C-Mode-Dateiserver ausführen. Der Benutzer verwendet für die Ausführung der Sicherung einen Windows-Client für Sichern/Archivieren und die Datenträger werden als CIFS-Freigaben bereitgestellt. Die Konfiguration des C-Mode-Dateiservers ist wie folgt:

ONTAP 8.31-Management-Dateiserver

```
Hostname: netapplmgmt.example.com
Benutzer: netapplmgmt_user
Kennwort: pass4netapplmgmt
CIFS-Domänencontroller: WINDC
Domänenbenutzer: domainuser
```

Storage Virtual Machine mit flexiblem Datenträger

```
Hostname: netappl-v1.example.com
Name der Storage Virtual Machine: netappl-client1
CIFS-Freigabe: demovol
Datenträgername: demovol
```

Storage Virtual Machine mit infinitem Datenträger

```
Hostname: netappl-v4.example.com
Name der Storage Virtual Machine: netappl-infiniteVolume1
CIFS-Freigabe: InfiniteVol
```

Der Benutzer führt auf dem Client für Sichern/Archivieren die folgenden Schritte aus:

1. Konfigurieren des Clients mit Berechtigungsnachweisen des Management-Dateiservers durch Ausgabe des folgenden Befehls:
`dsmc set password -type=filer netapplmgmt.example.com netapplmgmt_user pass4netapplmgmt`
2. Definieren der Storage Virtual Machine-Zuordnungen für jede Storage Virtual Machine mit den folgenden Befehlen:
`dsmc set netappsvm netappl-v1.example.com netapplmgmt.example.com netappl-client1`
`dsmc set netappsvm netappl-v4.example.com netapplmgmt.example.com netappl-infiniteVolume1`
3. Zuordnen ferner Datenträger zu Laufwerksbuchstaben für jede Storage Virtual Machine:
`net use y: \\netappl-v1.example.com\demovol WINDC\domainuser`
`net use z: \\netappl-v4.example.com\InfiniteVol WINDC\domainuser`
4. Ausführen einer progressiven vollständigen Teilsicherung des flexiblen Datenträgers und des unendlichen Datenträgers:
`dsmc incr y: -snapdiff -snapdiffhttps`
`dsmc incr z: -snapdiff -snapdiffhttps`
 Sie müssen die progressive vollständige Teilsicherung nur einmal ausführen. Nachdem diese Sicherung erfolgreich abgeschlossen wurde, führen Sie in zukünftigen Sicherungsoperationen Differenzsicherungen aus.
5. Ausführen einer Momentaufnahmedifferenzsicherung des flexiblen Datenträgers und des unendlichen Datenträgers:
`dsmc incr y: -snapdiff -snapdiffhttps`
`dsmc incr z: -snapdiff -snapdiffhttps`

SnapMirror-Unterstützung für momentaufnahmegestützte progressive Teilsicherung von NetApp (snapdiff)

Sie können die SnapDiff-Sicherungsverarbeitung von NetApp in Verbindung mit der SnapMirror-Replikation von NetApp verwenden, um Datenträger des NetApp-Quellen- oder -Ziel-Dateiservers zu sichern.

In einer NetApp-SnapMirror-Umgebung werden Daten auf Datenträgern, die dem primären Datacenter zugeordnet sind, auf Datenträger gespiegelt, die einem fernen Server an einem Standort zur Wiederherstellung nach einem Katastrophenfall zugeordnet sind. Der NetApp-Dateiserver im primären Datacenter wird als Quellen-Dateiserver bezeichnet und der NetApp-Dateiserver am Standort zur Wiederherstellung nach einem Katastrophenfall als Ziel-Dateiserver. Mithilfe des Clients für Sichern/Archivieren können Sie Momentaufnahmedifferenzsicherungen der Datenträger auf dem Quellen- und Ziel-Dateiserver erstellen.

Szenario: Daten auf einem Datenträger des Quellen-Dateiservers sichern

Sie können in der Konfiguration des Clients für Sichern/Archivieren angeben, dass Daten von den Datenträgern des Quellen-Dateiservers gesichert werden sollen. Für dieses Szenario müssen Sie einen Knoten des Clients für Sichern/Archivieren so konfigurieren, dass er Zugriff auf die Datenträger des NetApp-Quellen-Dateiservers hat; dabei werden mit NFS exportierte Freigaben zum Anhängen der Dateiserverdatenträger verwendet.

Angenommen, es wird eine Konfiguration verwendet, in der der Quellen-Dateiserver den Namen ProdFiler hat. Außerdem wird angenommen, dass auf dem Dateiserver ProdFiler ein Datenträger mit dem Namen UserDataVol vorhanden ist und dass mithilfe von NFS über einen Clientknoten für Sichern/Archivieren auf den Datenträger zugegriffen werden kann. Es wird angenommen, dass die Freigabe als UserDataVol_Share angehängt ist.

Wenn Sie eine Momentaufnahmedifferenzsicherung einleiten, erstellt der NetApp-Dateiserver eine neue Differenzmomentaufnahme auf dem Datenträger, der gerade gesichert wird. Diese Differenzmomentaufnahme wird mit der Basismomentaufnahme (die vorherige Momentaufnahme) verglichen. Der Name der Basismomentaufnahme wurde bei Beendigung der vorherigen Sicherung auf dem IBM Spectrum Protect-Server registriert. Der Inhalt dieser Basismomentaufnahme wird mit der Differenzmomentaufnahme verglichen, die auf dem Datenträger des Quellen-Dateiservers erstellt wird. Unterschiede zwischen den beiden Momentaufnahmen werden auf dem Server gesichert.

Die Momentaufnahmedifferenzsicherung wird mit dem folgenden Befehl eingeleitet. Der Befehl wird an der Konsole eines Clientknotens eingegeben, der für den Zugriff auf die Datenträger auf dem Quellen-Dateiserver sowie für den Schutz dieser Datenträger konfiguriert ist. Da dieser Befehl für die Sicherung von Datenträgern auf einem Quellen-Dateiserver ausgegeben wird, wird eine neue Momentaufnahme (die Differenzmomentaufnahme) erstellt und die auf dem IBM Spectrum Protect-Server registrierte Momentaufnahme wird als Basismomentaufnahme verwendet. Die Erstellung sowohl der Differenzmomentaufnahme als auch der Basismomentaufnahme ist das Standardverhalten. Die Option `-diffsnapshot=create` ist ein Standardwert und muss in diesem Befehl nicht explizit angegeben werden.

```
dsmc incr \\ProdFiler\UserDataVol_Share -snapdiff -diffsnapshot=create
```

Daten auf einem Ziel-Dateiserver sichern

Eine typischere Konfiguration besteht darin, die Sicherungen vom Quellen-Dateiserver auszulagern. Hierbei werden Sicherungen der Quelldatenträger mithilfe der replizierten Datenträgermomentaufnahmen, die auf dem Ziel-Dateiserver gespeichert sind, erstellt. Gewöhnlich stellt die Sicherung eines Ziel-Dateiservers ein Problem dar, weil für die Erstellung einer Momentaufnahmedifferenzsicherung eine neue Momentaufnahme auf dem Datenträger, den Sie gerade sichern, erstellt werden muss. Die Datenträger des Ziel-Dateiservers, in denen der Inhalt der Quelldatenträger gespiegelt ist, sind schreibgeschützte Datenträger. Daher können auf ihnen keine Momentaufnahmen erstellt werden.

Um diese Einschränkung, die aufgrund des Schreibschutzes besteht, zu umgehen, werden Clientkonfigurationsoptionen zur Verfügung gestellt, mit denen Sie die vorhandenen Basis- und Differenzmomentaufnahmen auf dem schreibgeschützten Zieldatenträger verwenden können, um Änderungen auf dem IBM Spectrum Protect-Server zu sichern.

Wie in dem Szenario für den Quellen-Dateiserver erfolgt der Zugriff auf die Datenträger des Ziel-Dateiservers mithilfe von mit NFS exportierten Freigaben.

Zusammenfassung der Momentaufnahmedifferenzoptionen

Die Option `useexistingbase` bewirkt, dass die jüngste Momentaufnahme auf dem Datenträger als Basismomentaufnahme verwendet wird, wenn eine Basismomentaufnahme erstellt werden muss. Eine neue Basismomentaufnahme wird erstellt, wenn eine der folgenden Bedingungen erfüllt ist:

- Wenn diese Sicherung die Erstsicherung ist.
- Wenn `createnewbase=yes` angegeben ist.
- Wenn die Basismomentaufnahme, die durch eine vorherige Differenzmomentaufnahme registriert wurde, nicht mehr vorhanden ist und keine Momentaufnahme vorhanden ist, die älter als die fehlende Basismomentaufnahme ist.

Wenn diese Option nicht angegeben wird, wird eine neue Momentaufnahme auf dem Datenträger erstellt, der gesichert wird. Da Datenträger des Ziel-Dateiservers schreibgeschützt sind, muss `useexistingbase` bei der Erstellung von Momentaufnahmedifferenzsicherungen von Datenträgern des Ziel-Dateiservers angegeben werden. Wenn `useexistingbase` nicht angegeben wird, schlagen Momentaufnahmedifferenzsicherungen eines Datenträgers des Ziel-Dateiservers fehl, weil die neue Momentaufnahme auf dem schreibgeschützten Datenträger nicht erstellt werden kann.

Verwenden Sie bei der Sicherung von Datenträgern des Ziel-Dateiservers sowohl die Option `useexistingbase` als auch die Option `diffsnapshot=latest`, um sicherzustellen, dass während der Datenträgersicherung die neuesten Basis- und Differenzmomentaufnahmen verwendet werden.

Mit der Option `basesnapshotname` geben Sie an, welche Momentaufnahme auf dem Datenträger des Ziel-Dateiservers als Basismomentaufnahme verwendet werden soll. Wenn Sie diese Option nicht angeben, wird die jüngste Momentaufnahme auf dem Datenträger des Ziel-Dateiservers als Basismomentaufnahme verwendet. Den Namen der Basismomentaufnahme können Sie mithilfe von Platzhalterzeichen angeben.

Mit der Option `diffsnapshotname` können Sie angeben, welche Differenzmomentaufnahme auf dem Datenträger des Ziel-Dateiservers während einer Momentaufnahmedifferenzsicherung verwendet werden soll. Diese Option wird nur angegeben, wenn Sie auch `diffsnapshot=latest` angeben. Den Namen der Differenzmomentaufnahme können Sie mithilfe von Platzhalterzeichen angeben.

Die Option `diffsnapshot=latest` gibt an, dass Sie die neueste Momentaufnahme, die auf dem Dateiserver gefunden wird, als Quellenmomentaufnahme verwenden wollen.

Weitere Informationen zu diesen Optionen finden Sie in den Abschnitten der *Clientoptionsreferenz*.

Befehlsbeispiele für Momentaufnahmedifferenzsicherungen

In den nachfolgenden Beispielen wird davon ausgegangen, dass Datenträger auf einem Quellen-Dateiserver mithilfe der SnapMirror-Technologie von NetApp auf einem Dateiserver für die Wiederherstellung nach einem Katastrophenfall (Hostname DRFiler) repliziert werden. Da die Datenträger auf DRFiler schreibgeschützt sind, verwenden Sie die Optionen zur Angabe, welche der replizierten Momentaufnahmen als Basismomentaufnahme und welche der Momentaufnahmen als Differenzmomentaufnahme verwendet werden soll. Werden bei der Erstellung einer Momentaufnahmedifferenzsicherung eines Ziel-Dateiservers die zu verwendenden Momentaufnahmen angegeben, wird kein Versuch unternommen, eine Momentaufnahme auf den schreibgeschützten Datenträgern zu erstellen.

Die folgenden Befehle werden verwendet, um Momentaufnahmedifferenzsicherungen einzuleiten. Bei den meisten dieser Befehle werden Momentaufnahmedifferenz-

sicherungen mithilfe von Momentaufnahmen erstellt, die auf den Datenträgern des Ziel-Dateiservers gespeichert sind. Achten Sie bei der Sicherung von einem Datenträger des Ziel-Dateiservers darauf, dass die Option `-useexistingbase` angegeben wird, weil diese Option dafür sorgt, dass kein Versuch zur Erstellung einer neuen Momentaufnahme auf den schreibgeschützten Datenträgern des Ziel-Dateiservers unternommen wird.

Beispiel 1: Ziel-Dateiserversicherung in täglichen, durch den NetApp-Momentaufnahmescheduler erstellten Standardsicherungen durchführen

```
dsmc incr \\DRFiler\UserDataVol_Share -snapdiff -useexistingbase  
-diffsnapshot=latest -basesnapshotname="nightly.?"
```

Sie können ein Fragezeichen (?) als Entsprechung für ein einzelnes Zeichen verwenden. In diesem Beispiel wird durch die Angabe von `-basesnapshotname=nightly.?` die jüngste Basismomentaufnahme mit dem Teilnamen „nightly.“, an den sich ein einzelnes Zeichen anschließt (z. B. `nightly.0`, `nightly.1` etc.) verwendet.

Beispiel 2: Datenträger eines Ziel-Dateiservers mithilfe manuell (nicht durch den NetApp-Momentaufnahmescheduler) erstellter Momentaufnahmen sichern

```
dsmc incr \\DRFiler\UserDataVol_Share -snapdiff -useexistingbase  
-diffsnapshot=latest -basesnapshotname="share_vol_base?"  
-diffsnapshotname="share_vol_diff?"
```

Auch in diesem Beispiel wird das Fragezeichen (?) zur Veranschaulichung der Syntax verwendet, wenn die Namen der Basis- und der Differenzmomentaufnahme unterschiedliche Nummern enthalten.

Beispiel 3: Datenträger eines Ziel-Dateiservers sichern und die für die Basis- und Differenzmomentaufnahmen zu verwendenden Momentaufnahmen angeben

```
dsmc incr \\DRFiler\UserDataVol_Share -snapdiff -useexistingbase  
-diffsnapshot=latest -basesnapshotname="share_vol_base"  
-diffsnapshotname="share_vol_diff_snap"
```

Beispiel 4: Scriptgenerierte Momentaufnahmen sichern, die eine Namenskonvention verwenden

In diesem Beispiel fügt ein auf dem NetApp-Dateiserver ausgeführtes Script den Momentaufnahmenamen ein Datum und eine Zeitmarke hinzu. Eine am 3. November 2012 um 23:36:33 Uhr erstellte Momentaufnahme heißt beispielsweise `UserDataVol_20121103233633_snapshot`. Sie können Platzhalterzeichen in den Optionen verwenden, um die jüngsten Basis- und Differenzmomentaufnahmen auszuwählen. Beispiel:

```
dsmc incr \\DRFiler\UserDataVol_Share -snapdiff -useexistingbase  
-basesnapshotname="UserDataVol_Share_*_snapshot" -diffsnapshot=latest  
-diffsnapshotname="UserDataVol_Share_*_snapshot"
```

`-useexistingbase` wählt die jüngste Basismomentaufnahme aus. Wird in `-basesnapshotname` ein Stern (*) als Platzhalterzeichen hinzugefügt, wird die jüngste Basismomentaufnahme ausgewählt, die der Scriptnamenskonvention entspricht. Die Option `-diffsnapshot=latest` verhindert die Erstellung einer neuen Differenzmomentaufnahme und `-diffsnapshotname=` wählt die jüngste vorhandene Differenzmomentaufnahme aus, die der Scriptnamenskonvention entspricht. (Das Platzhalterzeichen * entspricht einer beliebigen Zeichenfolge.)

Beispiel 5: Momentaufnahmedifferenzsicherung mithilfe einer auf dem Quellen-Dateiserver vorhandenen Differenzmomentaufnahme durchführen

Soll eine auf dem Quellen-Dateiserver vorhandene Differenzmomentaufnahme verwendet werden, geben Sie `-diffsnapshot=latest` an, um die Er-

stellung einer neuen Differenzmomentaufnahme zu verhindern. Geben Sie außerdem die Option `-diffsnapshotname` an, um festzulegen, welche vorhandene Differenzmomentaufnahme verwendet werden soll. Die von Ihnen angegebene Momentaufnahme wird mit der Basismomentaufnahme verglichen, die bei der Erstellung der letzten Sicherung in der IBM Spectrum Protect-Serverdatenbank registriert wurde. Beispiel:

```
dsmc incr \\ProdFiler\UserDataVol_Share -snapdiff -diffsnapshot=latest  
-diffsnapshotname="share_vol_diff_snap"
```

Workstation bei einem Server registrieren

Damit Sie IBM Spectrum Protect verwenden können, müssen Sie einen Knotennamen und ein Kennwort definieren und Ihren Knoten beim Server registrieren.

Der Prozess, bei dem ein Knotenname und ein Kennwort definiert werden, wird als *Registrierung* bezeichnet. Es sind zwei Registrierungstypen verfügbar: *offene* und *geschlossene* Registrierung.

Der Registrierungstyp für Ihren Standort wird von Ihrem IBM Spectrum Protect-Serveradministrator ausgewählt.

Einschränkung: Ab IBM Spectrum Protect-Server der Version 8.1.2 ist die offene Registrierung nicht mehr verfügbar. Sie müssen die geschlossene Registrierung verwenden. Die offene Registrierung ist nur für IBM Spectrum Protect-Server der Version 8.1.1, 8.1.0, 7.1.7 oder früher verfügbar.

Sie müssen ein Root oder ein berechtigter Benutzer sein, um diese erforderliche Task auszuführen.

Wenn Sie planen, den Web-Client zu verwenden, benötigen Sie eine Benutzer-ID mit Administratorberechtigung, die über Systemberechtigung, Maßnahmenberechtigung, Clientzugriffsberechtigung oder Clienteignerberechtigung verfügt. Wenn ein neuer Knoten registriert wird, muss der Serveradministrator eine Benutzer-ID mit Administratorberechtigung erstellen, die mit dem Knotennamen übereinstimmt. Standardmäßig hat dieser Knoten Clienteignerberechtigung.

Der IBM Spectrum Protect-Serveradministrator muss den Parameter `userid` im Serverbefehl **REGISTER NODE** angeben:

```
REGISTER NODE Knotenname Kennwort userid=Benutzer-ID
```

Dabei müssen der Knotenname und die Benutzer-ID mit Administratorberechtigung übereinstimmen. Beispiel:

```
REGISTER NODE node_a mypassword userid=node_a
```

Geschlossene Registrierung

Bei der geschlossenen Registrierung muss der IBM Spectrum Protect-Administrator Ihre Workstation als Clientknoten beim Server registrieren. Verwendet Ihr Unternehmen die geschlossene Registrierung, müssen Sie Ihrem IBM Spectrum Protect-Administrator einige Informationen zur Verfügung stellen.

Informationen zu diesem Vorgang

Die folgenden Informationen müssen Sie Ihrem IBM Spectrum Protect-Administrator bereitstellen:

- Ihren Knotennamen (dies ist der vom Befehl **hostname** zurückgegebene Wert, der Name Ihrer Workstation oder der mit der Option **nodename** angegebene Knotenname). Wenn Sie keinen Knotennamen mit der Option **nodename** angeben, ist die Standardanmelde-ID der Name, den der Befehl **hostname** zurückgibt.
- Das gewünschte Anfangskennwort, falls erforderlich.
- Kontaktinformationen, wie z. B. Benutzername, Benutzer-ID und Rufnummer.

Ihr IBM Spectrum Protect-Administrator definiert Folgendes für Sie:

- Die Maßnahmendomäne, zu der der Clientknoten des Benutzers gehört. Eine Maßnahmendomäne enthält die Maßnahmengruppen und Verwaltungsklassen, die steuern, wie IBM Spectrum Protect die von Ihnen gesicherten und archivierten Dateien verwaltet.
- Ob Dateien komprimiert werden können, bevor sie an den Server gesendet werden.
- Ob der Benutzer Sicherungs- und Archivierungsdaten aus dem Serverspeicher löschen darf.

Offene Registrierung

Bei der offenen Registrierung kann ein Systemadministrator Ihre Workstation als Clientknoten beim IBM Spectrum Protect-Server der Version 8.1.1, 8.1.0, 7.1.7 oder früher registrieren.

Informationen zu diesem Vorgang

Beim ersten Start einer Sitzung werden Sie zur Eingabe von Informationen aufgefordert, die für die Registrierung Ihrer Workstation bei dem in Ihrer Clientoptionsdatei angegebenen IBM Spectrum Protect-Server erforderlich sind. Sie müssen den Knotennamen, ein Kennwort und Kontaktinformationen angeben.

Bei Verwendung der offenen Registrierung:

- Wird der Clientknoten des Benutzers der Maßnahmendomäne **Standard** zugeordnet.
- Können Archivierungskopien, jedoch keine Sicherungsversionen von Dateien aus dem Serverspeicher gelöscht werden.

Falls erforderlich, kann Ihr IBM Spectrum Protect-Administrator diese Standardwerte später ändern.

Einschluss-/Ausschlussliste erstellen

Wenn Sie keine Einschluss-/Ausschlussliste erstellen, berücksichtigt der Client für Sichern/Archivieren alle Dateien für Sicherungsservices und verwendet die Standardverwaltungsklasse für Sicherungs- und Archivierungsservices.

Informationen zu diesem Vorgang

Hierbei handelt es sich um eine optionale Task, die aber sehr wichtig ist.

Mithilfe einer Einschluss-/Ausschlussliste können bestimmte Dateien oder Dateigruppen von den Sicherungsservices ausgeschlossen und Dateien bestimmte Verwaltungsklassen zugeordnet werden. Der Client sichert jede Datei, die nicht explizit ausgeschlossen wurde. Sie sollten die IBM Spectrum Protect-Clientverzeichnisse von den Sicherungsservices ausschließen. Mit dem Befehl **query inclexcl** können

Sie eine Liste der Einschluss- und Ausschlussanweisungen in der Reihenfolge anzeigen, in der sie bei der Bestimmung, ob ein Objekt eingeschlossen werden soll, geprüft werden.

Geben Sie die Einschluss-/Ausschlussliste in Ihrer Datei dsm.sys an. Wenn mehrere Server in der Datei dsm.sys definiert sind, muss für jeden Server eine eigene Einschluss-/Ausschlussliste angegeben werden. In dieser Liste können auch Include/Exclude-Anweisungen aus Einschluss-/Ausschlussdateien enthalten sein, die Sie mit der Option `inclexcl` angeben.

Wenn der Client Include/Exclude-Anweisungen verarbeitet, werden die Include/Exclude-Anweisungen innerhalb der Einschluss-/Ausschlussdatei in derselben Reihenfolge an die Position in dsm.sys gestellt, die durch die Option `inclexcl` belegt ist, und entsprechend verarbeitet.

Vorgehensweise

Für das Erstellen einer Einschluss-/Ausschlussliste bzw. für die Angabe einer Einschluss-/Ausschlussdatei können Sie mit folgenden Methoden arbeiten:

- Sie können Einschluss-/Ausschlussanweisungen in der Verzeichnisstruktur der GUI des Clients für Sichern/Archivieren oder des Web-Clients hinzufügen. Die Onlinehilfe bietet detaillierte Anweisungen.
 1. Öffnen Sie das Menü **Editieren** und wählen Sie **Clientvorgaben** aus. Wählen Sie im Dialog 'Vorgaben' die Registerkarte **Einschluss/Ausschluss** aus. Sie können eine INCLEXCL-Datei über den Profileditor angeben. Über den Profileditor können Sie die INCLEXCL-Datei jedoch nicht erstellen.
 2. Erstellen Sie anhand der aufgelisteten Schritte die Einschluss-/Ausschlussliste manuell.
- Sie können eine Einschluss-/Ausschlussliste manuell erstellen, indem Sie die folgenden Schritte ausführen:
 1. Legen Sie Ihre Einschluss- und Ausschlussanforderungen fest.
 2. Lokalisieren Sie die Serverzeilengruppe in Ihrer Datei dsm.sys. Jede Serverzeilengruppe muss über eine eigene Einschluss-/Ausschlussliste verfügen.
 3. Geben Sie Ihre `include`- und `exclude`-Anweisungen ein. Der Client wertet *zuerst* alle Anweisungen `exclude.fs` und `exclude.dir` aus (unabhängig von ihrer Position in der Einschluss-/Ausschlussliste) und entfernt die ausgeschlossenen Dateibereiche, Verzeichnisse und Dateien aus der Liste der Objekte, die für die Verarbeitung verfügbar sind. Alle anderen Include/Exclude-Anweisungen werden vom Ende der Liste aufwärts zum Anfang verarbeitet. Deshalb ist es wichtig, alle Include/Exclude-Anweisungen in der richtigen Reihenfolge einzugeben. Mit der folgenden Einschluss-/Ausschlussliste wird die Datei `includefile.cpp` beispielsweise *nicht gesichert*:

```
include /Users/user01/Documents/includefile.cpp
exclude /Users/user01/Documents/.../*
```

Mit der folgenden Einschluss-/Ausschlussliste wird die Datei `includefile.cpp` jedoch gesichert:

```
exclude /Users/user01/Documents/.../*
include /Users/user01/Documents/includefile.cpp
```
 4. Die Datei sichern und schließen.

Für Mac OS X: Stellen Sie sicher, dass Sie die Datei als einfache, in Unicode (UTF-8 oder UTF-16) codierte Textdatei sichern. Fügen Sie nicht die Erweiterung `.txt` hinzu.

5. Starten Sie den Client erneut, um Ihre Einschluss-/Ausschlussliste zu aktivieren.

Zugehörige Konzepte:

„Hinweise für Clients, die für Unicode aktiviert wurden“ auf Seite 472

„Auszuschließende Systemdateien“ auf Seite 134

Kapitel 9, „Speicherverwaltungsmaßnahmen“, auf Seite 309

Zugehörige Verweise:

„Incl|excl“ auf Seite 471

Einschluss-/Ausschlussoptionen

Dieser Abschnitt enthält kurze Beschreibungen der Optionen `include` und `exclude`, die Sie in Ihrer Clientoptionsdatei angeben können, eine minimale Einschluss-/Ausschlussliste für den Ausschluss von Systemdateien, eine Liste der unterstützten Platzhalterzeichen und Beispiele für die Verwendung von Platzhalterzeichen in `include`- und `exclude`-Mustern.

Dateibereiche und Verzeichnisse ausschließen

Verwenden Sie Anweisungen `exclude.dir`, um alle Dateien und Unterverzeichnisse im angegebenen Verzeichnis von der Verarbeitung auszuschließen.

Der Client für Sichern/Archivieren wertet *zuerst* alle Anweisungen `exclude.dir` aus (unabhängig von ihrer Position in der Einschluss-/Ausschlussliste) und entfernt die ausgeschlossenen Verzeichnisse und Dateien aus der Liste der Objekte, die für die Verarbeitung verfügbar sind. Die Anweisungen `exclude.dir` überschreiben alle Include-Anweisungen, die mit dem Muster übereinstimmen.

In Tabelle 27 sind die Optionen aufgelistet, die Sie verwenden können, um Dateibereiche und Verzeichnisse von der Verarbeitung auszuschließen.

Tabelle 27. Optionen zum Ausschließen von Dateibereichen und Verzeichnissen

Option	Beschreibung
<code>exclude.fs</code> „Exclude-Optionen“ auf Seite 438	Mit dem Muster übereinstimmende Dateibereiche werden ausgeschlossen. Vom Client wird der angegebene Dateibereich bei der Verarbeitung nicht berücksichtigt, und die gewöhnliche Verfallsverarbeitung gelöschter Dateien findet nicht statt. Wenn Sie einen Dateibereich ausschließen, der zuvor eingeschlossen war, bleiben bestehende Sicherungsversionen auf dem Server und unterliegen den Aufbewahrungszeitregeln, die in der zugeordneten Verwaltungsklassendefinition angegeben sind.

Tabelle 27. Optionen zum Ausschließen von Dateibereichen und Verzeichnissen (Forts.)

Option	Beschreibung
exclude.dir „Exclude-Optionen“ auf Seite 438	<p>Schließt ein Verzeichnis, seine Dateien sowie alle zugehörigen Unterverzeichnisse und ihre Dateien von der Sicherungsverarbeitung aus. Beispiel: Die Anweisung <code>exclude.dir /test/dan/data1</code> schließt das Verzeichnis <code>/test/dan/data1</code>, dessen Dateien und Unterverzeichnisse sowie die Dateien in den Unterverzeichnissen aus. Die Verwendung der Option <code>exclude.dir</code> ist der Standardoption <code>exclude</code> vorzuziehen, wenn große Verzeichnisse mit vielen Dateien, die Sie nicht sichern wollen, ausgeschlossen werden sollen. Sie können keine Include-Optionen verwenden, um eine Anweisung <code>exclude.dir</code> zu überschreiben. Verwenden Sie <code>exclude.dir</code> nur, wenn Sie einen gesamten Verzeichniszweig ausschließen wollen.</p> <ul style="list-style-type: none"> • Verwenden Sie die folgenden Anweisungen, um die Datenträger <code>/Volumes/disk2</code> insgesamt von der Sicherungsverarbeitung auszuschließen. Beachten Sie, dass der Datenträger (<code>/Volumes/disk2</code>) trotzdem gesichert wird, aber alle anderen Verzeichnisse auf <code>/Volumes/disk2</code> ausgeschlossen werden. <pre>exclude /Volumes/disk2/* exclude.dir /Volumes/disk2/*</pre> • Ein Alternativverfahren zum Ausschließen eines vollständigen Datenträgers von der Domänenteilsicherung wäre die Verwendung einer Domänenanweisung, um den Datenträger auszuschließen. Zum Beispiel: <pre>domain "-/Volumes/disk2"</pre> <p>Diese Alternative erlaubt dennoch eine selektive Sicherungsverarbeitung von Dateien auf <code>/Volumes/disk2</code>.</p>

Dateien und Verzeichnisse von einer journalbasierten Sicherung ausschließen

Es gibt zwei Methoden, Dateien und Verzeichnisse von einer journalbasierten Sicherung auszuschließen.

- Unter AIX und Linux werden bei der einen Methode der Clientoptionsdatei `Exclude`-Anweisungen hinzugefügt, um zu verhindern, dass die Dateien oder Verzeichnisse während der Sicherungsverarbeitung gesichert werden.
- Unter AIX und Linux werden bei der anderen Methode `Exclude`-Anweisungen zur Journalkonfigurationsdatei `tsmjbbd.ini` hinzugefügt, um zu verhindern, dass Journaleinträge für die Dateien oder Verzeichnisse hinzugefügt werden, die sie daran hindern, während einer journalbasierten Sicherung verarbeitet zu werden. Wenn Sie AIX Version 6.1 oder später ausführen, fügen Sie die Anweisung `exclude .snapshot` zur Datei `tsmjbbd.ini` hinzu, um zu verhindern, dass interne JFS2-Momentaufnahmeverzeichnisse vom Dämon für die journalbasierte Sicherung überwacht werden.

Anmerkung: Es besteht keine Korrelation zwischen den beiden `Exclude`-Anweisungen. Die bevorzugte Position für `Exclude`-Anweisungen ist die Datei `tsmjbbd.ini`. Dies verhindert, dass sie Eingang in die Journaldatenbank finden und während einer journalbasierten Sicherung verarbeitet werden.

Verarbeitung mit Ausschlussanweisungen steuern

Nachdem der Client alle Ausschlussanweisungen ausgewertet hat, werden die folgenden Optionen mit der Liste der verbleibenden Objekte abgeglichen, die für die Verarbeitung verfügbar sind.

In Tabelle 28 sind die Optionen aufgelistet, die Sie verwenden können, um die Verarbeitung mit Include- und Exclude-Anweisungen zu steuern.

Tabelle 28. Optionen zur Verarbeitungssteuerung mit Include- und Exclude-Anweisungen

Option	Beschreibung	Seite
Sicherungsverarbeitung		
exclude exclude.backup exclude.file exclude.file.backup	<i>Diese Optionen sind äquivalent.</i> Mit diesen Exclude-Optionen können Sie eine Datei oder Dateigruppe von den Sicherungsservices und von den Speicherverwaltungsservices (wenn der HSM-Client installiert ist) ausschließen. Die Option exclude.backup schließt Dateien nur von der normalen Sicherung aus, nicht von HSM.	auf Seite 438
include include.backup include.file	Mit diesen Include-Optionen können Sie Dateien einschließen oder Verwaltungsklassen für die Sicherungsverarbeitung zuordnen.	auf Seite 473
include.fs	Steuert, wie der Client Ihren Dateibereich für Teilsicherungen verarbeitet.	„Include-Optionen“ auf Seite 473
Archivierungsverarbeitung		
exclude.archive	Schließt eine Datei oder Dateigruppe von den Archivierungsservices aus.	„Exclude-Optionen“ auf Seite 438
include include.archive	<i>Diese Optionen sind äquivalent.</i> Mit diesen Include-Optionen können Dateien eingeschlossen oder Verwaltungsklassen für die Archivierungsverarbeitung zugeordnet werden.	auf Seite 473
Imageverarbeitung		
exclude.fs.nas	Bei Verwendung im Befehl backup nas werden Dateisysteme auf dem NAS-Dateiserver von der Imagesicherung ausgeschlossen. Wenn Sie keinen NAS-Knotennamen angeben, gilt das angegebene Dateisystem für alle NAS-Dateiserver. Der Befehl backup nas ignoriert alle anderen Exclude-Anweisungen einschließlich der Anweisungen exclude.fs und exclude.dir . Diese Option ist <i>nur</i> für AIX- und Solaris-Clients gültig.	„Exclude-Optionen“ auf Seite 438
exclude.image	Schließt angehängte Dateisysteme und unformatierte logische Datenträger, die dem angegebenen Muster entsprechen, von den Imagesicherungsoperationen aus. Imageteilsicherungsoperationen sind von exclude.image nicht betroffen. Diese Option ist für AIX-, Solaris- und alle Linux-Clients gültig.	„Exclude-Optionen“ auf Seite 438
include.fs.nas	Verwenden Sie die Option include.fs.nas , um Verwaltungsklasse an NAS-Dateisysteme zu binden. Um anzugeben, ob der Client während einer Imagesicherung des NAS-Dateisystems Inhaltsverzeichnisinformationen (TOC-Informationen) speichert, verwenden Sie die Option toc mit der Option include.fs.nas in Ihrer Datei dsm.sys . Weitere Informationen finden Sie in „Toc“ auf Seite 619. Diese Option ist <i>nur</i> für AIX- und Solaris-Clients gültig.	„Include-Optionen“ auf Seite 473

Tabelle 28. Optionen zur Verarbeitungssteuerung mit Include- und Exclude-Anweisungen (Forts.)

Option	Beschreibung	Seite
include.image	Schließt einen Dateibereich oder einen logischen Datenträger ein, ordnet eine Verwaltungsklasse zu oder ermöglicht es, einem bestimmten logischen Datenträger eine oder mehrere Optionen für die Imagesicherungsverarbeitung zuzuordnen, wenn die Option zusammen mit dem Befehl backup image verwendet wird. Der Befehl backup image ignoriert alle anderen Include-Optionen. Diese Option ist nur für AIX, Solaris, Linux x86_64 und Linux on POWER gültig.	473

Auszuschließende Systemdateien

Einige Systemdateien sollten in die Clientoptionsdatei gestellt werden, sodass sie ausgeschlossen werden.

Achtung: Diese Systemdateien sind entweder vom Betriebssystem gesperrt oder können beim Zurückschreiben Probleme verursachen. Hierbei handelt es sich um Systemdateien, die nicht wiederhergestellt werden können, ohne das Betriebssystem möglicherweise zu beschädigen, oder um temporäre Dateien mit Daten, die Sie problemlos erneut erstellen können.

Anmerkung: Dieser Abschnitt gilt nur für Mac OS X.

Die implizit generierten Anweisungen können in den Ausgabezeilen des Befehls **query inclexcl** mit der Quelle "Betriebssystem" eingesehen werden.

Der Client für Sichern/Archivieren fügt der Einschluss-/Ausschlussliste Ihrer Datei dsm.sys die folgenden Ausschlussanweisungen hinzu. Schließen Sie keine dieser Anweisungen in der Datei dsm.sys ein, sonst kommt es zu doppelten Einträgen.

```
EXCLUDE.ARCHIVE "/.../Desktop DB"
EXCLUDE.BACKUP "/.../Desktop DB"
EXCLUDE.ARCHIVE "/.../Desktop DF"
EXCLUDE.BACKUP "/.../Desktop DF"
EXCLUDE.ARCHIVE /.vol
EXCLUDE.BACKUP /.vol
EXCLUDE.ARCHIVE /automount
EXCLUDE.BACKUP /automount
EXCLUDE.ARCHIVE /Network
EXCLUDE.BACKUP /Network
EXCLUDE.ARCHIVE /dev
EXCLUDE.BACKUP /dev
EXCLUDE.BACKUP /.vol/.../*
EXCLUDE.ARCHIVE /.vol/.../*
EXCLUDE.BACKUP /automount/.../*
EXCLUDE.ARCHIVE /automount/.../*
EXCLUDE.BACKUP /Network/.../*
EXCLUDE.ARCHIVE /Network/.../*
EXCLUDE.BACKUP /dev/.../*
EXCLUDE.ARCHIVE /dev/.../*
EXCLUDE.DIR /.vol
EXCLUDE.DIR /automount
EXCLUDE.DIR /Network
EXCLUDE.DIR /dev
```

Anmerkung:

1. Geben Sie keine Datenträger an, deren Name Punkte enthält (...). Der Client für Sichern/Archivieren verwendet die Punktesequenz als Teil der Einschluss-/Ausschlussverarbeitung. Der Client meldet eine ungültige Einschluss-/Ausschlussanweisung zurück, wenn ein Datenträgername eine Punktesequenz enthält. Der Datenträger *muss* umbenannt werden.
2. Objekte mit dem Typ 'rhap' und dem Ersteller 'lcmt' werden von der Verarbeitung ausgeschlossen. Im Allgemeinen sind dies spezielle Dateisystemobjekte, die auch mit dem Befehl **mknod** erstellt werden können, oder sind UNIX-Mountpunkte. Die Objekte oder Mountpunkte müssen als Teil einer vollständigen Systemzurückschreibung manuell erneut erstellt werden.

Ihre Einschluss-/Ausschlussoptionsdatei sollte mindestens die folgende Einschluss-/Ausschlussliste umfassen:

```
EXCLUDE    /.../dsmsched.log
EXCLUDE    /.../dsmprune.log
EXCLUDE    /.../dsmj.log
EXCLUDE    /.../dsmerror.log
EXCLUDE    /.../.hotfiles.bTree

EXCLUDE.DIR /private/tmp
EXCLUDE.DIR /private/var/vm
EXCLUDE.DIR /private/var/tmp
EXCLUDE.DIR /private/var/db/netinfo/local.nidb

EXCLUDE.DIR /.../.Trashes
EXCLUDE.DIR /.../.Spotlight-*
EXCLUDE.DIR /.../Library/Caches
EXCLUDE.DIR /.../.fsevents
```

Dateien mit Platzhalterzeichen einschließen und ausschließen

Sie müssen besondere Escapezeichen verwenden, wenn Sie Dateien und Verzeichnisse einschließen oder ausschließen, deren Namen Platzhalterzeichen enthalten.

Der Client für Sichern/Archivieren behandelt Platzhalterzeichen auf verschiedenen Plattformen unterschiedlich.

Die Namen von Verzeichnissen und Dateien können verschiedene Symbole enthalten. Welche Typen von Symbolen zulässig sind, ist vom Betriebssystem abhängig.

Unter AIX können die Namen von Verzeichnissen oder Dateien beispielsweise die folgenden Symbole enthalten:

```
* ? : [ ]
```

Bei der Angabe von Dateien und Verzeichnissen in Include- und Exclude-Anweisungen müssen Sie das Escapezeichen "\" verwenden, um die Platzhalterzeichen anzugeben. Das Escapezeichen kann jedoch nur innerhalb der Zeichenklassen "[]" verwendet werden.

Die folgenden Beispiele zeigen, wie Dateien und Verzeichnisse, deren Namen Platzhalterzeichen enthalten, in Include/Exclude-Anweisungen mit dem Escapezeichen und Zeichenklassen anzugeben sind.

Zum Ausschließen des einzelnen Verzeichnisses /usr1/[dir2] von der Sicherungsverarbeitung geben Sie Folgendes in die Datei dsm.sys oder in die Einschluss-/Ausschlussdatei ein:

```
exclude.dir "/usr1/[\\[\\dir2\\]]"
```

Zum Ausschließen der einzelnen Datei /usr1/fi*le1 von der Sicherungsverarbeitung geben Sie die folgende Anweisung in die Datei dsm.sys oder in die Einschluss-/Ausschlussdatei ein:

```
exclude "/usr1/fi[\\*]le1"
```

Tipp: Wenn Sie den Profileditor verwenden, um eine einzelne Datei oder ein einzelnes Verzeichnis einzuschließen, deren bzw. dessen Name Platzhalterzeichen enthält, müssen Sie die Include- oder Exclude-Anweisung manuell editieren, um das Escapezeichen für das Platzhalterzeichen einzufügen. Der Profileditor fügt nicht automatisch Escapezeichen für Platzhalterzeichen ein. Orientieren Sie sich beim Editieren der Include- oder Exclude-Anweisungen in der Datei dsm.sys oder in der Einschluss-/Ausschlussdatei an den obigen Beispielen.

Zugehörige Konzepte:

„Platzhalterzeichen“ auf Seite 691

Dateigruppen mit Platzhalterzeichen einschließen und ausschließen

Sie können Platzhalterzeichen verwenden, um Dateigruppen einzuschließen oder auszuschließen.

Verwenden Sie die Platzhalterzeichen, die in der folgenden Tabelle aufgelistet sind, um Dateigruppen anzugeben, die Sie einschließen oder ausschließen wollen. Diese Tabelle gilt *nur* für Anweisungen include und exclude.

Eine sehr große Einschluss-/Ausschlussliste kann die Leistung bei der Sicherung beeinträchtigen. Verwenden Sie Platzhalterzeichen, um unnötige Include-Anweisungen zu vermeiden und den Umfang der Liste zu verringern.

Tabelle 29. Platzhalterzeichen und andere Sonderzeichen

Zeichen	Funktion
?	Das Platzhalterzeichen für ein Zeichen entspricht einem beliebigen Einzelzeichen, <i>mit Ausnahme</i> des Verzeichnistrennzeichens. Es entspricht nicht dem Ende der Zeichenfolge. Zum Beispiel: <ul style="list-style-type: none"> Das Muster ab? entspricht abc, aber entspricht nicht ab, abab oder abzzz. Das Muster ab?rs entspricht abfrs, aber entspricht nicht abrs oder abllrs. Das Muster ab?ef?rs entspricht abdefjrs, aber entspricht nicht abefrs, abdefrs oder abefjrs. Das Muster ab??rs entspricht abcdrs oder abzzrs, aber entspricht nicht abrs, abjrs oder abkkrs.
*	Das Platzhalterzeichen für alle Zeichen. Zum Beispiel: <ul style="list-style-type: none"> Das Muster ab* entspricht ab, abb oder abxxx, aber entspricht nicht a, b, aa, bb. Das Muster ab*rs entspricht abrs, abtrs oder abrsrs, aber entspricht nicht ars, aabrs oder abrss. Das Muster ab*ef*rs entspricht abefrs oder abefghrs, aber entspricht nicht abefr, abers. Das Muster abcd.* entspricht abcd.c oder abcd.txt, aber entspricht nicht abcd, abcdc oder abcdtxt.
/...	Das Platzhalterzeichen für <i>n</i> Zeichen entspricht null oder mehr Verzeichnissen.
[Mit dem Anfangszeichen für die Zeichenklasse wird die Aufzählung einer Zeichenklasse begonnen. Beispiel: <pre>xxx[abc] entspricht xxxa, xxxb oder xxxc.</pre>

Tabelle 29. Platzhalterzeichen und andere Sonderzeichen (Forts.)

Zeichen	Funktion
–	Das Zeichen für den Zeichenklassenbereich umfasst die Zeichen vom ersten angegebenen Zeichen bis zum letzten angegebenen Zeichen. Beispiel: xxx[a-z] entspricht xxxa, xxxb, xxxc, ... xxxz.
\	Das Literal-Escapezeichen. Wird das Literal-Escapezeichen in einer Zeichenklasse verwendet, wird das nächste Zeichen wörtlich behandelt. Außerhalb einer Zeichenklasse wird es nicht auf diese Weise behandelt. Soll beispielsweise ']' in eine Zeichenklasse eingeschlossen werden, ist [...\]] einzugeben. Das Escapezeichen löscht die normale Bedeutung von ']' als Zeichen zum Schließen der Zeichenklasse.
]	Mit dem Endzeichen für die Zeichenklasse wird die Aufzählung einer Zeichenklasse beendet.

Zugehörige Konzepte:

„Platzhalterzeichen“ auf Seite 691

Beispiele für Platzhalterzeichen in Einschluss- und Ausschlussmustern

Der Client für Sichern/Archivieren akzeptiert die Option `exclude.dir`, mit der Verzeichniseinträge ausgeschlossen werden können. Die Optionen `include` und `exclude.dir` können jedoch nicht gemeinsam verwendet werden.

Anmerkung: In der Datei `dsm.sys` funktionieren die Optionen `include` und `exclude` nicht mit symbolischen Verbindungen auf Verzeichnisse. Beispiel: Verwenden Sie in Ihren Include- oder Exclude-Anweisungen nicht `/u`, da `/u` eine symbolische Verbindung für das Verzeichnis `/home` darstellt. Anstelle von:

```
include /u/tmp/save.fil
```

Folgendes eingeben:

```
include /home/tmp/save.fil
```

Die Option `exclude` funktioniert jedoch mit symbolischen Verbindungen zu Verzeichnissen, wenn Sie einen Sicherungsbefehl mit dem absoluten Pfad eingeben, der die symbolische Verbindung enthält.

Tabelle 30 zeigt die Verwendung von Platzhalterzeichen zum Einschließen oder Ausschließen von Dateien.

Tabelle 30. Platzhalterzeichen in Include- und Exclude-Mustern verwenden

Task	Muster
Alle Dateien ausschließen, die mit <code>.doc</code> enden, mit Ausnahme der Dateien im Verzeichnis <code>Documents</code> im Ausgangsverzeichnis von <code>aleko</code> .	EXCLUDE <code>/.../*.doc</code> INCLUDE <code>"/home/aleko/Documents/*.doc"</code>
Alle Dateien mit der Erweiterung <code>bak</code> während der Sicherung ausschließen, mit Ausnahme der Dateien, die sich im Dateisystem <code>/usr</code> im Verzeichnis <code>dev</code> befinden.	exclude <code>/.../*.bak</code> include <code>/usr/dev/*.bak</code>
Alle Dateien und Ordner unter allen vorhandenen Ordnern <code>Documents</code> ausschließen; die Datei <code>Current</code> des Benutzers <code>aleko</code> soll hiervon <i>ausgenommen</i> werden.	EXCLUDE <code>/.../Documents/.../*</code> INCLUDE <code>"/home/aleko/Documents/Current"</code>

Tabelle 30. Platzhalterzeichen in Include- und Exclude-Mustern verwenden (Forts.)

Task	Muster
Alle Dateien in allen Verzeichnissen mit dem Namen "tmp" und ihren Unterverzeichnissen ausschließen; die Datei /home/tmp/save.fil soll hiervon <i>ausgenommen</i> werden.	exclude /.../tmp/.../* include /home/tmp/save.fil
Alle Dateien mit der Erweiterung .cpp in allen Verzeichnissen auf den Datenträgern Vol1, Vol2, Vol3 und Vol4 ausschließen.	EXCLUDE /Volumes/Vol[1-4]/.../*.cpp
Alle Dateien mit der Erweiterung .cpp in allen Verzeichnissen auf den Datenträgern Vol1, Vol2, Vol3 und Vol4 ausschließen.	EXCLUDE /Volumes/Vol[1-4]/.../*.cpp
Alle Dateien mit der Erweiterung .cpp in allen Verzeichnissen in den Dateisystemen /fs1, /fs2, /fs3 und /fs4 ausschließen.	EXCLUDE /fs[1-4]/.../*.cpp
Die Dateien mit der Erweiterung .cpp im Verzeichnis /fs2/source ausschließen.	EXCLUDE /fs2/source/*.cpp
Alle Dateien mit der Erweiterung .o in allen Verzeichnissen in den Dateisystemen /usr1, /usr2 und /usr3 ausschließen.	exclude /usr[1-3]/.../*.o
Nur die Dateien mit der Erweiterung .o ausschließen, die sich im Stammverzeichnis des Dateisystems usr2 befinden.	exclude /usr2/*.o
Alle Dateien ausschließen, die sich unter dem Verzeichnis tmp in einem beliebigen Dateisystem befinden.	exclude /.../tmp/.../*
Die vollständige Verzeichnisstruktur /var/spool von der gesamten Verarbeitung ausschließen.	exclude.dir /var/spool
Ein einzelnes Dateisystem von der Sicherungsverarbeitung ausschließen.	exclude.fs /fs1 exclude.fs home:
Alle Dateisysteme von der Sicherungsverarbeitung ausschließen, die an einer beliebigen Position in der Verzeichnisbaumstruktur /test/myfs/fs01 und /test/myfs/fs02 angehängt sind.	exclude.fs /test/myfs/fs01/.../* exclude.fs /test/myfs/fs02/*
Das Verzeichnis /home/mydir/test1 und alle Dateien und Unterverzeichnisse unter diesem Verzeichnis ausschließen.	exclude.dir /home/mydir/test1
Alle Verzeichnisse unter dem Verzeichnis /home/mydir ausschließen, deren Name mit test beginnt.	exclude.dir /home/mydir/test*
In allen Dateisystemen alle Verzeichnisse direkt unter dem Verzeichnis /mydir ausschließen, deren Name mit test beginnt.	exclude.dir /.../mydir/test*
Den unformatierten logischen Datenträger von der Imagesicherung ausschließen.	exclude.image /dev/hd0
Alle symbolischen Verbindungen oder Aliasnamen (Aliasnamen gelten für Mac OS X) von der Sicherungsverarbeitung ausschließen, außer dem Verzeichnis Docs für user1.	EXCLUDE.ATTRIBUTE.SYMLINK /.../* INCLUDE.ATTRIBUTE.SYMLINK /Users/user1/Docs/*

Zugehörige Konzepte:

„Beispiele für Platzhalterzeichen in Einschluss- und Ausschlussmustern“ auf Seite 137

Zugehörige Verweise:

„Exclude-Optionen“ auf Seite 438

Verarbeitung von symbolischen Verbindungen und Aliasnamen

Der Client für Sichern/Archivieren wertet alle Anweisungen `exclude.fs` und `exclude.dir` aus und entfernt die ausgeschlossenen Dateibereiche und Verzeichnisse.

Nach diesem ersten Auswertungsschritt wertet der Client alle Einschluss-/Ausschlussanweisungen für die Steuerung der Verarbeitung von symbolischen Verbindungen und Aliasnamen (`exclude.attribute.symlink` und `include.attribute.symlink`) aus und gleicht sie mit der verbleibenden Liste der Objekte ab, die für die Verarbeitung verfügbar sind.

Die Verarbeitung von Aliasnamen gilt für Mac OS X.

Tabelle 31 definiert Optionen für die Steuerung der Verarbeitung von symbolischen Verbindungen und Aliasnamen.

Tabelle 31. Optionen für das Steuern der Verarbeitung von symbolischen Verbindungen und Aliasnamen

Option	Beschreibung	Seite
<code>exclude.attribute.symlink</code>	Schließt eine Datei oder Dateigruppe, bei denen es sich um symbolische Verbindungen oder Aliasnamen handelt, nur von der Sicherungsverarbeitung aus.	„Exclude-Optionen“ auf Seite 438
<code>include.attribute.symlink</code>	Schließt eine Datei oder Dateigruppe, bei denen es sich um symbolische Verbindungen oder Aliasnamen handelt, innerhalb einer größeren Gruppe von ausgeschlossenen Dateien nur für die Sicherungsverarbeitung ein.	„Include-Optionen“ auf Seite 473

Komprimierungs- und Verschlüsselungsverarbeitung festlegen

Der Client für Sichern/Archivieren wertet die Option `exclude.dir` und andere Einschluss-/Ausschlussoptionen, die die Sicherungs- und Archivierungsverarbeitung steuern, aus und legt dann fest, für welche Dateien die Komprimierungs- und Verschlüsselungsverarbeitung ausgeführt wird.

Die folgenden Optionen bestimmen, für welche Dateien die Komprimierungs- und Verschlüsselungsverarbeitung ausgeführt wird.

Tabelle 32. Optionen für die Steuerung der Komprimierung und Verschlüsselung

Option	Beschreibung	Seite
Komprimierungsverarbeitung		
<code>exclude.compression</code>	Schließt Dateien von der Komprimierungsverarbeitung aus, wenn <code>compression=yes</code> angegeben ist. Diese Option gilt für Sicherungen und Archivierungen.	„Exclude-Optionen“ auf Seite 438

Tabelle 32. Optionen für die Steuerung der Komprimierung und Verschlüsselung (Forts.)

Option	Beschreibung	Seite
include.compression	Schließt Dateien für die Komprimierungsverarbeitung ein, wenn <code>compression=yes</code> angegeben ist. Diese Option gilt für Sicherungen und Archivierungen.	„Include-Optionen“ auf Seite 473
Verschlüsselungsverarbeitung		
exclude.encrypt	Schließt Dateien von der Verschlüsselungsverarbeitung aus.	„Exclude-Optionen“ auf Seite 438
include.encrypt	Schließt Dateien für die Verschlüsselungsverarbeitung ein. Die Daten, die Sie einschließen, werden in verschlüsselter Form gespeichert; die Verschlüsselung hat keine Auswirkungen auf das gesendete oder empfangene Datenvolumen. Wichtig: Die Option <code>include.encrypt</code> ist die einzige Möglichkeit, die Verschlüsselung auf dem Client für Sichern/Archivieren zu aktivieren. Werden keine Anweisungen <code>include.encrypt</code> verwendet, findet keine Verschlüsselung statt.	„Include-Optionen“ auf Seite 473

Dateien in der Einschluss-/Ausschlussliste voranzeigen

Sie können die Liste der Objekte, die gemäß der Einschluss-/Ausschlussliste gesichert oder archiviert werden sollen, vor dem Senden von Daten an den Server in einer Voranzeige aufrufen.

Die Verzeichnisstruktur in der GUI des Clients für Sichern/Archivieren zeigt detaillierte Informationen zu eingeschlossenen und ausgeschlossenen Objekten an. In den Verzeichnisstrukturfenstern der GUI des Clients für Sichern/Archivieren können Sie Dateien und Verzeichnisse auswählen, die eingeschlossen oder ausgeschlossen werden sollen. Sie sollten diesen Befehl **preview** verwenden, um sicherzustellen, dass Sie die richtigen Dateien einschließen und ausschließen. Im Folgenden wird ein Beispielszenario für die Verwendung der Funktion 'Voranzeige für Einschluss/Ausschluss' aufgeführt.

Beispiel: Führen Sie die folgenden Schritte aus, um die Dateien in Ihrem Dateibereich `/Users/home` zu sichern:

1. Starten Sie die GUI des Clients für Sichern/Archivieren und öffnen Sie die Baumstruktur für Sichern. Sie können alle Verzeichnisse und Dateien sehen, die von Ihrer Optionsdatei und anderen Quellen ausgeschlossen wurden.
2. Blättern Sie in der Baumstruktur abwärts. Sie stellen fest, dass alle `*.o`-Dateien in `/Volumes/home/mary/myobjdir` gesichert werden.
3. Sie wollen die `*.o`-Dateien nicht sichern. Also klicken Sie mit der rechten Maustaste auf eine `.o`-Datei und wählen "Dateiinformationen anzeigen" im Popup-Menü aus.
4. Der Dialog zeigt an, dass diese Dateien eingeschlossen sind. Daher klicken Sie auf die Schaltfläche "Erweitert" und erstellen eine Regel, um alle `.o`-Dateien im Dateibereich `DATA:\home` auszuschließen.

5. Am Ende Ihrer Optionsdatei wird eine Regel erstellt. Das aktuelle Verzeichnis wird in der Baumstruktur für Sichern aktualisiert und die Dateien .o werden mit einem roten 'X' markiert; dies gibt an, dass die Dateien ausgeschlossen sind.
6. Wenn Sie andere Verzeichnisse ansehen, zeigen diese die von Ihnen hinzugefügten neuen Ausschlüssen. Klicken Sie auf "Sichern" und sichern Sie die Dateien in Ihrem Dateibereich /home.

Zugehörige Verweise:

„**Preview Archive**“ auf Seite 742

„**Preview Backup**“ auf Seite 744

Verarbeitung von Einschluss- und Ausschlussoptionen

Der IBM Spectrum Protect-Server kann Include/Exclude-Optionen mithilfe des Parameters `incl excl` in einer Clientoptionsgruppe definieren.

Die vom Server angegebenen Include/Exclude-Anweisungen werden zusammen mit den Include/Exclude-Anweisungen in der Clientoptionsdatei ausgewertet. Die Server-Include-Exclude-Anweisungen werden immer erzwungen und an das Ende der Einschluss-/Ausschlussliste gestellt und somit vor den Client-Include-Exclude-Anweisungen ausgewertet.

Wenn die Einschluss-/Ausschlussliste in der Datei `dsm.sys` eine oder mehrere Optionen `incl excl` enthält, die Einschluss-/Ausschlussdateien angeben, werden die Include/Exclude-Anweisungen in diesen Dateien an der Position in die Liste eingefügt, an der sich die zugehörige Option `incl excl` befindet, und entsprechend verarbeitet.

Eine sehr große Einschluss-/Ausschlussliste kann die Leistung bei der Sicherung beeinträchtigen. Verwenden Sie Platzhalterzeichen, um unnötige Include-Anweisungen zu vermeiden und den Umfang der Liste zu verringern.

Bei einer Teilsicherung wertet der Client zuerst alle Anweisungen `exclude.fs` und `exclude.dir` aus und entfernt die ausgeschlossenen Dateibereiche, Verzeichnisse und Dateien aus der Liste der Objekte, die für die Verarbeitung verfügbar sind.

Nach der Auswertung aller Anweisungen `exclude.fs` und `exclude.dir` wertet der Client die Einschluss-/Ausschlussanweisungen zur Steuerung der Verarbeitung symbolischer Verbindungen oder Aliasnamen (`exclude.attribute.symlink` und `include.attribute.symlink`) von unten nach oben aus und stoppt, wenn eine Einschluss-/Ausschlussanweisung gefunden wird, die mit der Datei übereinstimmt, die gerade verarbeitet wird. Nach der Verarbeitung der Einschluss-/Ausschlussanweisungen zur Steuerung der Verarbeitung symbolischer Verbindungen oder Aliasnamen wertet der Client die verbleibende Einschluss-/Ausschlussliste von unten nach oben aus und stoppt, wenn eine Einschluss- oder Ausschlussanweisung gefunden wird, die mit der Datei übereinstimmt, die gerade verarbeitet wird. Die Reihenfolge, in der die Einschluss- und Ausschlussoptionen eingegeben werden, hat daher Einfluss darauf, welche Dateien eingeschlossen und welche Dateien ausgeschlossen werden.

Zum Anzeigen einer Liste, in der alle auf der Client-Workstation aktiven Include/Exclude-Anweisungen in der tatsächlichen Reihenfolge aufgeführt sind, in der sie verarbeitet werden, den Befehl **query incl excl** verwenden.

Das Clientprogramm verarbeitet die Liste der Include/Exclude-Anweisungen anhand folgender Regeln:

1. Dateien werden überprüft; Verzeichnisse werden nur überprüft, wenn die Option `exclude.dir` angegeben ist.
2. Dateinamen werden von unten nach oben mit den Mustern in der Einschluss-/Ausschlussliste abgeglichen. Wird eine Übereinstimmung gefunden, stoppt die Verarbeitung, und es wird überprüft, ob die Option `include` oder `exclude` lautet. Lautet die Option `include`, wird die Datei gesichert. Lautet die Option `exclude`, wird die Datei nicht gesichert.

Anmerkung: Wird keine Übereinstimmung gefunden, werden die Dateien implizit eingeschlossen und gesichert.

3. Wird eine Datei gesichert, wird sie an die Standardverwaltungsklasse gebunden, sofern sie nicht mit einer Anweisung `include` übereinstimmt, die einen anderen Verwaltungsklassennamen angegeben hat; in letzterem Fall wird sie an die angegebene Verwaltungsklasse gebunden.

Die folgenden Beispiele veranschaulichen die Verarbeitung von unten nach oben.

Beispiel 1

Nehmen wir an, La Pomme ist nicht der Startdatenträger.

```
EXCLUDE ../*.cpp
INCLUDE "/Volumes/La Pomme/Foo/.../*.cpp"
EXCLUDE "/Volumes/La Pomme/Foo/Junk/*.cpp"
```

Folgende Datei wird gerade verarbeitet: `/Volumes/La Pomme/Foo/Dev/test.cpp`. Folgende Verarbeitungsschritte werden durchgeführt:

1. Regel 3 (die letzte definierte Anweisung `include` oder `exclude`) wird aufgrund der Verarbeitung von unten nach oben zuerst überprüft. Das Muster `/Volumes/La Pomme/Foo/Junk/*.cpp` stimmt nicht mit dem Namen der Datei überein, die gerade verarbeitet wird.
2. Die Verarbeitung und Überprüfung werden bei Regel 2 fortgesetzt. Dieses Mal stimmt das Muster `/Volumes/La Pomme/Foo/.../*.cpp` mit dem Namen der Datei überein, die gerade verarbeitet wird. Die Verarbeitung stoppt, die Option wird überprüft und das Objekt wird eingeschlossen.
3. Datei `/Volumes/La Pomme/Foo/Dev/test.cpp` wird gesichert.

Beispiel 2

Nehmen wir an, La Pomme ist nicht der Startdatenträger.

```
EXCLUDE ../*.cpp
INCLUDE "/Volumes/La Pomme/Foo/.../*.cpp"
EXCLUDE "/Volumes/La Pomme/Foo/Junk/*.cpp"
```

Folgende Datei wird gerade verarbeitet: `/Volumes/La Pomme/Widget/Sample File`. Folgende Verarbeitungsschritte werden durchgeführt:

1. Regel 3 wird überprüft, ohne eine Übereinstimmung zu finden.
2. Regel 2 wird überprüft, ohne eine Übereinstimmung zu finden.
3. Regel 1 wird überprüft, ohne eine Übereinstimmung zu finden.
4. Da keine Übereinstimmung gefunden wurde, wird `Volumes/La Pomme/Widget/Sample File` implizit eingeschlossen und gesichert.

Beispiel 3

Sie haben die folgenden Anweisungen für die Optionen `include` und `exclude` definiert:

```
exclude *.o
  include /home/foo/.../*.o
exclude /home/foo/junk/*.o
```

Folgende Datei wird gerade verarbeitet: /home/foo/dev/test.o. Folgende Verarbeitungsschritte werden durchgeführt:

1. Regel 3 (die letzte definierte Anweisung) wird wegen der Verarbeitung von unten nach oben zuerst überprüft. Das Muster /home/foo/junk/*.o stimmt nicht mit dem Namen der Datei überein, die gerade verarbeitet wird.
2. Die Verarbeitung und Überprüfung werden bei Regel 2 fortgesetzt. Dieses Mal stimmt das Muster /home/foo/.../*.o mit dem Namen der Datei überein, die gerade verarbeitet wird. Die Verarbeitung stoppt, die Option wird überprüft und lautet include.
3. Die Datei /home/foo/dev/test.o wird gesichert.

Beispiel 4

Sie haben die folgenden Anweisungen für die Optionen include und exclude definiert:

```
exclude *.obj
  include /home/foo/.../*.o
exclude /home/foo/junk/*.o
```

Folgende Datei wird gerade verarbeitet: /home/widg/copyit.txt. Folgende Verarbeitungsschritte werden durchgeführt:

1. Regel 3 wird überprüft, ohne eine Übereinstimmung zu finden.
2. Regel 2 wird überprüft, ohne eine Übereinstimmung zu finden.
3. Regel 1 wird überprüft, ohne eine Übereinstimmung zu finden.
4. Da keine Übereinstimmung gefunden wurde, wird die Datei /home/widg/copyit.txt implizit eingeschlossen und gesichert.

Beispiel 5

Sie haben die folgenden Anweisungen für die Optionen include und exclude definiert:

```
exclude /.../*.o
  include /home/foo/.../*.o
exclude /home/foo/junk/*.o
```

Zurzeit wird die folgende Datei verarbeitet: /home/lib/objs/printf.o. Folgende Verarbeitungsschritte werden durchgeführt:

1. Regel 3 wird überprüft, ohne eine Übereinstimmung zu finden.
2. Regel 2 wird überprüft, ohne eine Übereinstimmung zu finden.
3. Regel 1 wird überprüft, und es wird eine Übereinstimmung gefunden.
4. Die Verarbeitung stoppt, die Option wird überprüft und das Objekt wird ausgeschlossen.
5. Die Datei /home/lib/objs/printf.o wird nicht gesichert.

Beispiel 6

Sie haben die folgenden Anweisungen für die Optionen include und exclude definiert:

```
exclude.attribute.symlink /*
exclude /*
  include /home/foo/.../*.o
exclude /home/foo/junk/*.o
```

Zurzeit wird die folgende Datei verarbeitet: /home/lib/objs/printf.o. Folgende Verarbeitungsschritte werden durchgeführt:

1. Die Anweisung `exclude.attribute.sym link` wird zuerst überprüft. Ist die Datei `printf.o` eine symbolische Verbindung, wird sie ausgeschlossen, andernfalls wird mit dem nächsten Schritt fortgefahren. Bitte beachten Sie, dass die Anweisungen `exclude.attribute.sym link` immer vor den anderen Include/Exclude-Anweisungen verarbeitet werden, unabhängig von Ihrer Position in der Einschluss-/Ausschlussliste.
2. Regel 3 wird überprüft, ohne eine Übereinstimmung zu finden.
3. Regel 2 wird überprüft, ohne eine Übereinstimmung zu finden.
4. Regel 1 wird überprüft, und es wird eine Übereinstimmung gefunden.
5. Die Verarbeitung stoppt, die Option wird überprüft und das Objekt wird ausgeschlossen.
6. Datei `/home/lib/objs/printf.o` wird nicht gesichert.

Zugehörige Konzepte:

„Dateibereiche und Verzeichnisse ausschließen“ auf Seite 131

Kapitel 10, „Verarbeitungsoptionen“, auf Seite 323

Zugehörige Verweise:

„Exclude-Optionen“ auf Seite 438

„Query Inclexcl“ auf Seite 760

Kapitel 3. Erste Schritte

Bevor Sie den IBM Spectrum Protect-Client für Sichern/Archivieren verwenden können, müssen Sie wissen, wie eine GUI- oder Befehlszeilensitzung gestartet und der Client-Scheduler automatisch gestartet wird. Sie lernen auch andere häufig verwendete Tasks kennen.

Führen Sie die folgenden Tasks aus, bevor Sie den Client für Sichern/Archivieren verwenden:

- „Java-GUI-Sitzung starten“ auf Seite 153
- „Befehlszeilensitzung starten“ auf Seite 155
- „Web-Client-Sitzung starten“ auf Seite 158
- „Client-Scheduler automatisch starten“ auf Seite 160
- „Kennwort ändern“ auf Seite 160

Sie können auch die folgenden Tasks ausführen:

- „Dateilisten mithilfe der GUI des Clients für Sichern/Archivieren sortieren“ auf Seite 162
- „Onlinehilfe anzeigen“ auf Seite 163
- „Sitzung beenden“ auf Seite 164

Sicherheitseinstellungen des Clients konfigurieren, um die Verbindung zum IBM Spectrum Protect-Server der Version 8.1.2 und höher herzustellen

Wenn Sie die Verbindung zum IBM Spectrum Protect-Server der Version 8.1.2 und höher herstellen, gibt es mehrere Konfigurationsoptionen, die zu den Sicherheitseinstellungen des IBM Spectrum Protect-Clients gehören. Wenn Sie die Standardwerte für diese Optionen akzeptieren, erfolgt die Konfiguration des Clients aus Gründen einer verbesserten Sicherheit transparent; dies wird für die meisten Anwendungsfälle empfohlen.

Konfiguration mithilfe der Standardsicherheitseinstellungen (Schnellzugriffspfad)

Schnellzugriffspfaddetails sind die Konfigurationsoptionen, die Auswirkungen auf die Sicherheit der Clientverbindung zum Server und das Verhalten für verschiedene Anwendungsfälle haben, wenn Standardwerte akzeptiert werden. Das Szenario mit dem Schnellzugriffspfad minimiert die Schritte im Konfigurationsprozess an Endpunkten.

In diesem Szenario werden Zertifikate automatisch vom Server abgerufen, wenn der Client zum ersten Mal die Verbindung herstellt, vorausgesetzt der IBM Spectrum Protect-Serverparameter **SESSIONSECURITY** ist auf **TRANSITIONAL** gesetzt. Dies ist der Standardwert bei der ersten Verbindung. Sie können diesem Szenario unabhängig davon folgen, ob Sie zuerst das Upgrade für den IBM Spectrum Protect-Server auf Version 8.1.2 und höhere V8-Stufen ausführen und anschließend das Upgrade für den Client auf diese Stufen ausführen oder umgekehrt.

Anmerkung: Wenn ein Client unter Verwendung von Version 8.1.6 oder höheren V8-Stufen die Verbindung zum IBM Spectrum Protect-Server herstellt und entweder Shared Memory oder Named Pipes für die Kommunikation verwendet, ändert sich der Wert des Parameters **SESSIONSECURITY** für den Client in **STRICT**. Wenn in diesem Fall statt Shared Memory oder Named Pipes TCP/IP für die Kommunikation verwendet werden soll und der Client noch nicht über das Zertifikat des Servers verfügt, setzen Sie zunächst den Parameter **SESSIONSECURITY** auf **TRANSITIONAL** zurück. Anschließend müssen Sie die Verbindung zum Server herstellen, um die Zertifikate automatisch abzurufen.

Achtung: Dieses Szenario kann nicht verwendet werden, wenn der IBM Spectrum Protect-Server für die LDAP-Authentifizierung konfiguriert ist. Wenn LDAP verwendet wird, können Sie die erforderlichen Zertifikate manuell mithilfe des Dienstprogramms dsmcert importieren. Weitere Informationen finden Sie in „Konfiguration ohne automatische Verteilung von Zertifikaten“ auf Seite 148.

Clientoptionen mit Auswirkungen auf die Sitzungssicherheit

Die folgenden Clientoptionen geben Sicherheitseinstellungen für den Client an. Weitere Informationen zu diesen Optionen finden Sie in „Clientoptionsreferenz“ auf Seite 355.

- **SSLREQUIRED.** Mit dem Standardwert `Default` werden bestehende Verbindungen mit Sitzungssicherheit zu Servern einer Version vor Version 8.1.2 aktiviert und der Client automatisch zum Herstellen einer sicheren Verbindung zu einem Server der Version 8.1.2 oder höher unter Verwendung von TLS für die Authentifizierung konfiguriert.
- **SSLACCEPTCERTFROMSERV.** Der Standardwert `Yes` ermöglicht es dem Client, automatisch ein selbst signiertes öffentliches Zertifikat vom Server zu akzeptieren und den Client automatisch für die Verwendung dieses Zertifikats zu konfigurieren, wenn der Client die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt.
- **SSL.** Der Standardwert `No` gibt an, dass keine Verschlüsselung verwendet wird, wenn Daten zwischen dem Client und einem Server einer Version vor Version 8.1.2 übertragen werden. Wenn der Client die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt, gibt der Standardwert `No` an, dass Objektdaten nicht verschlüsselt werden. Alle anderen Informationen werden verschlüsselt, wenn der Client mit dem Server kommuniziert. Der Wert `Yes` gibt an, dass SSL zum Verschlüsseln aller Informationen, einschließlich Objektdaten, verwendet wird, wenn der Client mit dem Server kommuniziert.
- **SSLFIPSMODE.** Der Standardwert `No` gibt an, dass keine mit FIPS zertifizierte SSL-Bibliothek erforderlich ist.

Darüber hinaus gelten die folgenden Optionen nur, wenn der Client SSL-Verbindungen zu einem Server einer Version vor Version 8.1.2 verwendet. Sie werden ignoriert, wenn der Client die Verbindung zu einem Server einer höheren Version herstellt.

- **SSLDISABLELEGACYTLS.** Der Wert `No` gibt an, dass der Client für SSL-Sitzungen nicht TLS 1.2 erfordert. Der Client lässt Verbindungen mit TLS 1.1 und niedrigeren SSL-Protokollen zu. Wenn der Client mit einem IBM Spectrum Protect-Server der Version 8.1.1 oder früher kommuniziert, ist `No` der Standardwert.
- **LANFREESL.** Der Standardwert `No` gibt an, dass der Client bei der Kommunikation mit dem Speicheragenten nicht SSL verwendet, wenn die LAN-unabhängige Datenübertragung konfiguriert ist.
- **REPLSSLPORT.** Gibt an, ob die TCP/IP-Anschlussadresse für SSL aktiviert ist, wenn der Client mit dem Zielreplikationsserver kommuniziert.

Anwendungsfälle für Standardsicherheitseinstellungen

- Zuerst wird das Upgrade für den Server auf Version 8.1.2 oder höher durchgeführt. Anschließend wird das Upgrade für den Client durchgeführt. Der vorhandene Client verwendet *keine* SSL-Kommunikation:
 - Es sind keine Änderungen an den Sicherheitsoptionen für den Client erforderlich.
 - Für die Konfiguration erfolgt ein automatisches Update für die Verwendung von TLS, wenn sich der Client beim Server authentifiziert.
- Zuerst wird das Upgrade für den Server auf Version 8.1.2 oder höher durchgeführt. Anschließend wird das Upgrade für den Client durchgeführt. Der vorhandene Client *verwendet* die SSL-Kommunikation:
 - Es sind keine Änderungen an den Sicherheitsoptionen für den Client erforderlich.
 - Es wird weiterhin die SSL-Kommunikation mit dem vorhandenen öffentlichen Serverzertifikat verwendet.
 - Die SSL-Kommunikation wird automatisch für die Verwendung der TLS-Version erweitert, die für den Server erforderlich ist.
- Zuerst wird das Upgrade für den Client auf Version 8.1.2 oder höher durchgeführt. Anschließend wird das Upgrade für den Server durchgeführt. Der vorhandene Client verwendet *keine* SSL-Kommunikation:
 - Es sind keine Änderungen an den Sicherheitsoptionen für den Client erforderlich.
 - Das vorhandene Authentifizierungsprotokoll wird weiterhin für Server einer Version vor Version 8.1.2 verwendet.
 - Für die Konfiguration erfolgt ein automatisches Update für die Verwendung von TLS, wenn sich der Client beim Server authentifiziert, nachdem für den Server ein Update auf Version 8.1.2 oder höher durchgeführt wurde.
- Zuerst wird das Upgrade für den Client auf Version 8.1.2 oder höher durchgeführt. Anschließend wird das Upgrade für den Server durchgeführt. Der vorhandene Client *verwendet* die SSL-Kommunikation:
 - Es sind keine Änderungen an den Sicherheitsoptionen für den Client erforderlich.
 - Es wird weiterhin die SSL-Kommunikation mit dem vorhandenen öffentlichen Serverzertifikat mit Servern einer Version vor Version 8.1.2 verwendet.
 - Die SSL-Kommunikation wird automatisch für die Verwendung der TLS-Version erweitert, die für den Server erforderlich ist, nachdem für den Server ein Update auf Version 8.1.2 oder höher durchgeführt wurde.
- Zuerst wird das Upgrade für den Client auf Version 8.1.2 oder höher durchgeführt. Anschließend stellt der Client die Verbindung zu mehreren Servern her. Das Upgrade für die Server erfolgt zu unterschiedlichen Zeiten:
 - Es sind keine Änderungen an den Sicherheitsoptionen für den Client erforderlich.
 - Der Client verwendet die vorhandene Authentifizierung und das vorhandene Sitzungssicherheitsprotokoll zum Herstellen der Verbindung zu Servern einer Version vor Version 8.1.2; für den Client erfolgt ein automatisches Upgrade für die Verwendung der TLS-Authentifizierung, wenn der Client zum ersten Mal die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt. Die Sitzungssicherheit wird für jeden Server separat verwaltet.
- Neue Clientinstallation mit einem Server der Version 8.1.2 oder höher:
 - Konfigurieren Sie den Client gemäß einer neuen Installation.

- Mit den Standardwerten für die Sicherheitsoptionen wird der Client automatisch für die mit TLS verschlüsselte Sitzungsauthentifizierung konfiguriert.
- Setzen Sie den Parameter SSL auf Yes, wenn die Verschlüsselung aller Datenübertragungen zwischen dem Client und dem Server erforderlich ist.
- Neue Clientinstallation mit einem Server einer Version vor Version 8.1.2:
 - Konfigurieren Sie den Client gemäß einer neuen Clientinstallation.
 - Akzeptieren Sie die Standardwerte für die Parameter für die Clientsitzungssicherheit, wenn die SSL-Verschlüsselung aller Datenübertragungen nicht erforderlich ist.
 - Das Nicht-SSL-Authentifizierungsprotokoll wird so lange verwendet, bis für den Server ein Upgrade auf Version 8.1.2 oder höher durchgeführt wird.
 - Setzen Sie den Parameter SSL auf Yes, wenn die Verschlüsselung aller Datenübertragungen zwischen dem Client und dem Server erforderlich ist, und fahren Sie mit der manuellen Konfiguration für SSL fort.
 - Konfigurationsanweisungen finden Sie in „IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren“ auf Seite 77.
 - Die SSL-Kommunikation wird automatisch für die Verwendung der TLS-Version erweitert, die für den Server erforderlich ist, nachdem für den Server ein Update auf Version 8.1.2 oder höher durchgeführt wurde.

Zugehörige Verweise:

„Sslrequired“ auf Seite 602
 „Sslacceptcertfromserv“ auf Seite 599
 „Ssl“ auf Seite 598
 „Sslfipsmode“ auf Seite 601
 „Ssldisablelegacytls“ auf Seite 600
 „Lanfreessl“ auf Seite 498
 „Replsslport“ auf Seite 552

Konfiguration ohne automatische Verteilung von Zertifikaten

Dieses Szenario erläutert die einzelnen Konfigurationsoptionen, die Auswirkungen auf die Sicherheit des Clients haben, wenn die automatische Verteilung von Zertifikaten vom Server nicht zulässig ist. Die automatische Verteilung von Zertifikaten vom Server ist beispielsweise nicht zulässig, wenn der Server für die Verwendung der LDAP-Authentifizierung konfiguriert ist oder wenn Zertifikate von einer Zertifizierungsstelle signiert werden müssen.

Optionen mit Auswirkungen auf die Sitzungssicherheit

Die Optionen für Sicherheitseinstellungen entsprechen den in „Konfiguration mithilfe der Standardsicherheitseinstellungen (Schnellzugriffspfad)“ auf Seite 145 beschriebenen Optionen, mit der Ausnahme, dass Sie die Option SSLACCEPTCERTFROMSERV auf No setzen müssen, um sicherzustellen, dass der Client nicht automatisch ein selbst signiertes öffentliches Zertifikat vom Server akzeptiert, wenn der Client zum ersten Mal die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt.

Anwendungsfälle für die Konfiguration des Clients ohne automatische Verteilung von Zertifikaten

Ist die automatische Verteilung von Zertifikaten nicht möglich oder nicht gewünscht, verwenden Sie das Dienstprogramm 'dsmcert', um das Zertifikat zu importieren. Fordern Sie das erforderliche Zertifikat vom IBM Spectrum Protect-Server oder von einer Zertifizierungsstelle an. Die Zertifizierungsstelle kann ein Unternehmen wie VeriSign oder Thawte oder eine interne Zertifizierungsstelle innerhalb Ihres Unternehmens sein.

- Zuerst wird das Upgrade für den Server auf Version 8.1.2 durchgeführt. Anschließend wird das Upgrade für den Client durchgeführt. Der vorhandene Client verwendet *keine* SSL-Kommunikation:
 - Setzen Sie die Option SSLACCEPTCERTFROMSERV auf den Wert No.
 - Fordern Sie das erforderliche Zertifikat vom IBM Spectrum Protect-Server oder von einer Zertifizierungsstelle an und verwenden Sie das Dienstprogramm 'dsmcert', um das Zertifikat zu importieren. Konfigurationsanweisungen finden Sie in „IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren“ auf Seite 77.
- Zuerst wird das Upgrade für den Server auf Version 8.1.2 oder höher durchgeführt. Anschließend wird das Upgrade für den Client durchgeführt. Der vorhandene Client *verwendet* die SSL-Kommunikation:
 - Es sind keine Änderungen an den Sicherheitsoptionen für den Client erforderlich. Wenn der Client bereits über ein Serverzertifikat für die SSL-Kommunikation verfügt, ist die Option SSLACCEPTCERTFROMSERV nicht zutreffend.
 - Es wird weiterhin die SSL-Kommunikation mit dem vorhandenen öffentlichen Serverzertifikat verwendet.
 - Die SSL-Kommunikation wird automatisch für die Verwendung der TLS-Version erweitert, die für den Server erforderlich ist.
- Zuerst wird das Upgrade für den Client auf Version 8.1.2 oder höher durchgeführt. Anschließend wird das Upgrade für den Server durchgeführt. Der vorhandene Client verwendet *keine* SSL-Kommunikation:
 - Setzen Sie die Option SSLACCEPTCERTFROMSERV auf den Wert No.
 - Das vorhandene Authentifizierungsprotokoll wird weiterhin für Server einer Version vor Version 8.1.2 verwendet.
 - Bevor der Client die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt, müssen Sie folgende Schritte ausführen:
 - Fordern Sie das erforderliche Zertifikat vom IBM Spectrum Protect-Server oder von einer Zertifizierungsstelle an und verwenden Sie das Dienstprogramm 'dsmcert', um das Zertifikat zu importieren. Konfigurationsanweisungen finden Sie in „IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren“ auf Seite 77.
- Zuerst wird das Upgrade für den Client auf Version 8.1.2 oder höher durchgeführt. Anschließend wird das Upgrade für den Server durchgeführt. Der vorhandene Client *verwendet* die SSL-Kommunikation:
 - Es sind keine Änderungen an den Sicherheitsoptionen für den Client erforderlich. Wenn der Client bereits über ein Serverzertifikat für die SSL-Kommunikation verfügt, ist die Option SSLACCEPTCERTFROMSERV nicht zutreffend.
 - Es wird weiterhin die SSL-Kommunikation mit dem vorhandenen öffentlichen Serverzertifikat mit Servern einer Version vor Version 8.1.2 verwendet.
 - Die SSL-Kommunikation wird automatisch für die Verwendung der TLS-Version erweitert, die für den Server erforderlich ist, nachdem für den Server ein Update auf Version 8.1.2 oder höher durchgeführt wurde.

- Zuerst wird das Upgrade für den Client auf Version 8.1.2 oder höher durchgeführt. Anschließend stellt der Client die Verbindung zu mehreren Servern her. Das Upgrade für die Server erfolgt zu unterschiedlichen Zeiten:
 - Setzen Sie die Option SSLACCEPTCERTFROMSERV auf den Wert No.
 - Das vorhandene Authentifizierungsprotokoll wird weiterhin für Server einer Version vor Version 8.1.2 verwendet.
 - Bevor der Client die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt oder wenn die SSL-Kommunikation für eine Version des Servers erforderlich ist, müssen Sie folgende Schritte ausführen:
 - Fordern Sie das erforderliche Zertifikat vom IBM Spectrum Protect-Server oder von einer Zertifizierungsstelle an und verwenden Sie das Dienstprogramm 'dsmcert', um das Zertifikat zu importieren. Konfigurationsanweisungen finden Sie in „IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren“ auf Seite 77.
 - Der Client verwendet die vorhandene Authentifizierung und das vorhandene Sitzungssicherheitsprotokoll zum Herstellen der Verbindung zu Servern einer Version vor Version 8.1.2; für den Client erfolgt ein automatisches Upgrade für die Verwendung der TLS-Authentifizierung, wenn der Client zum ersten Mal die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt. Die Sitzungssicherheit wird für jeden Server separat verwaltet.
- Neue Clientinstallation mit einem Server der Version 8.1.2 oder höher:
 - Konfigurieren Sie den Client gemäß einer neuen Installation.
 - Setzen Sie die Option SSLACCEPTCERTFROMSERV auf den Wert No.
 - Fordern Sie das erforderliche Zertifikat vom IBM Spectrum Protect-Server oder von einer Zertifizierungsstelle an und verwenden Sie das Dienstprogramm 'dsmcert', um das Zertifikat zu importieren. Konfigurationsanweisungen finden Sie in „IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren“ auf Seite 77.
 - Setzen Sie den Parameter SSL auf Yes, wenn die Verschlüsselung aller Datenübertragungen zwischen dem Client und dem Server erforderlich ist.
- Neue Clientinstallation, Server hat eine Version vor Version 8.1.2, mit SSL verschlüsselte Sitzungen *sind* erforderlich:
 - Konfigurieren Sie den Client gemäß einer neuen Installation.
 - Setzen Sie den Parameter SSL auf den Wert Yes.
 - Fordern Sie das erforderliche Zertifikat vom IBM Spectrum Protect-Server oder von einer Zertifizierungsstelle an und verwenden Sie das Dienstprogramm 'dsmcert', um das Zertifikat zu importieren. Konfigurationsanweisungen finden Sie in „IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren“ auf Seite 77.
- Neue Clientinstallation, Server hat eine Version vor Version 8.1.2, mit SSL verschlüsselte Sitzungen *sind nicht* erforderlich:
 - Konfigurieren Sie den Client gemäß einer neuen Installation.
 - Setzen Sie die Option SSLACCEPTCERTFROMSERV auf den Wert No.
 - Das Nicht-SSL-Authentifizierungsprotokoll wird so lange verwendet, bis für den Server ein Upgrade auf Version 8.1.2 oder höher durchgeführt wird.
 - Bevor der Client die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt, müssen Sie folgende Schritte ausführen:
 - Fordern Sie das erforderliche Zertifikat vom IBM Spectrum Protect-Server oder von einer Zertifizierungsstelle an und verwenden Sie das Dienstprogramm 'dsmcert', um das Zertifikat zu importieren. Konfigurationsan-

weisungen finden Sie in „IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren“ auf Seite 77.

Zugehörige Verweise:

„Sslrequired“ auf Seite 602
„Sslacceptcertfromserv“ auf Seite 599
„Ssl“ auf Seite 598
„Sslfipsmode“ auf Seite 601
„Ssldisablelegacytls“ auf Seite 600
„Lanfreessl“ auf Seite 498
„Replsslport“ auf Seite 552

Sicherer Kennwortspeicher

In IBM Spectrum Protect Version 8.1.2 und Version 7.1.8 befindet sich das IBM Spectrum Protect-Kennwort an einer anderen Position.

In den Clients der Version 8.1.0, 7.1.6 und früher wurde das IBM Spectrum Protect-Kennwort bei Windows-Clients in der Windows-Registrierungsdatenbank und bei UNIX- und Linux-Clients in der Datei TSM.PWD gespeichert.

Ab Version 8.1.2 und Version 7.1.8 werden alle IBM Spectrum Protect-Kennwörter in den Schlüsselspeichern von IBM Global Security Kit (GSKit) gespeichert. Der Importprozess für Serverzertifikate ist vereinfacht. Informationen zum Importieren von Serverzertifikaten finden Sie in „IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren“ auf Seite 77.

Wenn Sie ein Upgrade auf den IBM Spectrum Protect-Client der Version 8.1.2 oder höher von einem früheren Client durchführen, der die alten Kennwortpositionen verwendet, werden die vorhandenen Kennwörter in die folgenden Dateien im neuen Kennwortspeicher migriert:

TSM.KDB

In dieser Datei werden die verschlüsselten Kennwörter gespeichert.

TSM.sth

In dieser Datei wird der Verschlüsselungszufallsschlüssel gespeichert, mit dem Kennwörter in der Datei TSM.KDB verschlüsselt werden. Diese Datei wird durch das Dateisystem geschützt. Diese Datei wird für automatisierte Operationen benötigt.

TSM.IDX

Eine indexierte Datei zur Protokollierung der Kennwörter in der Datei TSM.KDB.

Bei Data Protection for VMware-Clients wird das Verwaltungskennwort des Data Protection for VMware-GUI-Servers in einen Schlüsselspeicher migriert.

Kennwortpositionen auf UNIX- und Linux-Clients

Auf UNIX- und Linux-Clients werden die in den Dateien TSM.PWD vorhandenen Kennwörter in den neuen Kennwortspeicher an derselben Position migriert. Bei Rootbenutzern lautet die Standardposition für den Kennwortspeicher /etc/adsm. Bei Benutzern ohne Rootberechtigung wird die Position des Kennwortspeichers mit der Option passworddir angegeben.

Die Datei TSM.PWD wird nach der Migration gelöscht.

Anmerkung: In den folgenden Situationen befindet sich der neue Kennwortspeicher nicht an der Standardposition (/etc/adsm):

- Die Datei TSM.PWD ist im Verzeichnis /etc/adsm nicht vorhanden.
- Die Optionsdatei gibt eine Option passworddir an, die auf eine andere Position zeigt.

Trusted Communication Agent nicht mehr verfügbar

Der bisher von Benutzern ohne Rootberechtigung in Version 8.1.0 und 7.1.6 und früheren Clients verwendete Trusted Communication Agent (TCA) ist nicht mehr verfügbar. Rootbenutzer können Benutzern ohne Rootberechtigung die Verwaltung ihrer Dateien mit den folgenden Methoden ermöglichen:

Help-Desk

Bei der Help-Desk-Methode führt der Rootbenutzer alle Sicherungs- und Zurückschreibungsoperationen aus. Der Benutzer ohne Rootberechtigung muss sich an den Rootbenutzer wenden, um die Sicherung oder Zurückschreibung bestimmter Dateien anzufordern.

Berechtigter Benutzer

Bei der Methode mit einem berechtigten Benutzer erhält ein Benutzer ohne Rootberechtigung Schreib-/Lesezugriff auf den Kennwortspeicher. Hierbei wird die Option passworddir verwendet, um auf eine Kennwortposition zu zeigen, auf die der Benutzer ohne Rootberechtigung Schreib-/Lesezugriff hat. Mit dieser Methode können Benutzer ohne Rootberechtigung ihre eigenen Dateien sichern und zurückschreiben, die Verschlüsselung verwenden und ihre eigenen Kennwörter mit der Option passwordaccess generate verwalten.

Weitere Informationen finden Sie in „Benutzern ohne Rootberechtigung die Verwaltung eigener Daten ermöglichen“ auf Seite 55.

Ist keine dieser Methoden zufriedenstellend, müssen Sie die früheren Clients verwenden, die über den Trusted Communication Agent (TCA) verfügen.

IBM Spectrum Protect-Clientauthentifizierung

Wenn Sie die grafische Benutzerschnittstelle oder Befehlszeilenschnittstelle des IBM Spectrum Protect-Clients verwenden, können Sie sich mit einem Knotennamen und einem Kennwort *oder* mit einer Benutzer-ID mit Administratorberechtigung und dem zugehörigen Kennwort anmelden.

Der Client fordert Sie zur Eingabe Ihrer Benutzer-ID auf und vergleicht sie mit dem konfigurierten Knotennamen. Wenn sie übereinstimmen, versucht der Client, die Benutzer-ID als Knotenname zu authentifizieren. Wenn die Authentifizierung fehlschlägt oder wenn die Benutzer-ID nicht mit dem konfigurierten Knotennamen übereinstimmt, versucht der Client, die Benutzer-ID als Benutzer-ID mit Administratorberechtigung zu authentifizieren.

Damit eine Benutzer-ID für Verwaltungsaufgaben für die Clients für Sichern/Archivieren verwendet werden kann, muss die Benutzer-ID über eine der folgenden Berechtigungen verfügen:

Systemberechtigung

Berechtigung über das gesamte System. Ein Administrator mit Systemberechtigung kann jede Verwaltungstask ausführen.

Maßnahmenberechtigung

Berechtigung über die Maßnahmen domäne des Knotens. Ermöglicht einem Administrator, Maßnahmenobjekte zu verwalten, Clientknoten zu registrieren und Clientoperationen für Clientknoten zu planen.

Clienteigner

Berechtigung über den registrierten IBM Spectrum Protect-Clientknoten. Sie können über den Web-Client oder den Client für Sichern/Archivieren auf den Client zugreifen. Sie sind Eigner der Daten und haben das Recht, über Remotezugriff physisch auf die Daten zuzugreifen. Sie können Dateien auf demselben System oder einem anderen System sichern und zurückschreiben und Sie können Dateibereiche oder Archivierungsdaten löschen.

Clientzugriff

Um den Web-Client für die Sicherung und Zurückschreibung von Dateien auf einem fernen Clientsystem verwenden zu können, müssen Sie über eine Benutzer-ID mit Administratorberechtigung verfügen, die gleichzeitig Clientzugriffsberechtigung für den Knotennamen des fernen Clientsystems hat. Wenn IBM Spectrum Protect-Administratoren mit Clientzugriffsberechtigung für Ihren Knotennamen keine Dateien auf Ihrem System sichern und zurückschreiben können sollen, geben Sie die Option `revokeremoteaccess` in Ihrer Clientoptionsdatei an.

Die Clientzugriffsberechtigung ermöglicht IBM Spectrum Protect-Administratoren nur, Dateien auf fernen Systemen zu sichern und zurückzuschreiben. Sie haben keinen physischen Zugriff auf die Daten. Das heißt, sie können die Daten, die zu dem fernen System gehören, nicht auf ihr eigenes System zurückschreiben. Um Daten, die zu einem fernen System gehören, auf Ihr eigenes System zurückschreiben zu können, müssen Sie mindestens über Clienteignerberechtigung verfügen.

Verwenden Sie eine der folgenden Methoden, um festzustellen, welche Berechtigung Sie haben:

- Wählen Sie im Hauptfenster der IBM Spectrum Protect-GUI **Datei > Verbindungsinformationen** aus.
- Verwenden Sie den IBM Spectrum Protect-Serverbefehl `QUERY ADMIN` vom Verwaltungsbefehlszeilenclient aus.

Zugehörige Verweise:

„Revokeremoteaccess“ auf Seite 561

 Befehl `QUERY ADMIN`

Java-GUI-Sitzung starten

Welche Schritte zum Starten der grafischen Benutzerschnittstelle (GUI) des Clients für Sichern/Archivieren ausgeführt werden, ist vom Betriebssystem abhängig.

Vorgehensweise

Führen Sie die entsprechende Prozedur für Ihr Betriebssystem zum Starten der Java-GUI aus.

Betriebssystem	Prozedur
Mac OS X	<ul style="list-style-type: none"> • Doppelklicken Sie auf die Anwendung 'IBM Spectrum Protect', um den Client für Sichern/Archivieren ohne Systemadministratorberechtigungen zu starten. Wenn Sie den Client ohne Systemadministratorberechtigungen ausführen, können Sie Dateien verwalten, deren Eigner der aktuelle Benutzer ist. • Doppelklicken Sie auf IBM Spectrum Protect-Tools für Administratoren und wählen Sie IBM Spectrum Protect aus. Nach der Eingabe eines Benutzernamens und eines Kennworts für den Systemadministrator wird der Client mit Systemadministratorberechtigungen gestartet. Wenn Sie den Client mit Systemadministratorberechtigungen ausführen, können Sie Dateien verwalten, deren Eigner alle Benutzer des Systems sind. • Sie können den Client für Sichern/Archivieren auch mit dem Befehl dsmj starten. Sie können den Client entweder als Vordergrund- oder als Hintergrundprozess ausführen. Das Script dsmj wird in /Library/Application Support/tivoli/tsm/client/ba/bin installiert.
AIX, Linux, Solaris	<p>Auf anderen UNIX-Systemen als Mac OS X muss die GUI des Clients für Sichern/Archivieren vom X Window System ausgeführt werden. Wenn das Symbol für IBM Spectrum Protect auf dem Desktop angezeigt wird, ist der Client bereits aktiv. Doppelklicken Sie auf das Symbol, um das Fenster 'IBM Spectrum Protect' zu öffnen. Wenn das Symbol für IBM Spectrum Protect auf Ihrem Desktop nicht angezeigt, starten Sie die grafische Benutzerschnittstelle des Clients für Sichern/Archivieren mit dem Befehl dsmj. Sie können den Client entweder als Vordergrund- oder als Hintergrundprozess ausführen.</p>

Der Client für Sichern/Archivieren lokalisiert und verwendet die Optionen, die in der Clientsystemoptionsdatei (dsm.sys) und in der Clientoptionsdatei (dsm.opt) angegeben sind.

Zugehörige Konzepte:

Kapitel 2, „IBM Spectrum Protect-Client konfigurieren“, auf Seite 53

IBM Spectrum Protect-Kennwort

Der IBM Spectrum Protect-Administrator kann für die Verbindung zum Server die Eingabe eines Kennworts durch den Benutzer erforderlich machen.

Der IBM Spectrum Protect-Client fordert Sie zur Eingabe des Kennworts auf, falls ein Kennwort erforderlich ist. Wenden Sie sich an den IBM Spectrum Protect-Administrator, wenn Ihnen das Kennwort nicht bekannt ist.

Zugehörige Tasks:

„Kennwort ändern“ auf Seite 160

Setup-Assistent

Wenn die grafische Benutzerschnittstelle des Clients (Client-GUI) startet, wird geprüft, ob eine Clientoptionsdatei vorhanden ist.

Ist die Clientoptionsdatei nicht vorhanden (dies ist normalerweise der Fall, wenn Sie den Client zum ersten Mal auf Ihrem System installiert haben), startet der Setup-Assistent automatisch und führt Sie durch den Konfigurationsprozess.

Die Clientoptionsdatei ist die Datei `dsm.sys`.

Befehlszeilensitzung starten

Sie können eine Befehlszeilensitzung starten, indem Sie den Befehl **dsmc** aufrufen.

Anmerkung: Wenn das Verzeichnis `/usr/bin` eine symbolische Verbindung zu der ausführbaren IBM Spectrum Protect-Datei enthält und alle DSM-Umgebungsvariablen definiert sind, können Sie den Befehl **dsmc** in jedem Verzeichnis eingeben. Andernfalls geben Sie den vollständig qualifizierten Pfad des Befehls ein.

Anmerkung: Unter Mac OS X können Systemadministratoren mit dem Befehl **sudo** weitere Berechtigungen erhalten, sodass der Client für Sichern/Archivieren auf Dateien für alle Benutzer im System zugreifen kann.

Geben Sie in der Befehlszeile **dsmc** gefolgt von dem Befehl ein (*Stapelmodus*). Wenn das Verzeichnis `/usr/bin` oder `opt/bin` eine symbolische Verbindung zum IBM Spectrum Protect-Installationsverzeichnis enthält, können Sie den Befehl **dsmc** in jedem Verzeichnis eingeben. Andernfalls können Sie den vollständig qualifizierten Namen eingeben.

Der Client kann nur mit dem Befehl "dsmc" gestartet werden, wenn die Umgebungsvariable PATH mit dem Pfad zu der Clientposition aktualisiert wurde.

Der IBM Spectrum Protect-Administrator kann für die Verbindung zum Server die Eingabe eines Kennworts durch den Benutzer erforderlich machen. Der Client fordert Sie zur Eingabe des Kennworts auf, falls ein Kennwort erforderlich ist. Wenden Sie sich an Ihren Administrator, wenn Ihnen das Kennwort nicht bekannt ist.

Zugehörige Konzepte:

„Optionen im interaktiven Modus“ auf Seite 689

„Tasks für Rootbenutzer und berechtigte Benutzer UNIX- und Linux-Clients“ auf Seite 53

Kapitel 11, „Befehle verwenden“, auf Seite 683

Stapelmodus verwenden

Verwenden Sie den *Stapelmodus*, um einen einzelnen Clientbefehl einzugeben. Bei Verwendung des Stapelmodus muss dem Befehl die Zeichenfolge **dsmc** vorausgehen.

Informationen zu diesem Vorgang

Soll beispielsweise der Befehl **incremental** ausgegeben werden, geben Sie bei der Eingabeaufforderung Folgendes ein:

```
dsmc incremental
```

Einige Befehle erfordern ein Argument oder mehrere Argumente. Beispiel: Der Befehl zum Archivieren einer Datei:

```
dsmc archive /home/proj1/file1.txt
```

Abhängig von der aktuellen Einstellung der Option `passwordaccess` fordert der Client Sie möglicherweise zur Eingabe Ihres Kennworts auf, bevor der Befehl in einer Sitzung im Stapelmodus verarbeitet wird.

Wenn Sie Ihr Kennwort eingeben, wird das Kennwort nicht am Bildschirm angezeigt.

Zugehörige Verweise:

„Passwordaccess“ auf Seite 525

Folge von Befehlen im interaktiven Modus ausgeben

Der *interaktive* Modus (Dialogmodus) wird verwendet, wenn eine Reihe von Befehlen ausgegeben werden soll.

Informationen zu diesem Vorgang

Die Verbindung zum Server wird im interaktiven Modus nur einmal hergestellt, sodass eine Folge von Befehlen im interaktiven Modus schneller verarbeitet werden kann als im Stapelmodus.

Damit eine Clientbefehlssitzung im interaktiven Modus gestartet wird, muss einer der beiden folgenden Befehle eingegeben werden:

- `dsmc`
- `dsmc loop`

Die folgende Eingabeaufforderung wird auf Ihrem Bildschirm angezeigt:

```
Protect>
```

Im interaktiven Modus darf den Befehlen nicht die Zeichenfolge **dsmc** vorangestellt werden. Beispielsweise wird zum Archivieren einer Datei dann nicht **dsmc archive**, sondern nur **archive** eingegeben.

Soll beispielsweise eine Datei archiviert werden, geben Sie den Befehl mit der Dateispezifikation ein:

```
archive /home/proj1/file1.txt
```

Abhängig von der aktuellen Einstellung der Option `passwordaccess` fordert der Client Sie möglicherweise zur Eingabe Ihres Kennworts auf, bevor die Eingabe des Befehls in einer interaktiven Sitzung zulässig ist.

Wenn Sie Ihr Kennwort eingeben, wird das Kennwort nicht am Bildschirm angezeigt.

Eingabezeichenfolgen angeben, die Leerzeichen oder Hochkommas oder Anführungszeichen enthalten

Sie müssen bestimmte Regeln einhalten, wenn Sie eine Eingabezeichenfolge angeben, die Leerzeichen oder Hochkommas oder Anführungszeichen enthält.

Halten Sie die folgenden Regeln ein, wenn Sie eine Eingabezeichenfolge angeben, die Leerzeichen oder Hochkommas oder Anführungszeichen enthält:

- Enthält die Eingabezeichenfolge mindestens ein Leerzeichen, schließen Sie die Zeichenfolge in Hochkommas oder Anführungszeichen ein. Sie können Hochkommas oder Anführungszeichen verwenden, sie müssen jedoch paarig angegeben werden.
- Enthält die Eingabezeichenfolge ein Hochkomma, schließen Sie die Zeichenfolge, wie im folgenden Beispiel gezeigt, in Anführungszeichen ein:
`-description="Annual backup of the accounting department's monthly reports"`
- Enthält die Eingabezeichenfolge ein Anführungszeichen, schließen Sie die Zeichenfolge, wie im folgenden Beispiel gezeigt, in Hochkommas ein:
`-description='Neue Übersetzungen von "Odyssee" und "Ilias"'`
- Enthält die Eingabezeichenfolge Leerzeichen und Hochkommas oder Anführungszeichen, schließen Sie die Zeichenfolge in Hochkommas bzw. Anführungszeichen ein. Dabei dürfen die Hochkommas oder Anführungszeichen am Anfang und am Ende der Zeichenfolge nicht identisch mit den Hochkommas oder Anführungszeichen innerhalb der Zeichenfolge sein.

Einschränkung: Eine Eingabezeichenfolge, die Hochkommas und Anführungszeichen enthält, ist keine gültige Eingabezeichenfolge.

Die folgenden Regeln gelten für diese Datentypen:

- Vollständig qualifizierte Namen.
- Die Beschreibung (`description`), die Sie im Befehl **archive** angeben.
- Einen beliebigen Wert für einen Optionswert, wobei die Zeichenfolge Leerzeichen oder Anführungszeichen enthalten kann.

Wichtig: In Eingabezeichenfolgen können Sie keine Escapezeichen verwenden. Escapezeichen werden ebenso wie alle anderen Zeichen behandelt. Im Folgenden finden Sie einige Beispiele, in denen Escapezeichen nicht erkannt werden:

- Wenn die Zeichenfolge sich in einer Optionsdatei befindet.
- Wenn die Zeichenfolge sich in einer Listendatei befindet.
- Wenn die Zeichenfolge im interaktiven Modus eingegeben wird.

Weitere Hinweise zum Starten

Optionen können als Argumente in den Befehlen **dsmj** und **dsmc** angegeben werden. Mithilfe von Optionen kann beispielsweise das für die Anzeige von Datum, Uhrzeit und Zahlen verwendete Format geändert werden oder das Kennwort eingeschlossen werden, sodass der Client für Sichern/Archivieren nicht zur Eingabe des Kennworts auffordert.

Informationen zu diesem Vorgang

Wenn Sie mehrere Server in `dsm.sys` definiert haben und auf einen anderen (als den in Ihrer Clientbenutzeroptionsdatei `dsm.opt` definierten) Server für Sicherungs-/Archivierungsservices zugreifen möchten, können Sie darüber hinaus mit der Option `servername` diesen Server angeben.

Beispiel:

```
dsmj -servername=server_b
```

Die Java-GUI (dsmj) akzeptiert Befehlszeilenparameter wie die Java-X-Optionen. Daher ist es jetzt auch möglich, die Größe des Java-Heapspeichers zu ändern. Beispiel:

```
dsmj -Xmx512M
```

Web-Client in der neuen Sicherheitsumgebung verwenden

Ab IBM Spectrum Protect Version 8.1.2 können Sie nicht mehr die GUI des Web-Clients verwenden, um eine Verbindung zum IBM Spectrum Protect-Server der Version 8.1.2 oder einer höheren Version 8 oder zum Server der Version 7.1.8 oder einer höheren Version 7 herzustellen.

Wenn eine Verbindung zum IBM Spectrum Protect-Server der Version 8.1.2 oder einer höheren Version 8 oder zum Server der Version 7.1.8 oder einer höheren Version 7 besteht, verwenden Sie die folgenden Alternativen für die GUI des Web-Clients:

- Verwenden Sie zum Sichern und Zurückzuschreiben Ihrer Daten die GUI des Clients für Sichern/Archivieren oder die Befehlszeilenschnittstelle. Geben Sie zum Starten der Befehlszeilenschnittstelle **dsmc** in die Befehlszeile ein. Geben Sie zum Starten der GUI des Clients für Sichern/Archivieren **dsmj** für UNIX- und Linux-Clients bzw. **dsm** für Windows-Clients ein.

Weitere Informationen finden Sie in:

- Kapitel 4, „Daten sichern“, auf Seite 167
- Kapitel 5, „Daten zurückschreiben“, auf Seite 247

- Verwenden Sie zum Sichern und Zurückzuschreiben von NAS-Dateiservern unter Verwendung von NDMP (Network Data Management Protocol) die GUI des Clients für Sichern/Archivieren.

Weitere Informationen finden Sie in:

- „NAS-Dateisysteme mit Network Data Management Protocol sichern“ auf Seite 219
- „NAS-Dateisysteme zurückschreiben“ auf Seite 264

Tipp: Wenn Sie bereits ein Upgrade für den Client für Sichern/Archivieren auf Version 8.1.2 oder höher durchgeführt haben, können Sie den Client deinstallieren und den Client der Version 8.1.0 erneut installieren, um den Web-Client weiterhin zu verwenden. Der IBM Spectrum Protect-Serveradministrator muss den Parameter SESSIONSECURITY auf dem Knoten auf TRANSITIONAL zurücksetzen. Weitere Informationen finden Sie in UPDATE NODE (Knotenattribute aktualisieren).

Web-Client-Sitzung starten

Der Web-Client ist eine Java Web Start-Anwendung, die unabhängig von der Web-Browser-Software gestartet und verwaltet werden kann. Nach der Installation und Konfiguration des Web-Clients auf Ihrer Workstation können Sie den Web-Client für den Fernzugriff verwenden, um Daten auf dem Clientknoten über Fernzugriff zu sichern, zurückzuschreiben, zu archivieren oder abzurufen. Der Web-Client erleichtert die Verwendung von Einheiten für behindertengerechte Bedienung für Benutzer mit Behinderungen und bietet eine verbesserte Navigation über die Tastatur.

Vorbereitende Schritte

Stellen Sie sicher, dass der Web-Client vor seiner Verwendung konfiguriert wird. Sie können den Web-Client mithilfe des Clientkonfigurationsassistenten konfigurieren.

In dem Abschnitt über Softwarevoraussetzungen für Ihr Betriebssystem finden Sie Informationen zu den Browsern, die von dieser Software unterstützt werden.

Zur Ausführung des Web-Clients in Firefox-Browsern muss **JavaScript aktivieren** ausgewählt sein. Diese Option ist in Firefox standardmäßig aktiviert.

Vorgehensweise

1. Geben Sie in Ihrem Web-Browser die URL der Client-Workstation an, auf der Sie den Web-Client installiert haben. Geben Sie außerdem die HTTP-Anschlussnummer an, die auf der Client-Workstation für den Web-Client definiert ist. Die Standardanschlussnummer ist 1581. Das folgende Beispiel zeigt die Syntax einer Web-Client-URL:

```
http://myhost.mycompany.com:1581
```

Wenn Sie während einer Operation eine andere URL eingeben oder auf **Zurück** klicken, wird die Verbindung zum Web-Client getrennt und die aktuelle Operation beendet.

2. Führen Sie die Anweisungen auf der Startseite des Web-Clients in IBM Spectrum Protect aus, um den Web-Client zu starten.

Jedes Mal, wenn der Web-Client gestartet wird, wird eine Java Web Start-Anwendung (Datei `.jnlp`) in Ihren Browser heruntergeladen. Öffnen Sie die Datei `dsm.jnlp`, um den Web-Client zu starten.

Sie können den Web-Browser nach dem Start des Web-Clients schließen.

Tipp: Der Web-Client wird in der Sprache der Workstation des Web-Browsers ausgeführt, da er die JRE verwendet, die lokal auf der Workstation installiert ist. Wenn beispielsweise für die Workstation Ihres Web-Browsers die englische Ländereinstellung aktiv ist und für den fernen Clientknoten Japanisch festgelegt ist, wird die Startseite des Web-Clients in Japanisch, der Web-Client jedoch in Englisch angezeigt.

Zugehörige Konzepte:

„Übersicht über die Konfiguration des Web-Clients“ auf Seite 67

Benutzerberechtigungen

Wenn Sie planen, den Web-Client zu verwenden, stellen Sie sicher, dass Ihnen eine Benutzer-ID mit Administratorberechtigung zugeordnet ist, die über Systemberechtigung, Maßnahmenberechtigung, Clientzugriffsberechtigung oder Clienteignerberechtigung verfügt.

Wenn ein neuer Knoten beim Server registriert wird, muss dem Knoten eine Benutzer-ID mit Administratorberechtigung mit Clienteignerberechtigung zugeordnet werden, die mit dem Knotennamen übereinstimmt.

Der IBM Spectrum Protect-Serveradministrator muss den Parameter `userid` im Serverbefehl **REGISTER NODE** angeben:

```
REGISTER NODE Knotenname Kennwort userid=Benutzer-ID
```

Dabei müssen der Knotenname und die Benutzer-ID mit Administratorberechtigung übereinstimmen. Beispiel:

```
REGISTER NODE node_a mypassword userid=node_a
```

Tipp: Mithilfe der Option `revokeremoteaccess` können Sie verhindern, dass IBM Spectrum Protect-Administratoren mit Clientzugriffsberechtigung über den Web-Client Clientoperationen auf Ihrer Workstation ausführen. IBM Spectrum Protect-

| Administratoren mit Clienteigner-, System- oder Maßnahmenberechtigung können
| jedoch weiterhin über den Web-Client Clientoperationen auf Ihrer Workstation aus-
| führen.

| **Zugehörige Konzepte:**

| „IBM Spectrum Protect-Clientauthentifizierung“ auf Seite 152

| **Zugehörige Verweise:**

| „Revokeremoteaccess“ auf Seite 561

Client-Scheduler automatisch starten

Sie können den Client-Scheduler beim Start Ihrer Workstation automatisch starten.

Hat der IBM Spectrum Protect-Administrator Zeitpläne für Ihren Knoten definiert, können Sie nach dem Starten des Client-Schedulers die Workstation automatisch sichern (oder andere geplante Aktionen ausführen).

Sie können auch den IBM Spectrum Protect-Clientakzeptorservice zum Verwalten des Schedulers verwenden.

Zugehörige Tasks:

„Client-Scheduler-Prozess für die Ausführung als Hintergrundtask und den automatischen Start beim Systemstart definieren“ auf Seite 297

Kennwort ändern

Der IBM Spectrum Protect-Administrator kann für die Verbindung zum Server die Eingabe eines Kennworts durch den Benutzer erforderlich machen.

Informationen zu diesem Vorgang

Der Client für Sichern/Archivieren fordert Sie zur Eingabe des Kennworts auf, falls ein Kennwort erforderlich ist. Wenden Sie sich an den IBM Spectrum Protect-Administrator, wenn Ihnen das Kennwort nicht bekannt ist.

Wichtig: Das Kennwort, das Thema dieses Abschnitts ist, unterscheidet sich von dem Kennwort für die Verschlüsselung von Dateien.

Die Änderung des Kennworts über die grafische Benutzerschnittstelle wird wie folgt vorgenommen:

Vorgehensweise

1. Starten Sie auf Mac OS X-Clients den Client für Sichern/Archivieren mit den IBM Spectrum Protect-Tools für Administratoren.
2. Öffnen Sie im Hauptfenster das Menü **Dienstprogramme** und wählen Sie **Kennwort ändern** aus.
3. Geben Sie das aktuelle und das neue Kennwort ein und geben Sie danach im Feld **Kennwort bestätigen** das neue Kennwort nochmals ein.
4. Klicken Sie auf **Ändern**.

Ergebnisse

Zum Ändern des Kennworts über den Befehlszeilenclient geben Sie den folgenden Befehl ein:

Für UNIX-, Linux- und Windows-Clients:

```
dsmc set password
```

Für Mac OS X-Clients geben Sie den folgenden Befehl ein, um Ihr Kennwort über den Befehlszeilenclient zu ändern:

```
sudo dsmc set password
```

Geben Sie dann nach entsprechender Aufforderung das alte und das neue Kennwort ein.

Die maximale Kennwortlänge beträgt 63 Zeichen. Kennwortbedingungen variieren, abhängig davon, wo die Kennwörter gespeichert und verwaltet werden, und abhängig von der Version des IBM Spectrum Protect-Servers, zu dem Ihr Client die Verbindung herstellt.

Wenn Ihr IBM Spectrum Protect-Server die Version 6.3.3 oder höher aufweist und Sie einen LDAP-Verzeichnissever zum Authentifizieren von Kennwörtern verwenden

Verwenden Sie die folgenden Zeichen, um ein Kennwort zu erstellen:

```
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 . ! @ # $ % ^ & * _ - + = ` ( )  
| { } [ ] : ; < > , ? / ~
```

Bei den Kennwörtern muss die Groß-/Kleinschreibung beachtet werden. Außerdem können die Kennwörter weiteren Einschränkungen aufgrund von LDAP-Richtlinien unterliegen.

Wenn Ihr IBM Spectrum Protect-Server die Version 6.3.3 oder höher aufweist und Sie keinen LDAP-Verzeichnissever zum Authentifizieren von Kennwörtern verwenden

Verwenden Sie die folgenden Zeichen, um ein Kennwort zu erstellen:

```
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 werden in der IBM Spectrum Protect-Serverdatenbank gespeichert. Bei diesen Kennwörtern muss die Groß-/Kleinschreibung nicht beachtet werden.

Wenn Ihr IBM Spectrum Protect-Server eine Version vor Version 6.3.3 aufweist

Verwenden Sie die folgenden Zeichen, um ein Kennwort zu erstellen:

```
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 werden in der IBM Spectrum Protect-Serverdatenbank gespeichert. Bei diesen Kennwörtern muss die Groß-/Kleinschreibung nicht beachtet werden.

Hinweis:

Schließen Sie in der Befehlszeile alle Parameter, die mindestens ein Sonderzeichen enthalten, in Anführungszeichen ein. Ohne Anführungszeichen können die Sonderzeichen als Shell-Escapezeichen, als Dateiumleitungszeichen oder als andere Zeichen, die eine Bedeutung für das Betriebssystem haben, interpretiert werden.

Auf AIX-, Linux- und Solaris-Systemen:

Schließen Sie die Befehlsparameter in Hochkommas (') ein.

Beispiel für die Befehlszeile:

```
dsmc set password -type=vmguest 'Win 2012 SQL'  
'tsml2dag\administrator' '7@#$$%^&7'
```

Anführungszeichen sind nicht erforderlich, wenn Sie ein Kennwort mit Sonderzeichen in einer Optionsdatei eingeben.

Zugehörige Konzepte:

„Client-Scheduler automatisch starten“ auf Seite 160

Zugehörige Tasks:

„Weitere Hinweise zum Starten“ auf Seite 157

Zugehörige Verweise:

„Password“ auf Seite 524

„Set Password“ auf Seite 820

Dateilisten mithilfe der GUI des Clients für Sichern/Archivieren sortieren

Mithilfe der GUI des Clients für Sichern/Archivieren können Sie Dateien anzeigen, sortieren oder auswählen.

Informationen zu diesem Vorgang

Tabelle 33. Über die GUI des Clients für Sichern/Archivieren mit Ihren Dateien arbeiten

Task	Prozedur
Dateien anzeigen	Zum Anzeigen von Dateien in einem Verzeichnis klicken Sie auf das Ordnersymbol neben dem Verzeichnisnamen. Die Dateien werden im Fenster Dateiliste rechts angezeigt.
Dateiliste sortieren	<ul style="list-style-type: none">• Klicken Sie auf die entsprechende Spaltenüberschrift im Fenster Dateiliste.
Aktive und inaktive Sicherungsversionen anzeigen	<ul style="list-style-type: none">• Klicken Sie auf die Option Aktive/inaktive Dateien anzeigen im Menü Sicht.• Klicken Sie in der Funktionsleiste auf das Tool Aktive und inaktive Dateien anzeigen.
Nur aktive Sicherungsversionen anzeigen	Klicken Sie auf die Option Nur aktive Dateien anzeigen im Menü Sicht .
Dateien zum Zurückschreiben oder Abrufen auswählen	<ul style="list-style-type: none">• Klicken Sie auf das Auswahlfeld neben dem Verzeichnis, das Sie zurückschreiben oder abrufen wollen.• Heben Sie die Dateien hervor, die Sie zurückschreiben oder abrufen wollen, und klicken Sie auf das Tool Einträge auswählen in der Funktionsleiste.• Heben Sie die Dateien hervor, die Sie zurückschreiben oder abrufen wollen, und klicken Sie auf die Option Einträge auswählen im Menü Editieren.

Tabelle 33. Über die GUI des Clients für Sichern/Archivieren mit Ihren Dateien arbeiten (Forts.)

Task	Prozedur
Auswahl von Dateien zurücknehmen	<ul style="list-style-type: none"> • Klicken Sie auf das markierte Auswahlfeld neben dem Verzeichnis oder Dateinamen. • Heben Sie die Dateien hervor, deren Auswahl Sie zurücknehmen wollen, und klicken Sie auf das Tool Auswahl der Einträge zurücknehmen in der Funktionsleiste. • Heben Sie die Dateien hervor, deren Auswahl Sie zurücknehmen wollen, und klicken Sie auf die Option Auswahl der Einträge zurücknehmen im Menü Editieren.
Dateiinformati- onen anzeigen	<ul style="list-style-type: none"> • Heben Sie den Dateinamen hervor und klicken Sie auf die Schaltfläche Dateiinformati- onen anzeigen in der Funktionsleiste. • Heben Sie den Dateinamen hervor und klicken Sie auf Dateiinformati- onen im Menü Sicht.

Anmerkung:

1. Falls nicht anders angegeben, gelten die in der oben stehenden Tabelle enthaltenen Tasks und Prozeduren für alle Client-GUIs.
2. Mithilfe der Client-GUIs können Sie eine Liste der Dateien nach verschiedenen Attributen wie Name, Verzeichnis, Größe oder Änderungsdatum sortieren. Das Sortieren von Dateien nach dem Datum der letzten Sicherung kann sehr nützlich zum Bestimmen des Datums und der Uhrzeit für das Zurückschreiben nach Zeitpunkt sein.
3. Eine *aktive* Datei ist die letzte (jüngste) Sicherungsversion einer Datei, die bei der letzten Sicherung auf der Workstation des Benutzers vorhanden war. Alle anderen Sicherungsversionen dieser Datei sind *inaktiv*. Es werden nur aktive Sicherungsversionen von Dateien angezeigt, sofern Sie nicht die Menüoption **Aktive/inaktive Dateien anzeigen** ausgewählt haben. Wird die Datei aus der Workstation gelöscht, wird die aktive Version bei der nächsten Teilsicherung inaktiv.

Im Befehlszeilenclient können Sie **query**-Befehle mit der Option **inactive** verwenden, um sowohl aktive als auch inaktive Objekte anzuzeigen. Sie können **restore**-Befehle mit den Optionen 'pick' und 'inactive' verwenden, um eine Liste der aktiven und inaktiven Sicherungen anzuzeigen, aus denen Sie auswählen können.

Zugehörige Verweise:

„Inactive“ auf Seite 471

„Pick“ auf Seite 528

Onlinehilfe anzeigen

Zum Anzeigen der Onlinehilfe stehen die folgenden Möglichkeiten zur Verfügung: in der GUI des Clients für Sichern/Archivieren, über den Web-Client oder über die **dsmc**-Befehlszeile.

Informationen zu diesem Vorgang

- In der GUI des Clients für Sichern/Archivieren:
 - Öffnen Sie das Hilfemenü. Klicken Sie auf **Hilfe** oder drücken Sie die Taste F1.
 - Klicken Sie auf die Schaltfläche **Hilfe** im aktuellen Fenster.

- Klicken Sie auf Mac-Systemen auf das Fragezeichen (?) in der GUI. Daraufhin werden Onlineinformationen zur aktuellen Operation angezeigt.
- Über die **dsmc**-Befehlszeile: Geben Sie den Befehl **help** ein. Das vollständige Inhaltsverzeichnis für den verfügbaren Hilfetext wird angezeigt.

Zugehörige Verweise:

„**Help**“ auf Seite 731

Sitzung beenden

Sie können eine Clientsitzung über die GUI des Clients für Sichern/Archivieren oder die **dsmc**-Befehlszeile beenden.

Informationen zu diesem Vorgang

- Über die GUI des Clients für Sichern/Archivieren:
 - Öffnen Sie das Menü **Datei** und wählen Sie **Beenden** aus.
 - Drücken Sie Befehl+Q.
 - Öffnen Sie das Menü **Datei** und wählen Sie **Ende** aus.
 - Öffnen Sie das Menü **System** und wählen Sie **Schließen** aus.
 - Für den Web-Client: Öffnen Sie eine andere URL oder schließen Sie den Browser.
- Über die DSMC-Befehlszeile:
 - Im Stapelmodus stellt jeder Befehl **dsmc**, den Sie eingeben, eine vollständige Sitzung dar. Der Client beendet die Sitzung, wenn die Verarbeitung des Befehls beendet ist.
 - Um eine interaktive Sitzung zu beenden, geben Sie **quit** bei der Eingabeaufforderung **Protect>** ein.
 - Soll ein Befehl **dsmc** abgebrochen werden, bevor der Client die Verarbeitung beendet hat, geben Sie QQ an der IBM Spectrum Protect-Konsole ein. In vielen, aber nicht in allen Fällen wird der Befehl dadurch abgebrochen. Kann der Befehl nicht abgebrochen werden, geben Sie den UNIX-Befehl **kill -9** über eine verfügbare Eingabeaufforderung ein. Sie dürfen nicht Strg-C drücken oder den UNIX-Befehl **kill -15** verwenden, da dies zu unerwarteten Ergebnissen führen kann.

Zugehörige Verweise:

„**Loop**“ auf Seite 739

Onlineforen

Um an Benutzerdiskussionen zu IBM Spectrum Protect-Produkten teilnehmen zu können, können Sie eine Subskription für den Listenserver ADSM-L beantragen.

Informationen zu diesem Vorgang

Dieses Benutzerforum wird vom Marist College gepflegt. Obwohl es nicht offiziell von IBM unterstützt wird, nehmen Produktentwickler und andere Mitarbeiter des IBM Support auf informeller Basis ebenfalls an diesem Forum teil und bemühen sich, Ihre Fragen bestmöglich zu beantworten. Da dieses Forum kein offizieller IBM Unterstützungskanal ist, sollten Sie sich an die technische Unterstützung von IBM wenden, falls Sie eine Antwort direkt von IBM benötigen. Andernfalls gibt es keine Garantie dafür, dass sich IBM um Ihr Anliegen kümmert, wenn Sie eine Frage auf den Listenserver gestellt haben.

Sie können sich beim Listenserver registrieren lassen, indem Sie eine E-Mail an folgende Adresse senden:

`listserv@vm.marist.edu`

Der Hauptteil der Nachricht muss Folgendes enthalten:

`SUBSCRIBE ADSM-L vorname nachname`

Der Listenserver sendet Ihnen eine Antwort, in der Sie aufgefordert werden, die Subskriptionsanforderung zu bestätigen. Sobald Sie die Subskriptionsanforderung bestätigt haben, sendet Ihnen der Listenserver weitere Anweisungen. Danach können Sie Nachrichten auf den Listenserver stellen, indem Sie eine E-Mail an folgende Adresse senden:

`ADSM-L@vm.marist.edu`

Wenn Sie zu einem späteren Zeitpunkt die Subskription für ADSM-L aufheben möchten, können Sie eine Nachricht an folgende E-Mail-Adresse senden:

`listserv@vm.marist.edu`

Der Hauptteil der Nachricht muss Folgendes enthalten:

`SIGNOFF ADSM-L`

Sie können außerdem die ADSM-L-Archive lesen und durchsuchen, sich Diskussionsforen anschließen und auf andere Ressourcen unter folgender URL zugreifen:

<http://www.adsm.org>

Kapitel 4. Daten sichern

Verwenden Sie den Client für Sichern/Archivieren, um Sicherungsversionen Ihrer Dateien auf dem IBM Spectrum Protect-Server zu speichern. Sie können diese Sicherungsversionen zurückschreiben, wenn die ursprünglichen Dateien verloren gegangen oder beschädigt sind.

Alle Sicherungs- und Zurückschreibungsprozeduren des Clients gelten auch für den Web-Client.

Einschränkung: Der Web-Client stellt keinen Profileditor zum Definieren von Clientoptionen bereit.

Es folgt eine Liste der primären Sicherungstasks.

- „Sicherungen planen“
- „Hinweise vor der Sicherung (UNIX und Linux)“ auf Seite 169
- „Teilsicherung, selektive Sicherung oder Teilsicherung nach Datum ausführen (UNIX und Linux)“ auf Seite 182
- „Sicherungsdaten löschen“ auf Seite 197
- „Dateien aus einem oder mehreren Dateibereichen für eine Gruppensicherung sichern (UNIX und Linux)“ auf Seite 199
- „Imagesicherung“ auf Seite 206
- „NAS-Dateisysteme mit Network Data Management Protocol sichern“ auf Seite 219

Sicherungen planen

Als Erstbenutzer bzw. als Benutzer, der nur gelegentlich Dateien sichert, können Sie die Tabelle in diesem Abschnitt als Prüfliste für die Schritte verwenden, die vor einer Sicherung auszuführen sind.

Lesen Sie die Liste der Tasks, um festzustellen, ob Sie für die Sicherung Ihrer Daten bereit sind.

- Entscheiden Sie, ob Dateien gesichert oder archiviert werden sollen. Weitere Informationen siehe „Wann werden Dateien gesichert und wann archiviert?“ auf Seite 168.
- „Hinweise vor der Sicherung (UNIX und Linux)“ auf Seite 169 enthält wichtige Hinweise vor dem Sichern Ihrer Dateien und Verzeichnisse.
- Sollen Dateien von den Sicherungsservices ausgeschlossen werden? Weitere Informationen siehe „Einschluss-/Ausschlussoptionen für die Verarbeitungssteuerung“ auf Seite 172.

Zugehörige Konzepte:

Kapitel 1, „IBM Spectrum Protect-Clients für Sichern/Archivieren installieren“, auf Seite 1

Welche Dateien werden gesichert?

Wenn Sie eine Sicherung anfordern, sichert der Client eine Datei, wenn bestimmte Voraussetzungen erfüllt sind.

Damit der Client eine Datei sichert, müssen die folgenden Voraussetzungen erfüllt sein:

- Die ausgewählte Verwaltungsklasse enthält eine Sicherungskopiengruppe.
- Die Datei erfüllt die in der Sicherungskopiengruppe definierten Anforderungen bezüglich der Durchnummerierung. Lautet der Wert des Durchnummerierungsparameters der Kopiengruppe `static` oder `shrstatic` und ändert sich die Datei während der Sicherung, wird die Datei nicht gesichert.
- Die Datei erfüllt die in der Sicherungskopiengruppe definierten Anforderungen bezüglich des Modus (**mode**). Lautet der Parameter **mode** der Kopiengruppe `modified` (Geändert), muss sich die Datei seit der letzten Sicherung geändert haben. Lautet der Modus (**mode**) `absolute` (Absolut), kann die Datei gesichert werden, auch wenn sie sich nicht ändert.
- Die Datei erfüllt die in der Sicherungskopiengruppe definierten Anforderungen bezüglich der Häufigkeit. Seit der letzten Sicherung muss die angegebene Mindestanzahl Tage vergehen, damit eine Datei gesichert wird.
- Die Datei ist nicht durch eine Exclude-Anweisung von der Sicherung ausgeschlossen.
- Die Datei ist nicht durch das Betriebssystem von der Sicherung ausgeschlossen. Diese ausgeschlossenen Dateien befinden sich im Registry-Unterschlüssel `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup`.

Dateien, die zum Windows-Systemstatus gehören, können nur für die Sicherung ausgewählt werden, wenn der Systemstatus gesichert wird. Sie können den Systemstatus nur als Ganzes sichern, da Abhängigkeiten zwischen den Systemstatuskomponenten bestehen. Sie können die Dateien nicht einzeln sichern oder zurückschreiben. Da z. B. `C:\windows\system32\ntoskrnl.exe` zum Windows-Systemstatus gehört, wird diese Datei während einer Teilsicherung oder selektiven Sicherung des Laufwerks `C:\` nicht gesichert.

Zugehörige Konzepte:

Kapitel 9, „Speicherverwaltungsmaßnahmen“, auf Seite 309

„Verwaltungsklassen und Kopiengruppen“ auf Seite 310

Zugehörige Verweise:

„Absolute“ auf Seite 355

Wann werden Dateien gesichert und wann archiviert?

Wenn der Client für Sichern/Archivieren eine Datei sichert oder archiviert, werden eine Kopie der Datei und die zugehörigen Attribute an den Server gesendet. Sicherungs- und Archivierungsoperationen dienen jedoch unterschiedlichen Zwecken.

Verwenden Sie Sicherungen, um die eigenen Dateien gegen unvorhergesehene Beschädigung zu schützen, und Archivierungen, um Versionen Ihrer Dateien längerfristig aufzubewahren.

Sicherungsdaten werden nach Version verwaltet, wobei vordefinierte, auf Maßnahmen basierende Regeln verwendet werden. Mithilfe dieser Regeln kann der IBM Spectrum Protect-Administrator die folgenden Prozesse steuern:

- Die Anzahl der auf dem IBM Spectrum Protect-Server aufbewahrten Versionen
- Die Anzahl der Tage, die jede zusätzliche Sicherungskopie aufbewahrt wird
- Was mit den Sicherungsversionen geschieht, wenn die Datei auf dem Clientsystem gelöscht wird

Jede auf dem Server gespeicherte Kopie der Datei wird als separate und eindeutige Version der Datei betrachtet.

Das Archivieren ist ein leistungsfähiger und flexibler Mechanismus zum Speichern von Langzeitdaten. Archivierungsdaten (Archivierungskopien) werden eine angegebene Anzahl Tage lang aufbewahrt. In der Archivierungsfunktion gibt es kein Konzept und keine Unterstützung für Versionen. Der Benutzer oder Administrator ist für die Festlegung der Dateien verantwortlich, die einer Archivierung hinzugefügt werden.

Tipp: Wird eine Datei mehrmals mit derselben Archivierungsbeschreibung archiviert, wird bei jeder Ausführung der Archivierungsoperation eine neue Kopie der Datei zum Archiv hinzugefügt. Sie sollten in jedem Archiv nur eine Kopie einer Datei speichern, um die Abrufoperation zu vereinfachen.

Sicherungen schützen vor Beschädigung oder Verlust von Dateien, die bei einem versehentlichen Löschen, bei einer Beschädigung oder bei Plattenfehlern auftreten können. Der Server verwaltet mindestens eine Sicherungsversion für jede Datei, die gesichert wird. Ältere Versionen werden gelöscht, wenn neue Versionen erstellt werden. Die Anzahl der vom Server verwalteten Sicherungsversionen wird von Ihrem Administrator festgelegt.

Archivierungskopien werden für die langfristige Speicherung gesichert. Ihr Administrator kann angeben, wie lange Archivierungskopien aufbewahrt werden sollen. Der Server kann eine unbegrenzte Anzahl Archivierungsversionen einer Datei speichern. Archivierungen sind nützlich, wenn eine bestimmte Version Ihrer Dateien wiederhergestellt werden muss oder wenn eine Datei auf Ihrer Workstation gelöscht und bei Bedarf später wieder abgerufen werden soll. Beispielsweise sollen Tabellenkalkulationen möglicherweise für Steuerzwecke gespeichert werden, aber nicht auf Ihrer Workstation bleiben, da sie nicht verwendet werden.

Zugehörige Konzepte:

Kapitel 6, „Daten archivieren und abrufen (UNIX und Linux)“, auf Seite 279

„Daten aus einem Sicherungssatz zurückschreiben“ auf Seite 250

Hinweise vor der Sicherung (UNIX und Linux)

Verschiedene Faktoren in Ihrem System oder Ihrer Umgebung können sich auf die Art und Weise auswirken, wie der Client für Sichern/Archivieren Daten verarbeitet. Lesen Sie diese Hinweise, bevor Sie Ihre Daten sichern.

LAN-unabhängige Datenversetzung

Mit der LAN-unabhängigen Datenversetzung wird das Versetzen von Clientdaten vom DFV-Netz auf das Speicherbereichsnetz (SAN) verlagert. Dadurch wird die Belastung auf dem IBM Spectrum Protect-Server verringert.

Das SAN stellt einen Pfad zur Verfügung, mit dem Sie Daten auf bzw. von einer an das SAN angeschlossenen Speichereinheit sichern, zurückschreiben, archivieren und abrufen können. Die Clientdaten werden mithilfe des IBM Spectrum Protect-Speicheragenten über das SAN auf die Speichereinheit versetzt. Der Speicheragent muss auf demselben System wie der Client installiert werden.

AIX-, Linux- und Solaris-Clients unterstützen die LAN-unabhängige Datenversetzung.

Voraussetzungen für die LAN-unabhängige Datenversetzung

Um die LAN-unabhängige Unterstützung zu aktivieren, müssen Sie den IBM Spectrum Protect for SAN-Speicheragenten auf der Client-Workstation installieren und konfigurieren.

IBM Spectrum Protect for SAN ist ein separates Produkt.

Weitere Informationen zum Installieren und Konfigurieren des Speicheragenten finden Sie in der Dokumentation zu IBM Spectrum Protect for SAN.

Optionen für die LAN-unabhängige Datenversetzung

Um die LAN-unabhängige Datenversetzung zu aktivieren, können Sie verschiedene Clientoptionen verwenden. Sie müssen zunächst den Speicheragenten von IBM Spectrum Protect for SAN auf der Client-Workstation installieren und konfigurieren.

Verwenden Sie die folgenden Optionen, um die LAN-unabhängige Datenversetzung zu aktivieren:

enablelanfree

Gibt an, ob ein verfügbarer LAN-unabhängiger Pfad zu einer an ein SAN angeschlossenen Speichereinheit aktiviert werden soll.

lanfreecommmethod

Gibt ein Übertragungsprotokoll zwischen dem Client und dem Speicheragenten an.

lanfreeshmport

Gibt die eindeutige Zahl an, die vom Client und vom Speicheragenten verwendet wird, um den für die Datenübertragung verwendeten gemeinsam benutzten Speicherbereich (Shared Memory) zu identifizieren.

lanfreetcpport

Gibt die Nummer des TCP/IP-Anschlusses an, an dem der Speicheragent empfangsbereit ist.

lanfreetcpserveraddress

Gibt die TCP/IP-Adresse für den Speicheragenten an.

Zugehörige Verweise:

„Enablelanfree“ auf Seite 429

„Lanfreecommmethod“ auf Seite 495

„Lanfreeshmport“ auf Seite 496

„Lanfreessl“ auf Seite 498

„Lanfreetcpport“ auf Seite 497

„Lanfreetcpserveraddress“ auf Seite 499

Teilsicherungen auf Systemen mit Speicherengpässen

Die Leistung einer Teilsicherung nimmt ab, wenn auf dem System vor dem Start der Sicherung nur wenig Speicher verfügbar ist.

Ist der Speicher auf Ihrem System begrenzt, geben Sie die Option *memoryefficientbackup yes* in Ihrer Clientoptionsdatei an. Diese Option hat zur Folge, dass der Client für Sichern/Archivieren jeweils nur ein einzelnes Verzeichnis verarbeitet, wodurch der Speicherbedarf reduziert, die Sicherungszeit jedoch verlängert wird. Wenn Sie *yes* angeben, analysiert der Client jeweils nur ein einzelnes Verzeichnis für die Sicherung. Bleibt die Leistung schlecht, müssen Sie die Einstel-

lungen des DFV-Puffers und die DFV-Verbindung zwischen Ihrem System und dem IBM Spectrum Protect-Server überprüfen. Steht auf Ihrem System genügend Speicher zur Verfügung, führt das Setzen der Option `memoryefficientbackup` auf `yes` zu einer Verschlechterung der Sicherungsleistung.

Zugehörige Verweise:

„Memoryefficientbackup“ auf Seite 507

Teilsicherungen auf Systemen mit einer großen Anzahl an Dateien

Der Client kann große Speicherkapazitätsanteile verwenden, um Teilsicherungsoperationen auszuführen, insbesondere auf Dateisystemen, die eine große Anzahl an Dateien enthalten.

Der Begriff *Speicher*, wie er hier verwendet wird, bezeichnet den adressierbaren Hauptspeicher, der für den Clientprozess verfügbar ist. Der adressierbare Hauptspeicher ist eine Kombination aus physischem Arbeitsspeicher (RAM) und virtuellem Speicher.

Der Client verwendet durchschnittlich ca. 300 Byte an Speicher pro Objekt (Datei oder Verzeichnis). Somit erfordert der Client für ein Dateisystem mit einer Million Dateien und Verzeichnisse im Durchschnitt ca. 300 MB Speicher. Die genaue Speicherkapazität, die pro Objekt verwendet wird, variiert abhängig von der Länge des Objektpfads und der Länge des Namens oder von der Verschachtelungstiefe der Verzeichnisse. Die Anzahl Datenbyte ist kein wichtiger Faktor bei der Ermittlung des Speicherbedarfs für den Client für Sichern/Archivieren.

Die maximale Anzahl Dateien kann ermittelt werden, indem die für einen Prozess verfügbare maximale Speicherkapazität durch die pro Objekt benötigte durchschnittliche Speicherkapazität dividiert wird.

Der Gesamtspeicherbedarf kann durch eine der folgenden Methoden reduziert werden:

- Verwenden Sie die Clientoption **memoryefficientbackup diskcachemethod**. Mit dieser Auswahl wird die Speicherbelegung auf Kosten der Leistung und einer signifikanten Zunahme des für die Sicherung erforderlichen Plattenspeicherplatzes auf ein Minimum reduziert. Die Dateibeschreibungsdaten vom Server sind in einer plattenresidenten temporären Datenbank gespeichert, nicht im Hauptspeicher. Sobald die Verzeichnisse auf der Workstation durchsucht werden, wird die Datenbank befragt, um festzustellen, ob die einzelnen Objekte gesichert, aktualisiert oder als verfallen markiert werden sollen. Bei Beendigung der Sicherung wird die Datenbankdatei gelöscht.
- Verwenden Sie die Clientoption **memoryefficientbackup yes**. Der durchschnittlich vom Client verwendete Speicher ergibt sich dann aus 300 Byte mal der Anzahl an Verzeichnissen plus 300 Byte pro Datei in dem Verzeichnis, das verarbeitet wird. Bei Dateisystemen mit einer großen Anzahl (Millionen) an Verzeichnissen ist der Client unter Umständen trotzdem nicht in der Lage, ausreichend Speicher zuzuordnen, um Teilsicherungen mit **memoryefficientbackup yes** auszuführen.
- UNIX- und Linux-Clients können möglicherweise die Clientoption **virtualmountpoint** verwenden, um mehrere virtuelle Mountpunkte innerhalb eines einzelnen Dateisystems zu definieren, wobei jeder separat vom Client gesichert werden kann.
- Ist die Clientoption **resourceutilization** auf einen Wert größer als 4 gesetzt und werden mehrere Dateisysteme gesichert, wird durch Reduzieren von

resourceutilization auf maximal 4 der Prozess auf die Teilsicherung jeweils eines einzelnen Dateisystems begrenzt. Diese Einstellung verringert den Speicherbedarf. Ist aus Leistungsaspekten eine parallele Sicherung mehrerer Dateisysteme erforderlich und überschreitet der kombinierte Speicherbedarf die Verarbeitungslimits, können mehrere Instanzen des Sicherungsclients verwendet werden, um mehrere Dateisysteme parallel zu sichern. Wenn Sie z. B. zwei Dateisysteme gleichzeitig sichern wollen, aber deren Speicherbedarf die Grenzwerte eines einzelnen Prozesses überschreitet, dann starten Sie eine Instanz des Clients, um das eine Dateisystem zu sichern, und starten eine zweite Instanz des Clients, um das andere Dateisystem zu sichern.

- Verwenden Sie die Clientoption **-incrbydate**, um eine "Teilsicherung nach Datum" auszuführen.
- Verwenden Sie die Clientoption **exclude.dir**, um zu verhindern, dass der Client Verzeichnisse traversiert und sichert, die nicht gesichert werden müssen.
- Verwenden Sie mit Ausnahme von Mac OS X die Clientfunktion für Imagesicherung, um den gesamten Datenträger zu sichern. Eine Imagesicherung könnte in Wirklichkeit weniger Systemressourcen verwenden und schneller ausgeführt werden als eine Teilsicherung einiger Dateisysteme mit einer großen Anzahl kleiner Dateien.
- Reduzieren Sie die Anzahl Dateien pro Dateisystem, indem Sie die Daten auf mehrere Dateisysteme verteilen.

Zugehörige Verweise:

„Snapdiff“ auf Seite 581

„Exclude-Optionen“ auf Seite 438

„Incrbydate“ auf Seite 490

„Memoryefficientbackup“ auf Seite 507

„Resourceutilization“ auf Seite 557

„Virtualmountpoint“ auf Seite 630

Einschluss-/Ausschlussoptionen für die Verarbeitungssteuerung

Möglicherweise gibt es Dateien in Ihren Dateisystemen, die Sie nicht sichern wollen. Bei diesen Dateien kann es sich um Kerndateien, lokale Caches von Netzdateisystemen, Betriebssystem- oder Anwendungsdateien handeln, die durch Neuinstallation des Programms schnell wiederhergestellt werden könnten, oder um beliebige andere Dateien, die leicht wiederhergestellt werden könnten.

Sie können mithilfe der Optionen **exclude** und **include** in der Einschluss-/Ausschlussoptionsliste angeben, welche Dateien von der Sicherungsverarbeitung ausgeschlossen werden sollen.

Verwenden Sie die Optionen **include** und **exclude** in **dsm.sys**, um die Dateien zu definieren, die in die Teilsicherungsverarbeitung oder die selektive Sicherungsverarbeitung eingeschlossen oder davon ausgeschlossen werden sollen. Eine Datei ist für die Sicherung auswählbar, wenn sie nicht durch die Option **exclude** ausgeschlossen ist. Zum Einschließen bestimmter Dateien in die Sicherung muss die Option **include** nur verwendet werden, wenn sich diese Dateien in einem Verzeichnis befinden, das andere Dateien enthält, die ausgeschlossen werden sollen.

IBM Spectrum Protect bestimmt mithilfe von Verwaltungsklassen, wie die Sicherungen auf dem Server verwaltet werden. Bei jeder Sicherung einer Datei wird ihr eine Verwaltungsklasse zugeordnet. Bei der Verwaltungsklasse kann es sich um die

Standardverwaltungsklasse handeln, die für Sie ausgewählt wurde, oder um eine Verwaltungsklasse, die Sie der Datei mit der Option `include` in der Einschluss-/Ausschlussoptionsliste zuordnen. Wenn Sie eine Verwaltungsklasse zuordnen, muss sie eine Sicherungskopiengruppe enthalten, damit die Datei gesichert wird.

Zugehörige Tasks:

„Einschluss-/Ausschlussliste erstellen“ auf Seite 129

„Client-Scheduler-Prozess für die Ausführung als Hintergrundtask und den automatischen Start beim Systemstart definieren“ auf Seite 297

Datenverschlüsselung während Sicherungs- oder Archivierungsoperationen

Die Datensicherheit wird durch die Verschlüsselung von Daten sichergestellt. Verwenden Sie die Datenverschlüsselung für den Schutz von Daten während einer Sicherungs- oder Archivierungsoperation. Die Standardverschlüsselungsoption ist 128-Bit-AES-Verschlüsselung (AES = Advanced Encryption Standard). Für die höchste Stufe der Datenverschlüsselung verwenden Sie die 256-Bit-AES-Datenverschlüsselung durch Angabe der Option **encryptiontype**.

Die Daten, die Sie einschließen, werden in verschlüsselter Form gespeichert; die Verschlüsselung hat keine Auswirkungen auf das gesendete oder empfangene Datenvolumen.

Die Option **include.encrypt** ist die einzige Möglichkeit, die Verschlüsselung auf dem Client für Sichern/Archivieren zu aktivieren. Werden keine Anweisungen 'include.encrypt' verwendet, kann keine Verschlüsselung stattfinden.

Die Verschlüsselung ist nicht kompatibel mit Sicherungen virtueller VMware-Maschinen im Modus der immer inkrementellen Sicherung (**MODE=IFIncremental** und **MODE=IFFull**). Ist der Client für die Verschlüsselung konfiguriert, können Sie nicht die immer inkrementelle Sicherung verwenden.

Verwenden Sie die Optionen **include** und **exclude** in `dsm.sys`, um die Dateien zu definieren, die in die Teilsicherungsverarbeitung oder die selektive Sicherungsverarbeitung eingeschlossen oder davon ausgeschlossen werden sollen. Eine Datei ist für die Sicherung auswählbar, wenn sie nicht durch die Option **exclude** ausgeschlossen ist. Zum Einschließen bestimmter Dateien in die Sicherung muss die Option **include** nur verwendet werden, wenn sich diese Dateien in einem Verzeichnis befinden, das andere Dateien enthält, die ausgeschlossen werden sollen.

Um Dateidaten zu verschlüsseln, müssen Sie einen Kennwort für den Verschlüsselungsschlüssel auswählen, das der Client zum Generieren des Verschlüsselungsschlüssels zum Verschlüsseln und Entschlüsseln der Dateidaten generiert. Bewahren Sie das Kennwort für den Verschlüsselungsschlüssel für die spätere Verwendung auf. Sie können angeben, ob das Kennwort für den Verschlüsselungsschlüssel in einer Datei mit dem Namen `TSM.sth` gespeichert werden soll, indem Sie die Option **encryptkey** verwenden.

Die Verschlüsselung des IBM Spectrum Protect-Clients ermöglicht Ihnen, einen Wert mit einer Länge von bis zu 63 Zeichen einzugeben. Dieses Verschlüsselungskennwort muss bestätigt werden, wenn die Datei für die Sicherung verschlüsselt wird, und es muss außerdem eingegeben werden, wenn Zurückschreibungen verschlüsselter Dateien ausgeführt werden.

Beim Zurückschreiben der verschlüsselten Datei werden Sie in folgenden Fällen vom Client zur Eingabe des Schlüsselkennworts für die Entschlüsselung der Datei aufgefordert:

- Die Option **encryptkey** ist auf Prompt gesetzt.
- Der vom Benutzer angegebene Schlüssel im vorherigen Fall stimmt nicht überein.
- Die Option **encryptkey** ist auf Save gesetzt und das lokal gespeicherte Schlüsselkennwort stimmt nicht mit der verschlüsselten Datei überein.

Zugehörige Verweise:

„Encryptiontype“ auf Seite 431

„Encryptkey“ auf Seite 431

„Exclude-Optionen“ auf Seite 438

„Include-Optionen“ auf Seite 473

Dateisystem- und ACL-Unterstützung

Spezielle Dateisysteme enthalten dynamische Informationen, die vom Betriebssystem generiert werden; sie enthalten jedoch keine Daten oder Dateien. Die UNIX- und Linux-Clients ignorieren spezielle Dateisysteme und ihren Inhalt.

Das Standalone-Paket LSCqfs

Zu den speziellen Dateisystemen gehören die folgenden Typen:

- Dateisystem /proc auf den meisten UNIX-Plattformen
- Dateisystem /dev/fd unter Solaris
- /dev/pts unter Linux

Der Client für Sichern/Archivieren kann gängige spezifische Dateisystemtypen verarbeiten. Eine Liste der unterstützten Dateisystemtypen finden Sie in Tabelle 34.

Einschränkung: Die Tabelle zeigt vollständige Unterstützung für NFS unter AIX, einschließlich der Erhaltung von ACLs und erweiterten Attributen. Bei anderen Betriebssystemen werden NFS-Sicherungen unterstützt, aber die Sicherungen enthalten nur POSIX-Standardmetadaten (Zugriffsberechtigungen, Erstellungsdatum etc.). Weitere Informationen zur Sicherung von NFS-Dateisystemen finden Sie in „NFS-Dateien sichern“ auf Seite 224.

Tabelle 34. Unterstützte Dateisysteme und ACL-Unterstützung

Plattform	Dateisystem	ACL-Unterstützung
AIX	GPFS	Ja
	JFS	Ja
	JFS2	Ja
	JFS2 NFSV4	Ja
	VxFX	Ja

Tabelle 34. Unterstützte Dateisysteme und ACL-Unterstützung (Forts.)

Plattform	Dateisystem	ACL-Unterstützung
Linux x86_64	Btrfs	Ja
	XFS	Ja
	EXT2	Ja
	EXT3	Ja
	EXT4	Ja
	ReiserFS	Ja
	GPFS	Ja
	JFS	Nein
	VxFS	Nein
	NSS	Ja
Linux on Power Systems Servers	Btrfs	Ja
	XFS	Ja
	EXT2	Ja
	EXT3	Ja
	EXT4	Ja
	ReiserFS	Ja
	JFS	Nein
	GPFS	Ja
Linux on z Systems	Btrfs	Ja
	XFS	Ja
	EXT2	Ja
	EXT3	Ja
	EXT4	Ja
	ReiserFS	Ja
	JFS	Nein
	GPFS	Ja
Mac OS	HFS Standard (HFS)	Ja
	HFS Extended (HFS+)	Ja
	HFS Extended mit Unterscheidung der Groß-/Kleinschreibung (HFSX)	Ja
	Xsan (XSAN) UNIX	Ja
	Universal Disk Format (UDF)	Ja
	ISO9660	Ja
	Apple File System, Groß-/Kleinschreibung muss beachtet werden (APFSCS)	Ja
	Apple File System (APFS)	Ja

Tabelle 34. Unterstützte Dateisysteme und ACL-Unterstützung (Forts.)

Plattform	Dateisystem	ACL-Unterstützung
Solaris	UFS	Ja
	VxFS	Ja
	QFS	Nein
	ZFS	Ja

Bei Dateisystemen, bei denen NFS V4-ACLs definiert sind und verwendet werden (Solaris ZFS und AIX JFS2 V2), wird die Datei oder das Verzeichnis erneut vollständig gesichert, selbst wenn sich nur die UNIX-Standardberechtigungen oder ACLs geändert haben (wie z. B. mit dem Befehl CHMOD). Bei anderen Dateisystemen verursacht diese Art der Änderung nur eine Attributaktualisierung auf dem IBM Spectrum Protect-Server.

Zur Verarbeitung aller anderen Dateisysteme verwenden Sie die Option `virtual-mountpoint`, um Unterstützung für die folgenden Elemente zu aktivieren:

- Für Sicherung, Zurückschreibung, Archivierung und Abruf von Dateidaten
- Für grundlegende UNIX- und Linux-Berechtigungen
- Für Zeitmarken für Änderung, Zugriff und Modifikation und die Verzeichnisbaumstruktur

Keine anderen dateisystemspezifischen Attribute, z. B. die ACL, sind gültig. Der Dateisystemtyp für solche Dateisysteme wird auf "UNKNOWN" (UNBEKANNT) gesetzt.

Wird beispielsweise das Dateisystem `/media/abc/DATA1` vom Client nicht unterstützt, fügen Sie `dsm.sys` die folgende Anweisung hinzu, um die Daten in diesem Dateisystem zu sichern oder zu archivieren:

```
VIRTUALMOUNTPOINT /media/abc/DATA1
```

Diese Unterstützung steht nur zur Verfügung, wenn das Dateisystem selbst grundlegende POSIX-Systemaufrufe wie die Lese- und Schreibverarbeitung auf Ihrem System verwenden kann.

Die plattformübergreifende Sicherung und Zurückschreibung wird nicht unterstützt. Beispielsweise stehen Daten, die von einem AIX-Client gesichert wurden, nicht für die Zurückschreibung durch einen Windows-Client zur Verfügung und umgekehrt.

Anmerkung: Vom Mac OS X-Client gesicherte oder archivierte Daten können von keinem anderen Client zurückgeschrieben werden. Außerdem kann der Mac OS X-Client keine Daten von einem anderen Client zurückschreiben oder abrufen.

Die Methode zum Zurückschreiben oder Abrufen von ACL-Informationen in einen anderen Dateisystemtyp kann verwendet werden, wenn das ursprüngliche Dateisystem und das Zieldateisystem kompatible ACLs unterstützen. So können z. B. unter Solaris die ACL-Informationen, die von einem VxFS-Dateisystem gesichert wurden, auf ein UFS-Dateisystem zurückgeschrieben werden, da diese Dateisysteme kompatible ACLs unterstützen. Bei Operationen zum Zurückschreiben oder Abrufen in andere Dateisystemtypen werden die ACL-Informationen nicht zurückgeschrieben, wenn das ursprüngliche Dateisystem und das Zieldateisystem keine ACLs unterstützen.

Für das Dateisystem QFS gelten die folgenden Einschränkungen:

- Die Imagesicherung wird auf QFS-Dateisystemen nicht unterstützt.
- Der Solaris-Client für Sichern/Archivieren unterstützt nicht die Kombination von QFS und SAM, die benötigt wird, um Dateien auf tertiärem Hintergrundspeicher wie z. B. Bändern zu archivieren. Stattdessen ruft er Dateien automatisch vom Band auf Platte zurück, wenn er während einer Sicherung umgelagerte Dateien findet.
- Ein Dateisystem QFS enthält zwei versteckte Systemdateien und ein Systemverzeichnis, die nicht gesichert werden können. Dies kann akzeptiert werden, da eine Sicherung dieser Dateien nicht notwendig ist. Sie enthalten interne Daten zum Verwalten des Dateisystems. Die internen Daten werden automatisch von einer Sicherung ausgeschlossen und vom Dateisystem selbst automatisch erneut erstellt, wenn eine Zurückschreibung von Dateien in diesem Dateisystem ausgeführt wird.

Unter AIX werden Sicherungs-, Archivierungs-, Zurückschreibungs- und Abrufoperationen mit den Verarbeitungsmodi Teil, selektiv und Dateiliste bei Veritas-Dateisystemen und den zugehörigen ACLs unterstützt. Die Zurückschreibung eines Veritas-Datenträgers auf einen Logical Volume Manager-Datenträger und umgekehrt ist möglich, wenn beide Datenträger denselben Dateisystemtyp verwenden.

Die folgenden Informationen gelten nur für Mac OS X-Systeme:

- Auf Mac OS X-Systemen unterscheiden die Dateisysteme UFS und HFSX die Groß-/Kleinschreibung, während das Dateisystem HFS+ die Groß-/Kleinschreibung nicht unterscheidet, jedoch vorhandene Groß-/Kleinschreibung beibehält. Dateien, die Sie auf einem UFS- oder HFSX-Dateisystem sichern (diese unterscheiden die Groß-/Kleinschreibung), werden auf einem HFS+-Dateisystem möglicherweise nicht korrekt zurückgeschrieben (dieses unterscheidet die Groß-/Kleinschreibung nicht). Beispiel: Auf einem UFS-Dateisystem werden die Dateien `Afile` und `afile` als verschiedene Dateien angesehen. Auf einem HFS+-Dateisystem werden diese beiden Dateien jedoch als identisch angesehen.
- Wenn unter Mac OS X HFS+- oder UFS-Dateisysteme verwendet werden, bei denen die Groß-/Kleinschreibung beachtet werden muss, ist es wichtig, dass die Daten des HFSX- oder UFS-Dateisystems nicht in einem HFS+-Dateisystem auf dem IBM Spectrum Protect-Server gesichert werden. Entweder muss ein neuer Name auf dem System verwendet werden oder der vorhandene Dateibereich auf dem IBM Spectrum Protect-Server muss umbenannt werden. Beispiel: Angenommen, ein System verfügt über ein Dateisystem mit dem Namen `/Volumes/fs2` und dieses System wird mit einem HFS+-Dateisystem mit Unterscheidung der Groß-/Kleinschreibung erneut partitioniert. Entweder muss das Dateisystem `/Volumes/fs2` auf dem IBM Spectrum Protect-Server umbenannt werden oder auf dem lokalen System muss ein neuer Name verwendet werden. Wenn diese Umbenennung nicht erfolgt, werden HFSX-Daten, bei denen die Groß-/Kleinschreibung beachtet werden muss, mit HFS+-Daten gemischt, bei denen die Groß-/Kleinschreibung nicht beachtet werden muss und die bereits auf dem IBM Spectrum Protect-Server gespeichert sind.
- Unter Mac OS X werden Aliasnamen und symbolische Verbindungen gesichert. Der Client sichert jedoch nicht die Daten, auf die die symbolischen Verbindungen verweisen.
- Wenn unter Mac OS X auf einem HFS-Datenträger gesicherte Daten auf einen UFS-Datenträger zurückgeschrieben werden, werden die Ressourcenzweige nicht den richtigen Eignern zugeordnet. Beheben Sie diesen Fehler durch Verwenden des Befehls **chown** für die Ressourcenzweigdatei, um den Eigner zu ändern. In der Ressourcenzweigdatei sind strukturierte Daten in einer Datei gespeichert.

Unter Linux on POWER und Linux on System z müssen Sie `libacl.so` installieren, damit der Client ACLs sichert.

Wichtig: Wenn Sie GPFS für AIX, GPFS für Linux x86_64 oder GPFS für Linux on z Systems in einem Cluster mit mehreren Knoten ausführen und alle Knoten ein angehängtes GPFS-Dateisystem gemeinsam nutzen, verarbeitet der Client dieses Dateisystem als lokales Dateisystem. Der Client sichert während einer Teilsicherung das Dateisystem auf jedem Knoten. Um dies zu vermeiden, können Sie einen der folgenden Schritte ausführen:

- Konfigurieren Sie explizit die Anweisung `domain` in der Clientbenutzeroptionsdatei (`dsm.opt`), sodass die Dateisysteme, die auf diesem Knoten gesichert werden sollen, aufgelistet werden.
- Definieren Sie die Option `exclude.fs` in der Datei `dsm.sys`, damit das GPFS-Dateisystem von den Sicherungsservices ausgeschlossen wird.

Wenn der GPFS-Cluster unterschiedliche Plattformen enthält, dürfen Sie Clients für Sichern/Archivieren nur auf einer einzigen Plattform verwenden, um ein einzelnes Dateisystem zu schützen. Sie dürfen Clients für Sichern/Archivieren nicht auf mehreren Plattformen verwenden, um ein GPFS-Dateisystem zu schützen, das von mehreren Plattformen gemeinsam genutzt wird.

Angenommen, ein Cluster enthält Knoten auf AIX-, Linux x86- und Linux zSeries-Systemen. Sie können Dateisystem A mit AIX-Clients für Sichern/Archivieren und Dateisystem B mit Linux zSeries-Clients für Sichern/Archivieren schützen. Es ist auch möglich, Dateisystem A und Dateisystem B mit AIX-Clients für Sichern/Archivieren zu schützen. Wenn Sie Dateisystem A mit einem AIX-Client für Sichern/Archivieren schützen, dürfen Sie Dateisystem A nicht mit einem Client für Sichern/Archivieren auf einer anderen Plattform als AIX schützen.

Unterstützung der betriebssystemübergreifenden Wiederherstellung für in IBM Spectrum Scale-Dateisystemen gespeicherte Dateien

In einem IBM Spectrum Scale-Cluster mit mehreren Betriebssystemtypen kann eine Datei, die ACL-Metadaten oder Metadaten für erweiterte Attribute enthält und auf einem Quellenbetriebssystem gesichert wurde, auf einem Zielbetriebssystem zurückgeschrieben werden. Die ACL-Metadaten oder Metadaten für erweiterte Attribute werden korrekt zurückgeschrieben, falls beide Betriebssystemtypen auf der Quelle und auf dem Ziel dieselbe Version von IBM Spectrum Scale verwenden.

Die folgenden Quellenbetriebssystemtypen werden unterstützt:

- AIX
- Linux for IBM System Power Big Endian (pBE)
- Linux x86
- Linux for IBM System z

Die folgenden Zielbetriebssystemtypen werden unterstützt:

- Linux for IBM System Power Little Endian (pLE)
- Linux x86
- Linux for IBM System z

Die Sicherheitseinstellungen für betroffene Benutzer und Gruppen müssen auf den Quellen- und Zielsystemen übereinstimmen.

Mischen Sie keine Betriebssystemtypen bei Sicherungsaktivitäten. Wählen Sie nur einen einzigen Betriebssystemtyp aus, der in Ihrem IBM Spectrum Scale-Cluster verfügbar ist, und verwenden Sie ihn für alle Sicherungsoperationen.

Maximale Dateigröße für Operationen

Die maximale Dateigröße ist vom Typ eines Dateisystems abhängig. Der Client für Sichern/Archivieren überprüft während Sicherungs-, Archivierungs-, Zurückschreibungs- oder Abrufoperationen keine Dateigrößenbegrenzung.

Wenn das Dateisystem die Erstellung der Datei ermöglicht, sichert oder archiviert der Client die Datei.

In der folgenden Tabelle sind die maximalen Dateigrößen für die nativen Dateisysteme auf UNIX- und Linux-Clientplattformen angegeben.

Tabelle 35. Maximale Dateigröße

Plattform	Max. Dateigröße (in Byte)
AIX 6.1 (JFS2) - maximale Größe	Maximale JFS2-Dateisystemgröße: 32 TB Maximale JFS2-Dateigröße: 16 TB Minimale JFS2-Dateisystemgröße: 16 MB
Alle Linux-Clients	9 223 372 036 854 775 807 (8 EB - 1)
Mac OS X	HFS - 2 147 485 648 (2 GB) HFS+, HFSX, XSAN und UFS - 9 223 372 036 854 775 808 (8 EB)
Solaris	1 099 511 627 775 (1 TB - 1)
Solaris (ZFS)	18 446 744 073 709 551 616 (16 EB)

Lange Benutzer- und Gruppennamen

Der Client für Sichern/Archivieren kann problemlos Benutzer- und Gruppennamen mit einer Länge von bis zu 64 Zeichen handhaben. Namen, deren Länge 64 Zeichen überschreitet, erfordern jedoch eine besondere Handhabung durch IBM Spectrum Protect.

Wichtig: Überschreiten Sie nicht den Grenzwert von 64 Zeichen für Benutzer- und Gruppennamen. Andernfalls kürzt der Client den Namen unter Verwendung der folgenden Umsetzung so, dass dieser Grenzwert eingehalten wird: An die ersten 53 Zeichen wird ein Schrägstrich (/) und anschließend die numerische ID als Zeichenfolge angehängt.

Eine Fehlernachricht wird protokolliert, die sowohl den langen Namen als auch die daraus resultierende gekürzte Zeichenfolge enthält. Bei den meisten Funktionen müssen Sie sich über den gekürzten Namen nicht bewusst sein. Es gibt folgende Ausnahmen:

- Befehl **set access**
- Option **fromowner**
- (Berechtigungs-)Optionen **users** und **groups**

Wenn Sie einen Namen eingeben müssen, müssen Sie in jedem dieser Fälle entweder die Fehlernachricht mit der Konvertierung finden oder den Namen mithilfe der hier dargelegten Regel konstruieren.

Mac OS X-Datenträgernamen

Der Client für Sichern/Archivieren sichert Datenträger auf der Basis der Namen ihrer UNIX-Mountpunkte.

IBM Spectrum Protect verwaltet jeden Datenträgernamen als separaten Zurückschreibungs- oder Abrufdatenträger. Diese Datenträgernamen werden als Namen der Dateibereiche auf dem Server verwendet.

Wenn Sie den Namen eines Datenträgers ändern, der bereits gesichert wurde, betrachtet der Client den Datenträger als neuen Datenträger, ohne ihn mit dem bereits vorhandenen Datenträger in Zusammenhang zu bringen. Bei Sicherungen werden die Dateien unter dem neuen Namen gesichert. Eine Abweichung kann auftreten, wenn Sie Ihre Datenträger umbenennen oder wenn Sie auf IBM Spectrum Protect von einer anderen Workstation aus zugreifen als derjenigen, von der die Daten gesichert wurden.

Hinweise in Bezug auf Mac OS X-Datenträgernamen

IBM Spectrum Protect erstellt alle neuen Dateibereiche auf dem Server mit dem UNIX-Mountpunkt des Datenträgers.

Sind zwei Datenträger mit Namen wie "La Pomme" und "la pomme" vorhanden, werden zwei eindeutige UNIX-Mountpunkte erstellt.

Die folgenden Beispiele zeigen die beiden Mountpunkte, die erstellt werden:

```
/Volumes/La Pomme  
/Volumes/la pomme
```

Wenn doppelte Datenträger auf Ihrem Desktop doppelt vorhanden sind, können sich die UNIX-Mountpunkte von den Mountpunkten bei der letzten Sicherung unterscheiden, die vom Client ausgeführt wurde. Der Client sichert die Daten möglicherweise nicht im korrekten Dateisystem auf dem IBM Spectrum Protect-Server.

Sie können das Dateisystem überprüfen, in dem der Client die Daten sichert:

1. Wählen Sie im Fenster zum Durchführen von Sicherungen ein Dateisystem aus.
2. Klicken Sie auf **Datei → Info anzeigen**.

Der UNIX-Mountpunkt befindet sich im Informationsdialog.

Potenzielle Probleme mit Namen lassen sich am besten vermeiden, wenn Sie sicherstellen, dass die Datenträgernamen eindeutig sind.

Wichtig:

- Der Client verwendet weiterhin die vorhandenen Dateibereichsnamen auf dem IBM Spectrum Protect-Server. Nur bei neuen Dateibereichen wird der UNIX-Mountpunkt als Name verwendet.
- Geben Sie keine Datenträger an, deren Name Punkte enthält (...). Der Client verwendet die Punktesequenz als Teil der Einschluss-/Ausschlussverarbeitung. Der Client meldet eine ungültige Einschluss-/Ausschlussanweisung zurück, wenn ein Datenträgername eine Punktesequenz enthält. Der Datenträger *muss* umbenannt werden.

Hinweise in Bezug auf Datenträgernamen für Mac OS X-Dual-Boot-Systeme

Wenn Sie über mehrere Mac OS X-Versionen verfügen, zwischen denen Sie wechseln, müssen Sie verstehen, wie der Client die UNIX-Mountpfade für Dateibereichsnamen auf dem IBM Spectrum Protect-Server verwendet.

Angenommen, ein Dual-Boot-System verfügt über zwei Datenträger, El Capitan und Sierra. Im Finder und in der GUI des Clients für Sichern/Archivieren werden diese als El Capitan und Sierra angezeigt. Die UNIX-Mountpunkte sind jedoch davon abhängig, welche Version von Mac OS X aktiv ist. Wenn 'El Capitan' die Startdiskette ist, lauten die UNIX-Pfade wie folgt:

```
/
/Volumes/Sierra
```

Wenn 'Sierra' die Startdiskette ist, lauten die UNIX-Pfade wie folgt:

```
/
/Volumes/El Capitan
```

Wenn eine Sicherungs- oder Archivierungsoperation ausgeführt wird, sind die Dateibereichsnamen auch davon abhängig, welche Version von Mac OS X aktiv ist.

Unter beiden Mac OS X-Versionen werden Sicherungen in das Dateisystem / auf dem IBM Spectrum Protect-Server gestellt. Die Folge ist, dass die Dateisysteme vermischt werden.

Führen Sie eine der folgenden Tasks aus, um potenzielle Probleme mit Dual-Boot-Systemen zu vermeiden:

1. Wählen Sie eine Version von Mac OS X aus, unter der Sie IBM Spectrum Protect installieren und ausführen. Damit wird sichergestellt, dass UNIX-Mountpunkte jedes Mal, wenn der Client eine Sicherung ausführt, identisch sind.
2. Konfigurieren Sie jede Mac OS X-Version mit einem eindeutigen IBM Spectrum Protect-Knotennamen. Schließen Sie dann die andere Mac OS X-Version mit einer Anweisung 'domain' in der Systemoptionsdatei von der Sicherungsverarbeitung aus. Wenn beispielsweise der Datenträger 'Sierra' die Startdiskette ist, fügen Sie der Systemoptionsdatei die folgende Option hinzu:

```
DOMAIN -/Volumes/El Capitan
```

Wenn der Datenträger 'El Capitan' die Startdiskette ist, fügen Sie der Systemoptionsdatei Folgendes hinzu:

```
DOMAIN -/Volumes/Sierra
```

Unicode-Aktivierung für Mac OS X

Der Mac OS X-Client ist Unicode-aktiviert. Für neue Clients, die zum ersten Mal Daten auf dem Server speichern, ist keine spezielle Konfiguration erforderlich.

Der Server speichert Dateien und Verzeichnisse automatisch als Unicode-aktiviert. Wenn Sie jedoch ein Upgrade auf den Unicode-aktivierten Client durchführen, müssen Sie die Migration der vorhandenen Dateibereiche planen, sodass diese Unicode unterstützen können.

Alle Dateibereiche, die sich bereits auf dem Server befinden, müssen umbenannt werden, damit Unicode-aktivierte Dateibereiche erstellt werden können. Verwenden Sie die Option `autofsrename`, um vorhandene Dateibereiche umzubenennen.

Zugehörige Verweise:

„Autofsrename“ auf Seite 366

Mac OS X Time Machine-Sicherungsplatte

Time Machine ist die Sicherungsanwendung, die mit Mac OS X zur Verfügung gestellt wird.

IBM Spectrum Protect kann zusammen mit der Anwendung Mac OS X Time Machine verwendet werden. Aufgrund des besonderen Sicherungsverfahrens der Anwendung Mac OS X Time Machine sind jedoch die folgenden Hinweise zu beachten, bevor Sie den Client für Sichern/Archivieren zum Sichern von Mac OS X Time Machine-Daten verwenden.

- Die Mac OS X Time Machine-Sicherungsplatte verwendet sehr viele feste Verbindungen für sowohl Dateien als auch Verzeichnisse, um die Plattenbelegung zu minimieren. Beträgt die Kapazität der mit der Anwendung Mac OS X Time Machine gesicherten Platte beispielsweise 5 GB, werden bei der ersten Sicherung 5 GB Daten auf die Mac OS X Time Machine-Sicherungsplatte kopiert.

Bei nachfolgenden Sicherungen werden nur die Dateien kopiert, die sich seit der letzten Sicherung geändert haben. Für alle nicht geänderten Dateien und Verzeichnisse werden feste Verbindungen zu der Version erstellt, die bei der vorherigen Sicherung kopiert wurde.

Der Finder zeigt eine Größe von 5 GB für jede Sicherung an, sodass die Gesamtgröße 10 GB beträgt. Durch die Verwendung von festen Verbindungen liegt die gesamte Plattenbelegung jedoch nur knapp über 5 GB.

Alle fest verbundenen Objekte, die sich noch nicht auf dem IBM Spectrum Protect-Server befinden, werden gesichert.

So werden in dem Beispiel 10 GB Daten an den IBM Spectrum Protect-Server gesendet.

- Wenn fest verbundene Dateien zurückgeschrieben werden, erstellt der Client die ursprüngliche feste Verbindung erneut. Die erneute Erstellung der ursprünglichen festen Verbindung ist jedoch nur möglich, wenn *alle* fest verbundenen Dateien gleichzeitig zurückgeschrieben werden. Die gleichzeitige Zurückschreibung aller fest verbundenen Dateien ist keine praktische Methode für eine große Sicherungsplatte, die die Anwendung Mac OS X Time Machine verwendet.
- Wenn die Anwendung Mac OS X Time Machine Dateien auf die Sicherungsplatte kopiert, werden den Dateien Zugriffssteuerungslisten (ACLs) hinzugefügt, um ihre Löschung zu verhindern. Der Client für Sichern/Archivieren kann Dateien mit ACLs sichern und zurückschreiben. Bei allen zurückgeschriebenen Dateien müssen jedoch diese restriktiven ACLs in Kraft sein.

Tipp: Um die besten Ergebnisse zu erzielen, schließen Sie die Sicherungsdaten der Anwendung Time Machine aus. Alle Time Machine-Anwendungsdaten befinden sich in einem Verzeichnis mit dem Namen `Backups.backupdb`.

Zugehörige Konzepte:

„Auszuschließende Systemdateien“ auf Seite 134

Teilsicherung, selektive Sicherung oder Teilsicherung nach Datum ausführen (UNIX und Linux)

Der Administrator kann Zeitpläne definieren, durch die Dateien auf Ihrer Workstation automatisch gesichert werden. In den folgenden Abschnitten wird die Sicherung von Dateien ohne Zeitpläne beschrieben.

Es gibt zwei Arten der Teilsicherung: *vollständige Teilsicherung* und *partielle Teilsicherung*.

Zugehörige Tasks:

„Client-Scheduler-Prozess für die Ausführung als Hintergrundtask und den automatischen Start beim Systemstart definieren“ auf Seite 297

Vollständige und partielle Teilsicherung

Bei einer Teilsicherung werden nur neue und geänderte Dateien gesichert. Der Typ der Teilsicherung ist von den Objekten abhängig, die Sie für die Sicherung auswählen.

Wählen Sie vollständige Dateisysteme aus, führen Sie eine vollständige Teilsicherung aus. Wählen Sie eine Verzeichnisbaumstruktur oder einzelne Dateien aus, führen Sie eine partielle Teilsicherung durch.

Bei der ersten Ausführung einer vollständigen Teilsicherung sichert der Client für Sichern/Archivieren alle angegebenen Dateien und Verzeichnisse. Die Sicherungsoperation kann sehr lange dauern, wenn die Anzahl der Dateien groß ist oder wenn eine oder mehrere große Dateien gesichert werden müssen. Bei nachfolgenden vollständigen Teilsicherungen werden nur neue und geänderte Dateien gesichert. Der Sicherungsserver bewahrt aktuelle Versionen Ihrer Dateien auf, ohne Zeit oder Speicherplatz durch das Sichern von Dateien zu vergeuden, die im IBM Spectrum Protect-Serverspeicher vorhanden sind.

Abhängig von Ihren Speicherverwaltungsmaßnahmen kann der IBM Spectrum Protect-Server mehrere Versionen Ihrer Dateien im Speicher aufbewahren. Die zuletzt gesicherten Dateien sind aktive Sicherungsversionen. Ältere Kopien Ihrer gesicherten Dateien sind inaktive Versionen. Löschen Sie jedoch eine Datei von Ihrer Workstation, wird die aktive Sicherungsversion der Datei bei der nächsten vollständigen Teilsicherung zu einer inaktiven Version. Sie können eine inaktive Version einer Datei zurückschreiben. Die Anzahl der inaktiven Versionen, die vom Server verwaltet werden, und die Dauer ihrer Aufbewahrung werden durch Verwaltungsmaßnahmen gesteuert, die Ihr IBM Spectrum Protect-Serveradministrator definiert. Die aktiven Versionen stellen die Dateien dar, die in Ihrem Dateisystem zum Zeitpunkt der letzten Sicherung vorhanden waren.

Soll eine vollständige oder partielle Teilsicherung über die Client-GUI gestartet werden, wählen Sie **Sichern** und dann die Option **Teilsicherung (vollständig)** aus. In der Befehlszeile verwenden Sie den Befehl **incremental** und geben Sie Dateisysteme, Verzeichnisbaumstrukturen oder einzelne Dateien an, die bei der Sicherung berücksichtigt werden sollen.

Während einer Teilsicherung fragt der Client den Server oder die Journaldatenbank ab, um den genauen Status Ihrer Dateien seit der letzten Teilsicherung zu bestimmen. Der Client verwendet diese Informationen für die folgenden Tasks:

- Neue Dateien sichern.
- Dateien sichern, deren Inhalt sich seit der letzten Sicherung geändert hat.
Dateien werden gesichert, wenn sich eins der folgenden Attribute ändert:
 - Dateigröße
 - Datum oder Uhrzeit der letzten Änderung
 - Erweiterte Attribute
 - Zugriffssteuerungsliste

Wenn sich nur die folgenden Attribute ändern, werden die Attribute auf dem IBM Spectrum Protect-Server aktualisiert, die Datei aber nicht gesichert:

- Dateieigner
- Dateiberechtigungen

- Dateiindex
- Gruppen-ID
- Attribut für die Änderungszeit (ctime) (nur für Objekte in GPFS-Dateisystemen und wenn die Option **updatectime** auf yes gesetzt ist). Weitere ausführliche Informationen finden Sie bei der Option **updatectime**.
- Symbolposition (nur Mac OS X)
- Typ oder Ersteller (nur Mac OS X)

- Verzeichnissicherung.

Ein Verzeichnis wird in einer der folgenden Situationen gesichert:

- Das Verzeichnis wurde noch nicht gesichert.
- Die Verzeichnisberechtigungen haben sich seit der letzten Sicherung geändert.
- Die Verzeichniszugriffssteuerungsliste hat sich seit der letzten Sicherung geändert.
- Die erweiterten Attribute des Verzeichnisses haben sich seit der letzten Sicherung geändert.
- Das Attribut für die Änderungszeit (ctime) wurde seit der letzten Sicherung aktualisiert (nur für GPFS-Dateisysteme). Weitere ausführliche Informationen finden Sie bei der Option **updatectime**.

Verzeichnisse werden bei der Anzahl der gesicherten Objekte mitgezählt. Sollen Verzeichnisse und ihr Inhalt von der Sicherung ausgeschlossen werden, verwenden Sie die Option `exclude.dir`.

- Verfallsverarbeitung für Sicherungsversionen von Dateien auf dem Server durchführen, für die keine entsprechenden Dateien auf der Workstation vorhanden sind. Das Ergebnis ist, dass für Dateien, die auf Ihrer Workstation nicht mehr vorhanden sind, keine aktiven Sicherungsversionen mehr auf dem Server existieren. Inaktive Versionen werden jedoch gemäß den vom IBM Spectrum Protect-Administrator definierten Regeln aufbewahrt.
- Sicherungsversionen erneut binden, wenn sich die Zuordnung der Verwaltungsklassen ändert. Nur Objekte, die über aktive Sicherungsversionen verfügen, werden erneut gebunden. Objekte, für die nur inaktive Sicherungsversionen vorhanden sind, werden nicht erneut gebunden.

Während einer partiellen Teilsicherung werden Objekte wie folgt erneut gebunden oder sie verfallen wie folgt:

Wenn die Dateispezifikation allen Dateien in einem Pfad entspricht:

Erneutes Binden und Verfallsverarbeitung finden für alle auswählbaren Sicherungsversionen statt, die der Dateispezifikation entsprechen. Dies ist der Fall für einen Teilsicherungsbefehl wie `dsmc incr c:\mydir* -subdir=yes`.

Wenn die Dateispezifikation nicht allen Dateien in einem Pfad entspricht:

Erneutes Binden und Verfallsverarbeitung finden für alle auswählbaren Sicherungsversionen statt, die der Dateispezifikation entsprechen. Auswählbare Sicherungsversionen verfallen jedoch nicht bzw. werden nicht erneut gebunden, wenn sie sich in einem Verzeichnis befanden, das im Clientdateisystem nicht mehr vorhanden ist.

Ziehen Sie einen Teilsicherungsbefehl wie `dsmc incr c:\mydir*.txt -subdir=yes` in Betracht. Angenommen, einige Dateien in `c:\mydir\` haben nicht den Dateityp `txt`. Erneutes Binden und Verfallsverarbeitung finden nur für Dateien statt, die der Spezifikation `*.txt` entsprechen und deren Verzeichnisse im Clientdateisystem noch vorhanden sind.

Sie können mit der Option `preserveleastaccessdate` angeben, ob das Datum des letzten Zugriffs nach einer Sicherungs- oder Archivierungsoperation geändert werden soll. Standardmäßig ändert sich das Zugriffsdatum nach einer Sicherungs- oder Archivierungsoperation.

Zugehörige Konzepte:

Kapitel 9, „Speicherverwaltungsmaßnahmen“, auf Seite 309

Zugehörige Verweise:

„Exclude-Optionen“ auf Seite 438

„Preserveleastaccessdate“ auf Seite 536

„Updatectime“ auf Seite 624

Journalbasierte Sicherung unter AIX und Linux

Die journalbasierte Sicherung ist eine alternative Sicherungsmethode, die ein vom IBM Spectrum Protect-Journaldämonprozess verwaltetes Änderungsjournal verwendet.

Unter AIX wird die journalbasierte Sicherung auf JFS- und JFS2-Dateisystemen unterstützt.

Unter Linux wird die journalbasierte Sicherung für Ext2, Ext3, Ext4, XFS, ReiserFS, JFS, VxFS und NSS sowie für ein über NFS gemeinsam genutztes lokales Dateisystem unterstützt. GPFS wird für journalbasierte Sicherungen nicht unterstützt.

Zur Unterstützung der journalbasierten Sicherung müssen Sie den IBM Spectrum Protect-Journaldämon installieren und konfigurieren.

Eine Sicherung eines bestimmten Dateisystems ist journalbasiert, wenn der Journaldämon installiert und für die Aufzeichnung des jeweiligen Dateisystems im Journal konfiguriert wurde und wenn für das Dateisystem ein gültiges Journal erstellt wurde. Die journalbasierte Sicherung wird durch die erfolgreiche Ausführung einer vollständigen Teilsicherung ermöglicht.

Der wichtigste Unterschied zwischen der traditionellen Teilsicherung und der journalbasierten Sicherung liegt in der Methode, mit der die Sicherungs- und Verfallskandidaten ermittelt werden.

Bei der traditionellen Teilsicherung wird die Liste der Sicherungs- und Verfallskandidaten erstellt, indem umfassende Listen lokaler Objekte und Listen aktiver Serverobjekte für das zu sichernde Dateisystem erstellt werden. Zum Erstellen der lokalen Liste wird das gesamte lokale Dateisystem durchsucht. Zum Erstellen der Serverliste wird der gesamte Serverbestand für alle aktiven Objekte abgefragt.

Die beiden Listen werden verglichen und die Kandidaten werden anhand der folgenden Kriterien ausgewählt:

- Ein Objekt wird als Sicherungskandidat ausgewählt, wenn es in der lokalen, aber nicht in der Serverliste vorhanden ist. Das Objekt ist auch ein Sicherungskandidat, wenn es in beiden Listen vorhanden ist, sich jedoch in Bezug auf die Kriterien für die Teilsicherung unterscheidet (beispielsweise geänderte Attribute, geändertes Datum und geänderte Größe).
- Ein Objekt wird als Verfallskandidat ausgewählt, wenn es in der Serverliste, aber nicht in der lokalen Liste vorhanden ist.

Bei der journalbasierten Sicherung wird die Kandidatenliste der Sicherungs- und Verfallsobjekte erstellt, indem der Journaldämon nach dem Inhalt des Änderungs-journals für das zu sichernde Dateisystem abgefragt wird.

Die Änderungsjournaleninträge werden gelöscht (als frei markiert), nachdem sie vom Sicherungscient verarbeitet und auf dem IBM Spectrum Protect-Server festgeschrieben wurden.

Sie können die journalbasierte Sicherung für die Sicherung von Dateisystemen verwenden, bei denen die Änderungsaktivität zwischen den Sicherungszyklen gering oder moderat ist. Wenn zwischen den Sicherungszyklen viele Dateiänderungen auftreten, sind die Änderungsjournalen sehr umfangreich. Umfangreiche Änderungsjournalen können zu Speicher- und Leistungsproblemen führen, die die Vorteile der journalbasierten Sicherung zunichte machen. Werden beispielsweise sehr umfangreiche Verzeichnisstrukturen erstellt, gelöscht, umbenannt oder versetzt, kann dies die Vorteile der journalbasierten Sicherung gegenüber der normalen Teilsicherung aufwiegen.

Die journalbasierte Sicherung ist nicht als vollständiger Ersatz für die traditionelle Teilsicherung gedacht. Sie sollten die journalbasierte Sicherung durch eine regelmäßige, vollständige, progressive Teilsicherung ergänzen. Führen Sie beispielsweise journalbasierte Sicherung täglich und vollständige Teilsicherungen wöchentlich aus.

Bei der journalbasierten Sicherung gelten einige Einschränkungen:

- Einzelne Serverattribute sind während einer journalbasierten Sicherung nicht verfügbar. Bestimmte Maßnahmeneinstellungen wie Kopienhäufigkeit und Kopienmodus werden möglicherweise nicht erzwungen.
- Andere plattformspezifische Verhaltensweisen verhindern möglicherweise, dass Objekte ordnungsgemäß verarbeitet werden. Aufgrund anderer Software, die das Standardverhalten des Dateisystems ändert, werden Dateisystemänderungen möglicherweise nicht festgestellt.
- Wenn das Dateisystem während einer journalbasierten Sicherung sehr aktiv ist, wird eine kleine Anzahl gelöschter Dateien möglicherweise nicht für den Verfall markiert.
- Wenn Sie Dateien in ein Dateisystem mit einem aktiven Journal zurückschreiben, werden einige der zurückgeschriebenen Dateien bei der nächsten journalbasierten Sicherung möglicherweise selbst dann erneut gesichert, wenn die Dateien seit dem Zurückschreiben nicht geändert wurden.
- Bei journalbasierten Sicherungen hat die Option „Skipaclupdatecheck“ auf Seite 581 keine Auswirkungen. Unabhängig davon, wie diese Option festgelegt ist, sichert der Client bei der Ausführung von journalbasierten Sicherungen eines Dateisystems eine Datei immer, wenn ihre ACL oder erweiterten Attribute seit der letzten Sicherung geändert wurden.

Sie sollten regelmäßig vollständige Teilsicherungen und häufigere Journalsicherungen ausführen. Bei der traditionellen Teilsicherung wird der gesamte Dateibestand auf dem Server mit dem gesamten lokalen Dateisystem verglichen. Daher ist die Teilsicherung immer die umfassendste Sicherungsmethode.

Anmerkung: Eine journalbasierte Sicherung wird möglicherweise nicht wieder durch die traditionelle Teilsicherung ersetzt, wenn die Maßnahmendomäne Ihres Knotens auf dem Server geändert wird. Dies ist vom Zeitpunkt der letzten Aktualisierung der Maßnahmengruppe in der Domäne und vom Datum der letzten Teilsicherung abhängig. In diesem Fall müssen Sie eine traditionelle vollständige Teilsicherung erzwingen, um die Dateien erneut an die neue Domäne zu binden.

Verwenden Sie die Option **nojournal** im Befehl **incremental**, um anzugeben, dass statt der standardmäßigen journalbasierten Sicherung eine traditionelle vollständige Teilsicherung ausgeführt werden soll.

Zurückschreibungsverarbeitung mit journalbasierten Sicherungen (AIX und Linux):

Der Journalservice versucht Änderungen zu ermitteln, die in einer Datei als Ergebnis einer Zurückschreibungsoperation auftreten. Wenn eine Datei seit ihrer Zurückschreibung unverändert ist, wird sie während der nächsten journalbasierten Sicherung nicht erneut gesichert. Es wird angenommen, dass Sie eine Datei zurückschreiben, weil sie die Daten enthält, die Sie benötigen. Daher ist eine erneute Sicherung der Datei bei der nächsten Journalsicherung sinnlos. Änderungen, die nach dem Zurückzuschreiben von Dateien an zurückgeschriebenen Dateien vorgenommen werden, müssen als neue Änderungen erkannt werden. Die Datei wird bei der nächsten Journalsicherung verarbeitet.

Wenn für ein bestimmtes Dateisystem ein aktives Journal vorhanden ist, benachrichtigt der Client für Sichern/Archivieren den Journaldämon, wenn eine Datei zurückgeschrieben werden soll. Bei den Änderungen der Datei, die innerhalb eines kurzen Zeitfensters nach der Benachrichtigung des Journaldämons auftreten, wird angenommen, dass sie durch das Zurückzuschreiben der Datei verursacht werden. Diese Änderungen werden nicht aufgezeichnet und die Datei wird bei der nächsten Journalsicherung nicht berücksichtigt.

Während der Journalverarbeitung werden Dateiänderungen, die durch das Zurückzuschreiben der Datei verursacht werden, meistens korrekt identifiziert und die Sicherung der Datei bei der nächsten Journalsicherung wird verhindert.

Systemische Systemverzögerungen, verursacht durch intensive Ein-/Ausgabe oder Dateisystemlatenzzeit, könnten den Beginn einer Zurückschreibungsoperation in dem vom Journaldämon vorgesehenen Zeitrahmen verhindern, nachdem der Dämon von einer anstehenden Zurückschreibung benachrichtigt wurde. Wenn eine solche Verzögerung auftritt, werden Änderungen der Datei als neue Änderungen betrachtet, die nach dem Zurückschreiben der Datei aufgetreten sind. Diese Änderungen werden aufgezeichnet und die Datei wird bei der nächsten Journalsicherung berücksichtigt. Systemische Verarbeitungsverzögerungen und Dateisystemlatenzzeiten liegen außerhalb des Einflussbereichs des Clients für Sichern/Archivieren und sind bekannte Einschränkungen der journalbasierten Sicherung.

Teilsicherung nach Datum

Um ein Dateisystem für Teilsicherungen nach Datum auswählen zu können, müssen Sie mindestens eine vollständige Teilsicherung dieses Dateisystems ausgeführt haben. Wird nur eine Teilsicherung für eine Verzeichnisverzweigung oder für eine einzelne Datei ausgeführt, kann das Dateisystem nicht für Teilsicherungen nach Datum ausgewählt werden.

Der Client sichert nur die Dateien, deren Änderungsdatum und -zeit nach dem Datum und der Zeit der letzten Teilsicherung des Dateisystems liegen, in dem sich die Dateien befinden. Dateien, die von dem Client nach der letzten Teilsicherung hinzugefügt wurden, aber deren Änderungsdatum vor der letzten Teilsicherung liegt, werden nicht gesichert.

Dateien, die nach der letzten Teilsicherung umbenannt wurden, aber ansonsten nicht geändert wurden, werden nicht gesichert. Durch das Umbenennen einer Datei werden das Änderungsdatum und die Änderungszeit der Datei nicht geändert.

Durch das Umbenennen einer Datei wird jedoch das Änderungsdatum des Verzeichnisses, in dem sich die Datei befindet, geändert. In diesem Fall wird das Verzeichnis gesichert, nicht aber die Dateien, die es enthält.

Wird eine Teilsicherung nach Datum für das gesamte Dateisystem ausgeführt, aktualisiert der Server das Datum und die Uhrzeit der letzten Teilsicherung. Wird eine Teilsicherung nach Datum nur für einen Teil eines Dateisystems ausgeführt, aktualisiert der Server nicht das Datum der letzten vollständigen Teilsicherung. In diesem Fall werden diese Dateien bei der nächsten Teilsicherung nach Datum erneut gesichert.

Anmerkung: Anders als bei Teilsicherungen werden bei Teilsicherungen nach Datum gelöschte Dateien nicht als verfallen gekennzeichnet und Sicherungsversionen nicht an eine neue Verwaltungsklasse gebunden, wenn Sie die Verwaltungsklasse ändern.

Zugehörige Tasks:

„Daten über die Java-GUI sichern“ auf Seite 193

Vergleich zwischen Teilsicherung nach Datum, journalbasierter Sicherung sowie NetApp-Momentaufnahmedifferenzsicherung und vollständiger Teilsicherung und partieller Teilsicherung

Teilsicherung nach Datum, journalbasierte Sicherung und NetApp-Momentaufnahmedifferenzsicherung sind Alternativen zur vollständigen und partiellen Teilsicherung.

Teilsicherung nach Datum

Für eine Teilsicherung nach Datum wird weniger Verarbeitungszeit als für eine vollständige Teilsicherung und weniger Speicher benötigt.

Bei einer Teilsicherung nach Datum werden möglicherweise nicht dieselben Sicherungsdateien in den Serverspeicher gestellt, da bei der Teilsicherung nach Datum:

- Keine Sicherungsversionen von Dateien als verfallen gekennzeichnet werden, die Sie von der Workstation löschen.
- Keine Sicherungsversionen an eine neue Verwaltungsklasse gebunden werden, wenn Sie die Verwaltungsklasse ändern.
- Keine Dateien mit Attributen gesichert werden, die sich ändern, es sei denn, das Änderungsdatum und die Änderungszeit ändern sich ebenfalls.
- Das Kopiengruppenattribut für die Häufigkeit in Verwaltungsklassen ignoriert wird (bei journalbasierten Sicherungen wird dieses Attribut ebenfalls ignoriert).

Journalbasierte Sicherung

Der Speicherbedarf für eine anfängliche Journalfunktionsumgebung ist derselbe wie der für eine vollständige Dateibereichsteilsicherung, da journalbasierte Sicherungen eine vollständige Dateibereichsteilsicherung ausführen müssen, damit die Journaldatenbank als gültig definiert und die Basis für die Journalführung erstellt wird.

Der Speicherbedarf für nachfolgende journalbasierte Sicherungen ist weit aus geringer. Journalsicherungssitzungen verlaufen parallel und werden durch die Clientoption `resourceutilization` auf dieselbe Weise geregelt

wie normale Sicherungssitzungen. Die Größe der Journaldatenbankdatei wird auf eine minimale Größe (kleiner als 1 KB) zurückgesetzt, wenn der letzte Eintrag aus dem Journal gelöscht worden ist. Da Einträge aus dem Journal gelöscht werden, sobald sie vom Client verarbeitet wurden, sollte die vom Journal belegte Plattengröße nach einer vollständigen Journalsicherung minimal sein. Eine vollständige Teilsicherung mit aktiver Journalfunktion beansprucht weniger Verarbeitungszeit als eine Teilsicherung nach Datum.

Bei der journalbasierten Sicherung gelten unter AIX und Linux einige Einschränkungen. Weitere Informationen finden Sie in „Journalbasierte Sicherung unter AIX und Linux“ auf Seite 185.

NetApp-Momentaufnahmedifferenz

Bei NAS- und N-Series-Dateiservern, auf denen ONTAP 7.3.0 oder höher aktiv ist, können Sie die Option `snappdiff` zum Aufrufen der NetApp-Momentaufnahmedifferenzsicherung verwenden, wenn eine Teilsicherung des gesamten Datenträgers ausgeführt wird. Durch Verwendung dieser Option wird die Speicherbelegung reduziert und die Verarbeitung beschleunigt.

Beachten Sie die folgenden Einschränkungen bei der Ausführung einer Teilsicherung des gesamten Datenträgers über die Option `snappdiff`, um sicherzustellen, dass die Daten gesichert werden, wenn es erforderlich ist.

- Eine Datei ist aufgrund einer Ausschlussregel in der Einschluss-/Ausschlussdatei ausgeschlossen. Der Client führt eine Sicherung der aktuellen Momentaufnahme aus, während diese Ausschlussregel aktiv ist. Folgendes geschieht, wenn Sie keine Änderungen an der Datei vorgenommen, jedoch die Regel für den Ausschluss dieser Datei entfernt haben. NetApp erkennt diese Änderung an den Einschluss-/Ausschlussregeln nicht, da nur Änderungen an Dateien durch den Vergleich von zwei Momentaufnahmen festgestellt werden.
- Wenn Sie der Optionsdatei eine Include-Anweisung hinzugefügt haben, tritt diese Einschlussoption erst in Kraft, wenn NetApp feststellt, dass die Datei sich geändert hat. Der Client überprüft während einer Sicherung nicht jede Datei auf dem Datenträger.
- Wenn Sie mit dem Befehl **`dsmc delete backup`** explizit eine Datei aus dem IBM Spectrum Protect-Bestand gelöscht haben, erkennt NetApp nicht, dass eine Datei manuell aus dem IBM Spectrum Protect-Speicher gelöscht wurde. Daher verbleibt die Datei ungeschützt im IBM Spectrum Protect-Speicher, bis sie auf dem Datenträger geändert wird und die Änderung von NetApp erkannt wird, wodurch der Client angewiesen wird, die Datei erneut zu sichern.
- Maßnahmenänderungen wie die Änderung der Maßnahme von **`mode=modified`** in **`mode=absolute`** werden nicht festgestellt.
- Der gesamte Dateibereich wird aus dem IBM Spectrum Protect-Datenbestand gelöscht. Diese Aktion bewirkt, dass die Option `snappdiff` eine neue Momentaufnahme erstellt, die als Quelle verwendet wird, und eine vollständige Teilsicherung ausgeführt wird.
- Momentaufnahmedifferenzsicherungsoperationen werden in der IBM Spectrum Protect for Virtual Environments-Umgebung nicht unterstützt. Sie können keine Momentaufnahmedifferenzsicherungsoperationen für ein Dateisystem ausführen, das sich auf einem NetApp-Dateiserver auf einem Host befindet, auf dem auch die Einheit zum Versetzen von Daten von Data Protection for VMware oder Data Protection for Microsoft Hyper-V installiert ist.

Die NetApp-Software bestimmt, was ein geändertes Objekt ist, nicht IBM Spectrum Protect.

Wenn Sie eine Datenträgergesamtsicherung eines über NFS-Mount angehängten NetApp- oder N-Series-Datenträgers ausführen, werden möglicherweise auch alle Momentaufnahmen im Momentaufnahmeverzeichnis gesichert.

Führen Sie einen der folgenden Schritte aus, um zu vermeiden, dass alle Momentaufnahmen im Momentaufnahmeverzeichnis gesichert werden:

- NDMP-Sicherungen ausführen
- Sicherungen mithilfe der Option `snapshotroot` ausführen
- Teilsicherungen mithilfe der Option `snappdiff` ausführen

Tipp: Wenn Sie eine Teilsicherung mit der Option `snappdiff` ausführen und regelmäßige Teilsicherungen planen, verwenden Sie die Option `createnewbase=yes` mit der Option `snappdiff`, um eine Basismomentaufnahme zu erstellen und als Quelle für eine Teilsicherung zu verwenden.

- Das Momentaufnahmeverzeichnis bei Sicherungen ausschließen

Auf Linux-Systemen befindet sich das Momentaufnahmeverzeichnis in `.snapshot`.

Anmerkung: Das Verzeichnis `.snapshot` wird bei einigen Versionen von Red Hat Linux nicht gesichert. Sie müssen es daher nicht ausschließen.

Momentaufnahme-differenzsicherung mit einer HTTPS-Verbindung

Sie können eine sichere HTTPS-Verbindung für die Kommunikation des Clients für Sichern/Archivieren mit einem NetApp-Dateiserver während einer Momentaufnahme-differenzsicherung verwenden.

Das HTTPS-Protokoll ist auf NetApp-Dateiservern standardmäßig aktiviert und kann nicht inaktiviert werden.

Wenn Sie eine Momentaufnahme-differenzsicherung ausführen, baut der Client für Sichern/Archivieren eine Verwaltungssitzung mit einem NetApp-Dateiserver auf. Die Berechtigungsnachweise des Dateiservers (z. B. der Hostname oder die IP-Adresse des Dateiservers, der Benutzername, mit dem eine Verbindung zum Dateiserver hergestellt wird, und das Kennwort des Dateiservers) werden lokal auf dem Client für Sichern/Archivieren gespeichert. Diese Informationen müssen an den Dateiserver übertragen werden, um die authentifizierte Verwaltungssitzung aufbauen zu können. Es ist wichtig, eine sichere Verbindung zu verwenden, weil der Client für die Authentifizierung der Verwaltungssitzung des Dateiservers das Kennwort des Dateiservers in Klartext übertragen muss.

Sie müssen die Option **`snappdiffhttps`** bei jeder Ausführung einer Momentaufnahme-differenzsicherung angeben, um eine sichere Verbindung mithilfe des HTTPS-Übertragungsprotokolls herzustellen. Ohne die Option **`snappdiffhttps`** kann der Client für Sichern/Archivieren Dateiserversitzungen nur mit dem HTTP-Protokoll aufbauen, was eine Aktivierung des HTTP-Verwaltungszugriffs auf dem Dateiserver erforderlich machen würde. Mit der Option **`snappdiffhttps`** können Sie eine sichere Verwaltungssitzung mit dem NetApp-Dateiserver aufbauen, ohne dass hierfür der HTTP-Verwaltungszugriff auf dem NetApp-Dateiserver aktiviert sein muss.

Einschränkungen:

Für Momentaufnahmedifferenzsicherungen mit HTTPS gelten die folgenden Einschränkungen:

- Die HTTPS-Verbindung wird nur für die sichere Übertragung von Daten über die Verwaltungssitzung zwischen dem Client für Sichern/Archivieren und dem NetApp-Dateiserver verwendet. Zu den Daten der Verwaltungssitzung gehören z. B. Berechtigungsnachweise des Dateiservers, Momentaufnahmeinformationen sowie Dateinamen und Attribute, die durch den Momentaufnahmedifferenzierungsprozess generiert werden. Über die HTTPS-Verbindung werden keine normalen Dateidaten übertragen, auf die der Client über die Dateifreigabe auf dem Dateiserver zugreift. Die HTTPS-Verbindung ist auch nicht für normale Dateidaten gültig, die der Client über das normale IBM Spectrum Protect-Client/Server-Protokoll an den IBM Spectrum Protect-Server überträgt.
- Die Option **snappdiffhttps** gilt nicht für vFilers, da das HTTPS-Protokoll auf dem NetApp vFiler nicht unterstützt wird.
- Die Option **snappdiffhttps** ist nur bei Verwendung der Befehlszeilenschnittstelle verfügbar. In der grafischen Benutzerschnittstelle (GUI) des Clients für Sichern/Archivieren kann sie nicht verwendet werden.

Zugehörige Tasks:

„NetApp und IBM Spectrum Protect für Teilsicherungen unter Verwendung der Momentaufnahmedifferenz konfigurieren“ auf Seite 119

„Momentaufnahmedifferenzsicherung mit einer HTTPS-Verbindung ausführen“

Zugehörige Verweise:

„Snappdiffhttps“ auf Seite 588

„Snappdiff“ auf Seite 581

Momentaufnahmedifferenzsicherung mit einer HTTPS-Verbindung ausführen

Wenn Sie eine Momentaufnahmedifferenzsicherung ausführen, können Sie mit der Option **snappdiffhttps** eine sichere HTTPS-Verbindung zwischen dem Client für Sichern/Archivieren und dem NetApp-Dateiserver erstellen.

Vorbereitende Schritte

Bevor Sie mit einer Momentaufnahmedifferenzsicherung über eine HTTPS-Verbindung beginnen, müssen Sie den Client wie in „NetApp und IBM Spectrum Protect für Teilsicherungen unter Verwendung der Momentaufnahmedifferenz konfigurieren“ auf Seite 119 beschrieben konfigurieren.

Diese Methode ist nur in der Befehlszeilenschnittstelle verfügbar.

Vorgehensweise

Geben Sie den Befehl **incremental** mit den Optionen **snappdiff** und **snappdiffhttps** in der Befehlszeilenschnittstelle an, um eine Momentaufnahmedifferenzsicherungsoperation über eine HTTPS-Verbindung zu starten.

Beispiel: Sie verwenden ein Linux-System mit einem über NFS-Mount angehängten Dateisystem/*vol/vol1*, das sich auf dem Dateiserver *homestore.example.com* befindet. Das Verzeichnis */net/home1* ist der Mountpunkt von */vol/vol1*. Geben Sie folgenden Befehl ein:

```
dsmc incr /net/home1 -snappdiff -snappdiffhttps
```

Zugehörige Konzepte:

„Momentaufnahmedifferenzsicherung mit einer HTTPS-Verbindung“ auf Seite 190

Zugehörige Verweise:

Selektive Sicherung

Verwenden Sie eine selektive Sicherung, wenn Sie bestimmte Dateien oder Verzeichnisse sichern möchten, unabhängig davon, ob eine aktuelle Kopie dieser Dateien auf dem Server vorhanden ist.

Teilsicherungen sind im Allgemeinen Teil eines automatisierten Systems zum Sichern vollständiger Dateisysteme. Dagegen können Sie mit selektiven Sicherungen eine Gruppe zu sichernder Dateien manuell auswählen, unabhängig davon, ob sich die Dateien seit der letzten Teilsicherung geändert haben.

Im Gegensatz zu Teilsicherungen bietet eine selektive Sicherung folgende Merkmale:

- Sie bewirkt keine Aktualisierung des Datums und der Uhrzeit der letzten Teilsicherung durch den Server.
- Verzeichnis- und Dateieinträge werden auch dann gesichert, wenn sich ihre Größe, ihre Änderungszeitmarken oder ihre Berechtigungen nicht geändert haben.
- Gelöschte Dateien verfallen nicht.
- Keine Sicherungsversionen an eine neue Verwaltungsklasse gebunden werden, wenn Sie die Verwaltungsklasse ändern.

Zugehörige Tasks:

„Daten über die Java-GUI sichern“ auf Seite 193

Zugehörige Verweise:

„Selective“ auf Seite 810

Sicherungen der globalen Zone und der nicht globalen Zonen in Solaris

Bei Solaris Zones führen Sie Teilsicherungen und selektive Sicherungen von Dateisystemen innerhalb der Zone aus, in der diese Dateisysteme erstellt wurden.

Behandeln Sie jede nicht globale Zone als separates System mit einem eigenen IBM Spectrum Protect-Knotennamen und führen Sie Sicherungen aus jeder der Zonen heraus aus.

Wenn Sie Teilsicherungen oder selektive Sicherungen nicht globaler Zonen aus der globalen Zone heraus ausführen, muss der Administrator der globalen Zone entscheiden, welche Dateien in der nicht globalen Zone bei Sicherungen berücksichtigt oder ausgeschlossen werden. Beispielsweise werden Einheiten-, System- und Kerneldateien der nicht globalen Zonen nicht automatisch von Sicherungen ausgeschlossen, sie dürfen jedoch nicht gesichert werden. Das Zurückschreiben solcher Dateien kann eine nicht globale Zone unbrauchbar machen.

Zugriffsberechtigungen sichern

Während Sie Ihre Dateien sichern, sichert der Client für Sichern/Archivieren auch UNIX-Standardzugriffsberechtigungen, die den Dateien zugeordnet sind.

Abhängig vom Betriebssystem werden auch erweiterte Berechtigungen gesichert. Beispielsweise sichert der Client Zugriffssteuerungslisten für Dateien auf einer AIX-Workstation.

Ein berechtigter Benutzer kann Dateien für einen anderen Benutzer sichern, dies darf jedoch nicht zu Konflikten bei den Eigentumsrechten führen. Der Sicherungs-

server zeichnet ordnungsgemäß auf, dass die Datei dem ursprünglichen Eigner gehört. Der berechtigte Benutzer muss dem ursprünglichen Eigner nicht den Zugriff auf die Sicherungsversionen erteilen.

Virtuellen Mountpunkt definieren

Wenn Sie ein berechtigter Benutzer sind und Dateien ab einem bestimmten Verzeichnis innerhalb eines Dateisystems sichern wollen, können Sie dieses Verzeichnis als virtuellen Mountpunkt definieren.

Das Definieren eines virtuellen Mountpunkts innerhalb eines Dateisystems stellt einen direkten Pfad auf die zu sichernden Dateien zur Verfügung, wodurch Verarbeitungszeit eingespart wird. Dies ist effizienter als zunächst das Dateisystem mit der Option `domain` zu definieren und anschließend mit der Option `exclude` die Dateien auszuschließen, die nicht gesichert werden sollen. Außerdem können hiermit Sicherungen und Archivierungen für bestimmte Verzeichnisse in separaten Dateibereichen im Speicher gespeichert werden.

Zugehörige Verweise:

„Virtualmountpoint“ auf Seite 630

Daten über die Java-GUI sichern

Aus der Verzeichnisbaumstruktur können bestimmte Dateien, vollständige Verzeichnisse oder vollständige Dateisysteme gesichert werden.

Informationen zu diesem Vorgang

Die zu sichernden Dateien können mithilfe einer Such- bzw. Filterfunktion gesucht werden. Beim Filtern werden nur die Dateien angezeigt, die mit den Filterkriterien für die Sicherung übereinstimmen.

Verwenden Sie die Java-GUI des Clients für Sichern/Archivieren, um Ihre Daten wie folgt zu sichern:

Vorgehensweise

1. Klicken Sie auf **Sichern** im Fenster IBM Spectrum Protect. Das Fenster 'Sichern' wird angezeigt.
2. Falls erforderlich, erweitern Sie die Verzeichnisbaumstruktur. Klicken Sie auf die Auswahlfelder neben den zu sichernden Objekten. Zum Suchen oder Filtern von Dateien klicken Sie auf das Symbol **Suchen** in der Funktionsleiste.
3. Geben Sie die Suchkriterien in das Fenster 'Dateien suchen (Sichern)' ein.
4. Klicken Sie auf die Schaltfläche **Suchen**. Das Fenster 'Übereinstimmende Dateien (Sichern)' wird angezeigt.
5. Klicken Sie auf die Auswahlfelder neben den Dateien, die gesichert werden sollen, und schließen Sie das Fenster 'Übereinstimmende Dateien (Sichern)'.
6. Geben Sie die Filterkriterien in das Fenster 'Dateien suchen (Sichern)' ein.
7. Klicken Sie auf die Schaltfläche **Filter**. Das Fenster 'Sichern' zeigt die gefilterten Dateien an.
8. Klicken Sie auf die Auswahlfelder neben den gefilterten Dateien oder Verzeichnissen, die gesichert werden sollen.
9. Wählen Sie eine der folgenden Sicherungsarten im Pulldown-Menü aus: (1) Zum Ausführen einer Teilsicherung klicken Sie auf **Teilsicherung (vollstän-**

dig). (2) Zum Ausführen einer Teilsicherung nach Datum klicken Sie auf **Teilsicherung (nur Datum)**. (3) Zum Ausführen einer selektiven Sicherung klicken Sie auf **Immer sichern**.

10. Klicken Sie auf **Sichern**. Im Fenster **Task-Liste** für die Sicherung wird der Verarbeitungsstatus der Sicherung angezeigt.

Ergebnisse

Beachten Sie die folgenden Hinweise, wenn Sie Ihre Daten über die Java-GUI sichern.

- Um bestimmte Sicherungsoptionen zu ändern, klicken Sie auf die Schaltfläche **Optionen**. Die ausgewählten Optionen sind *nur* während der aktuellen Sitzung wirksam.
- IBM Spectrum Protect bestimmt mithilfe von Verwaltungsklassen, wie die Sicherungen auf dem Server verwaltet werden. Bei jeder Sicherung einer Datei wird ihr eine Verwaltungsklasse zugeordnet. Bei der verwendeten Verwaltungsklasse kann es sich um die Standardverwaltungsklasse handeln, die Ihnen zugeordnet wird, oder um eine Verwaltungsklasse, die Sie der Datei mit der Option *include* in der Einschluss-/Ausschlussoptionsliste zuordnen. Wählen Sie **Dienstprogramme > Maßnahmeninformationen anzeigen** in der Java-GUI des Clients für Sichern/Archivieren oder in der Web-Client-GUI aus, um die Sicherungsmaßnahmen anzuzeigen, die vom IBM Spectrum Protect-Server für Ihren Clientknoten definiert wurden.
- Um eine automatische Teilsicherung Ihrer Standarddomäne auszuführen, wählen Sie **Aktionen → Domäne sichern** aus. Ihre Standarddomäne wird über die Option *domain* in Ihrer Clientbenutzeroptionsdatei (dsm.opt) definiert. Wenn Sie die Option *domain* nicht definiert haben, umfasst die Standarddomäne *alle lokalen Dateisysteme*.
- Sie können den Profileditor verwenden, um Dateisysteme in Ihrer Standarddomäne von der Sicherung auszuschließen.

Zugehörige Konzepte:

Kapitel 9, „Speicherverwaltungsmaßnahmen“, auf Seite 309

Zugehörige Verweise:

„Domain“ auf Seite 407

Daten über die Befehlszeile sichern

Sie können den Befehl **incremental** oder **selective** verwenden, um Sicherungen auszuführen.

Die folgende Tabelle enthält Beispiele zur Verwendung dieser Befehle, um verschiedene Tasks auszuführen.

Tabelle 36. Beispiele für die Sicherung über die Befehlszeile

Task	Befehl	Hinweise
<i>Teilsicherungen</i>		
Eine Teilsicherung Ihrer Clientdomäne ausführen.	dsmc incremental	Der Abschnitt „ Incremental “ auf Seite 732 enthält weitere Informationen zum Befehl incremental .

Tabelle 36. Beispiele für die Sicherung über die Befehlszeile (Forts.)

Task	Befehl	Hinweise
Zusätzlich zu den Dateisystemen /home, /usr und /datasave in Ihrer Clientdomäne die Dateisysteme /fs1 und /fs2 sichern.	<code>dsmc incremental -domain="/fs1 /fs2"</code>	Weitere Informationen zur Option <code>domain</code> befinden sich im Abschnitt „Domain“ auf Seite 407.
Die Dateisysteme /Volumes/fs1 und /Volumes/fs2 neben den Datenträgern sichern, die in Ihrer Clientdomäne definiert sind.	<code>dsmc incremental -domain="/Volumes/fs1 /Volumes/fs2"</code>	Weitere Informationen zur Option <code>domain</code> befinden sich im Abschnitt „Domain“ auf Seite 407.
Alle lokalen Dateisysteme in Ihrer Clientdomäne außer dem Dateisystem /home sichern.	<code>dsmc incremental -domain="all-local -/home"</code>	Sie können den Operator Bindestrich (-) nicht vor dem Domänenschlüsselwort <code>all-local</code> verwenden. Weitere Informationen siehe „Domain“ auf Seite 407. Bei Windows-Clients können Sie auf diese Weise auch die Domäne <code>systemstate</code> von der Sicherungsverarbeitung ausschließen.
Nur die Dateisysteme /fs1 und /fs2 sichern.	<code>dsmc incremental /fs1 /fs2</code>	Keine
Alle Dateien im Verzeichnis /home und in allen seinen Unterverzeichnissen sichern.	<code>dsmc incremental /home/ -subdir=yes</code>	Weitere Informationen zur Option <code>subdir</code> befinden sich im Abschnitt „Subdir“ auf Seite 605.
Alle Dateien im Verzeichnis /Users und in allen seinen Unterverzeichnissen sichern.	<code>dsmc incremental /Users/ -subdir=yes</code>	Weitere Informationen zur Option <code>subdir</code> befinden sich im Abschnitt „Subdir“ auf Seite 605.
Angenommen, Sie haben eine Momentaufnahme des Dateisystems /usr gestartet und die Momentaufnahme als /snapshot/day1 angehängt. Führen Sie eine Teilsicherung aller Dateien und Verzeichnisse unter der lokalen Momentaufnahme aus und verwalten Sie sie auf dem IBM Spectrum Protect-Server unter dem Dateibereichsnamen /usr.	<code>dsmc incremental /usr -snapshotroot=/snapshot/day1</code>	Der Client für Sichern/Archivieren betrachtet den Wert für <code>snapshotroot</code> als Dateibereichsnamen. Weitere Informationen finden Sie in „Snapshotroot“ auf Seite 593.
<i>Teilsicherung nach Datum</i>		
Eine Teilsicherung Ihrer Standardclientdomäne nach Datum ausführen.	<code>dsmc incremental -incrbydate</code>	Verwenden Sie die Option <code>incrbydate</code> im Befehl incremental , um neue und geänderte Dateien zu sichern, deren Änderungsdatum nach dem Datum der letzten auf dem Server gespeicherten Teilsicherung liegt. „Incrbydate“ auf Seite 490 enthält weitere Informationen zur Option <code>incrbydate</code> .

Selektive Sicherungen

Tabelle 36. Beispiele für die Sicherung über die Befehlszeile (Forts.)

Task	Befehl	Hinweise
Alle Dateien im Verzeichnis /home/proj oder /Users/van/Documents sichern.	dsmc selective /home/proj/ oder dsmc selective /Users/van/Documents/	Verwenden Sie den Befehl selective , um bestimmte Dateien oder Verzeichnisse unabhängig davon zu sichern, ob sich die Dateien seit der letzten Teilsicherung geändert haben. Mithilfe von Platzhalterzeichen können mehrere Dateien gleichzeitig gesichert werden. Der Abschnitt „ Selective “ auf Seite 810 enthält weitere Informationen zum Befehl selective .
Alle Dateien im Verzeichnis /home/proj und in allen seinen Unterverzeichnissen sichern.	dsmc selective /home/proj/ -subdir=yes	Wenn Sie beim Sichern eines bestimmten Pfads und einer bestimmten Datei -subdir=yes angeben, sichert der Client rekursiv alle Unterverzeichnisse unter diesem Pfad und alle Instanzen der angegebenen Datei, die sich unter einem dieser Unterverzeichnisse befinden. Wenn es sich bei einem Unterverzeichnis um ein angehängtes Dateisystem handelt, sichert der Client die Dateien in diesem Unterverzeichnis nicht, wenn Sie die Option subdir=yes verwenden. Weitere Informationen zur Option subdir finden Sie in „Subdir“ auf Seite 605.
Alle Dateien im Verzeichnis /Users/van/Documents und in allen seinen Unterverzeichnissen sichern.	dsmc selective /Users/van/Documents/ -subdir=yes	Wenn Sie beim Sichern eines bestimmten Pfads und einer bestimmten Datei die Option -subdir=yes angeben, sichert der Client rekursiv alle Unterverzeichnisse unter diesem Pfad und alle Instanzen der angegebenen Datei, die sich unter einem dieser Unterverzeichnisse befinden. Wenn es sich bei einem Unterverzeichnis um ein angehängtes Dateisystem handelt, sichert der Client die Dateien in diesem Unterverzeichnis nicht, wenn Sie die Option subdir=yes verwenden. Weitere Informationen zur Option subdir finden Sie in „Subdir“ auf Seite 605.
Die Dateien /home/dir1/h1.doc und /home/dir1/test.doc sichern.	dsmc selective /home/dir1/h1.doc /home/dir1/test.doc	Geben Sie die Option removeoperandlimit mit dem Befehl incremental oder selective an, wird die Beschränkung auf 20 Operanden nicht umgesetzt und nur durch die verfügbaren Ressourcen oder andere Begrenzungen des Betriebssystems eingeschränkt. Dies ermöglicht Ihnen, mehr als 20 Dateien in einem einzelnen Befehl anzugeben. Weitere Informationen zu dieser Option siehe „Removeoperandlimit“ auf Seite 546.

Tabelle 36. Beispiele für die Sicherung über die Befehlszeile (Forts.)

Task	Befehl	Hinweise
Die Dateien /Users/ann/Documents/h1.doc und /Users/ann/Documents/test.doc sichern.	<code>dsmc selective /Users/ann/Documents/h1.doc /Users/ann/Documents/test.doc</code>	Geben Sie die Option <code>removeoperandlimit</code> mit dem Befehl incremental oder selective an, wird die Beschränkung auf 20 Operanden nicht umgesetzt und nur durch die verfügbaren Ressourcen oder andere Begrenzungen des Betriebssystems eingeschränkt. Dies ermöglicht Ihnen, mehr als 20 Dateien in einem einzelnen Befehl anzugeben. Weitere Informationen zu dieser Option finden Sie in „Removeoperandlimit“ auf Seite 546.
Eine Liste von Dateien in der Datei /home/filelist.txt sichern.	<code>selective -filelist=/home/filelist.txt</code>	Verwenden Sie die Option <code>filelist</code> , um eine Liste von Dateien zu verarbeiten. Weitere Informationen siehe „Filelist“ auf Seite 453.
Alle Dateien sichern, die in der Datei /Users/filelist.txt aufgeführt sind.	<code>dsmc selective -filelist=/Users/filelist.txt</code>	Verwenden Sie die Option <code>filelist</code> , um eine Liste von Dateien zu verarbeiten. Weitere Informationen siehe „Filelist“ auf Seite 453.
Angenommen, Sie haben eine Momentaufnahme des Dateisystems /usr gestartet und die Momentaufnahme als /snapshot/day1 angehängt. Führen Sie eine selektive Sicherung der Verzeichnisbaumstruktur /usr/dir1/sub1 aus der lokalen Momentaufnahme durch und verwalten Sie sie auf dem IBM Spectrum Protect-Server unter dem Dateibereichsnamen /usr.	<code>dsmc selective /usr/dir1/sub1 -subdir=yes -snapshotroot=/snapshot/day1</code>	Der Client betrachtet den Wert für <code>snapshotroot</code> als Dateibereichsnamen. Weitere Informationen finden Sie in „Snapshotroot“ auf Seite 593.

Zugehörige Verweise:

„Incremental“ auf Seite 732

„Selective“ auf Seite 810

Sicherungsdaten löschen

Wenn Sie vom Administrator entsprechend berechtigt wurden, können Sie einzelne Sicherungskopien aus dem IBM Spectrum Protect-Server löschen, ohne den gesamten Dateibereich zu löschen. Um festzustellen, ob Sie über diese Berechtigung verfügen, wählen Sie **Datei > Verbindungsinformationen** in der GUI des Clients für Sichern/Archivieren oder im Hauptmenü des Web-Clients aus. Ihr Berechtigungstatus wird im Feld **Sicherungsdateien löschen** zur Verfügung gestellt.

Informationen zu diesem Vorgang

Wichtig: Nach dem Löschen von Sicherungsdateien können diese nicht mehr zurückgeschrieben werden. Stellen Sie vor dem Löschen sicher, dass die gesicherten Dateien nicht mehr benötigt werden. Der Client fordert eine Bestätigung für den Löschvorgang an. Geben Sie daraufhin *ja* an, werden die angegebenen Dateien sofort gelöscht und aus dem IBM Spectrum Protect-Serverspeicher entfernt.

Vorgehensweise

Um Sicherungskopien mithilfe der GUI des Clients für Sichern/Archivieren oder des Web-Clients zu löschen, gehen Sie wie folgt vor:

1. Wählen Sie im Menü **Dienstprogramme > Sicherungsdaten löschen** aus. Das Fenster **Sicherung löschen** wird angezeigt.
2. Erweitern Sie die Verzeichnisbaumstruktur, indem Sie auf das Pluszeichen (+) oder auf das Ordnersymbol neben dem Objekt, das eingeblendet werden soll, klicken.
3. Klicken Sie auf die Auswahlfelder neben den Objekten, die gelöscht werden sollen.
4. Wählen Sie einen Eintrag aus der Dropdown-Liste im oberen Bereich des Fensters **Sicherung löschen** aus, um anzugeben, welche Art von 'Sicherung löschen' ausgeführt werden soll. Sie können aktive Sicherungsversionen, inaktive Sicherungsversionen oder alle in der Baumstruktur ausgewählten Objekte löschen.
5. Klicken Sie auf **Löschen**, um mit dem Löschen der ausgewählten Einträge zu beginnen.

Ergebnisse

Anmerkung:

- Wenn Sie **Aktive Objekte löschen** oder **Inaktive Objekte löschen** angeben, werden nur die Dateien beim Entfernen berücksichtigt.
- Wenn Sie **Aktive Objekte löschen** oder **Inaktive Objekte löschen** angeben und ein Verzeichnis auswählen, das keine Dateien zum Entfernen enthält, wird während der Operation zum Löschen von Sicherungen die folgende Nachricht angezeigt:
ANS5030E Keine Objekte auf dem Server stimmen mit der Abfrage überein.
Das letzte übergeordnete inaktive Verzeichnis wird auf der Basis der Einstellungen für die Aufbewahrungsmaßnahme auf dem Server entfernt.
- Ein Verzeichnis wird nur gelöscht, wenn Sie **Alle Objekte löschen** auswählen.
- Um Dateibereiche zu löschen, klicken Sie im Hauptfenster auf **Dienstprogramme > Dateibereiche löschen**.
- Um Sicherungskopien mithilfe des Befehlszeilenclients zu löschen, verwenden Sie den Befehl **delete backup**.

Zugehörige Verweise:

„Delete Backup“ auf Seite 722

Dateibereiche löschen

Erteilt der IBM Spectrum Protect-Administrator einem Benutzer die Berechtigung, kann der Benutzer vollständige Dateibereiche aus dem Server löschen. Beim Löschen eines Dateibereichs werden alle Dateien und Images, sowohl Sicherungsversionen als auch Archivierungskopien, innerhalb dieses Dateibereichs gelöscht. Wird beispielsweise der Dateibereich /tmp gelöscht, werden alle Sicherungsversionen für alle Dateien in diesem Dateisystem und alle aus diesem Dateisystem archivierten Dateien gelöscht. Das Löschen eines Dateibereichs muss gründlich überlegt werden.

Informationen zu diesem Vorgang

Sie können einen Dateibereich auch mit dem Befehl **delete filespace** löschen. Verwenden Sie die Option `class` im Befehl **delete filespace**, um NAS-Dateibereiche zu löschen.

Sie können einzelne Sicherungsversionen löschen, indem Sie den Befehl **delete backup** verwenden.

Sie können Dateibereiche mithilfe der GUI des Clients für Sichern/Archivieren oder mithilfe von Befehlszeilenclients löschen. Um NAS-Dateibereiche zu löschen, verwenden Sie den Web-Client oder den Befehlszeilenclient.

Soll ein Dateibereich mit der grafischen Benutzerschnittstelle gelöscht werden, führen Sie die folgenden Schritte aus:

Vorgehensweise

1. Wählen Sie im Hauptfenster die Optionen **Dienstprogramme > Dateibereiche löschen** aus.
2. Klicken Sie auf die Auswahlfelder neben den Dateibereichen, die gelöscht werden sollen.
3. Klicken Sie auf die Schaltfläche **Löschen**. Der Client fordert Sie zur Bestätigung auf, bevor der Dateibereich gelöscht wird.

Zugehörige Verweise:

„Class“ auf Seite 374

„Delete Backup“ auf Seite 722

„Delete Filespace“ auf Seite 727

Dateien aus einem oder mehreren Dateibereichen für eine Gruppensicherung sichern (UNIX und Linux)

Mit dem Befehl **backup group** können Sie eine Gruppe, die eine Liste von Dateien aus einem oder mehreren Dateibereichsursprüngen enthält, erstellen und in einem virtuellen Dateibereich auf dem IBM Spectrum Protect-Server sichern.

Einschränkung: Der Befehl **backup group** gilt nicht für Mac OS X.

Über eine *Gruppensicherung* können Sie eine konsistente zeitpunktgesteuerte Sicherung für eine Gruppe von Dateien erstellen, die gemeinsam als logische Einheit verwaltet werden:

- Allen Objekten in der Gruppe wird dieselbe Verwaltungsklasse zugeordnet.
- Vorhandene Anweisungen *exclude* für Dateien in der Gruppe werden ignoriert.
- Alle Objekte in der Gruppe werden gemeinsam exportiert.
- Alle Objekte in der Gruppe verfallen gemeinsam wie in der Verwaltungsklasse angegeben. Keine Objekte in der Gruppe verfallen, bevor nicht alle anderen Objekte in der Gruppe verfallen, selbst wenn eine andere Gruppe, zu denen diese Objekte gehören, verfällt.

Eine Gruppensicherung kann zu einem Sicherungssatz hinzugefügt werden.

Mithilfe der Option `mode` können Sie eine Gesamtsicherung oder eine Differenzsicherung ausführen.

Beispiel: Geben Sie Folgendes ein, um eine Gesamtsicherung aller in der Datei /home/dir1/filelist1 aufgeführten Dateien auf den virtuellen Dateibereich /virtfs auszuführen, der das Hauptmember /home/group1 enthält:

```
dsmc backup group -filelist=/home/dir1/filelist1 -groupname=group1 -virtualfsname=
/virtfs -mode=full
```

Zugehörige Konzepte:

„Daten aus einem Sicherungssatz zurückschreiben“ auf Seite 250

Zugehörige Verweise:

„Backup Group“ auf Seite 699

„Include-Optionen“ auf Seite 473

„Mode“ auf Seite 509

Daten mit der Unterstützung für den Clientknoten-Proxy sichern (UNIX und Linux)

Sicherungen mehrerer Knoten, die Speicher gemeinsam benutzen, können zu einem einheitlichen Zielknotennamen auf dem IBM Spectrum Protect-Server konsolidiert werden.

Informationen zu diesem Vorgang

Die Konsolidierung von Sicherungen zu einem einheitlichen Zielknotennamen auf dem Server ist bei Konfigurationen hilfreich, bei denen sich die für die Durchführung der Sicherung zuständige Workstation mit der Zeit ändern kann, wie es beispielsweise bei einem Cluster der Fall ist.

Ein Agentenknoten ist ein Clientknoten, dem die Berechtigung erteilt wird, Clientoperationen im Namen eines Zielknotens auszuführen.

Ein Zielknoten ist ein Clientknoten, der einem oder mehreren Agentenknoten die Berechtigung erteilt, in seinem Namen Clientoperationen auszuführen.

Verwenden Sie die Option `asnodename` mit dem entsprechenden Befehl, um Daten unter dem Zielknotennamen auf dem Server zu sichern, zu archivieren, zurückzuschreiben und abzurufen.

Mit der Option `asnodename` können Daten außerdem von einem anderen System zurückgeschrieben werden als dem, auf dem die Sicherung ausgeführt wurde.

Beachten Sie Folgendes, wenn Sie einen Proxy-Knoten verwenden, um Daten auf anderen Knoten zu sichern oder zurückzuschreiben:

- Eine Proxy-Operation verwendet die Einstellungen für den Zielknoten (beispielsweise **maxnummp** und **deduplication**) sowie Zeitpläne, die auf dem IBM Spectrum Protect-Server definiert sind. Die Einstellungen und Zeitpläne für den Agentenknoten auf dem IBM Spectrum Protect-Server werden ignoriert.
- Auf allen Agentenknoten in der Mehrfachknotenumgebung muss derselben Betriebssystemtyp ausgeführt werden.
- Verwenden Sie keine Zielknoten als herkömmliche Knoten, insbesondere, wenn Sie Ihre Dateien vor der Sicherung auf dem Server verschlüsseln.
- Sie können nicht auf einen anderen Knoten zugreifen (weder über die GUI-Dropdown-Liste noch mithilfe der Option `fromnode`).
- Sie können keine NAS-Sicherung oder -Zurückschreibung durchführen.

Vorgehensweise

1. Installieren Sie den Client für Sichern/Archivieren auf allen Knoten in einer gemeinsamen Datenumgebung.
2. Registrieren Sie jeden Knoten beim IBM Spectrum Protect-Server. Registrieren Sie den einheitlichen Zielknotennamen, damit er von allen Agentenknoten in Ihrer gemeinsamen Datenumgebung gemeinsam genutzt werden kann.
3. Registrieren Sie jeden Knoten in der gemeinsamen Datenumgebung beim IBM Spectrum Protect-Server. Registrieren Sie den Agentenknotennamen, der für Authentifizierungszwecke verwendet wird. Daten werden nicht unter diesem Knotennamen auf dem Server gespeichert, wenn die Option `asnodename` verwendet wird.
4. Der IBM Spectrum Protect-Serveradministrator muss mithilfe des Befehls `GRANT PROXYNODE` allen Knoten in der gemeinsam genutzten Umgebung Proxy-Berechtigung erteilen, damit sie auf den Zielknotennamen zugreifen können.
5. Verwenden Sie den Verwaltungsklientbefehl `QUERY PROXYNODE`, um die Clientknoten des berechtigten Benutzers anzuzeigen, dem mit dem Befehl `GRANT PROXYNODE` die Berechtigung erteilt wurde.

Zugehörige Verweise:

„Asnodename“ auf Seite 359

Operationen mit mehreren Knoten von der GUI aktivieren

In der GUI können Sie Operationen mit mehreren Knoten aktivieren. Hierzu geben Sie im Profileditor den Namen des Zielknotens an, für den Ihnen Proxy-Berechtigung erteilt wurde.

Vorgehensweise

1. Prüfen Sie, ob der Clientknoten Proxy-Berechtigung für einen Zielknoten hat (oder berechtigt ist, als Zielknoten zu handeln). Verwenden Sie dazu den Verwaltungsklientbefehl `QUERY PROXYNODE`.
2. Wählen Sie **Editieren > Clientvorgaben** aus, um das Fenster 'Vorgaben' zu öffnen.
3. Wählen Sie die Registerkarte **Allgemein** aus und füllen Sie das Feld **Wie Knotenname** mit dem Namen des Zielknotens aus.
4. Klicken Sie auf **Anwenden** und anschließend auf **OK**, um das Fenster 'Vorgaben' zu schließen.

Nächste Schritte

Führen Sie einen der folgenden Schritte aus, um zu bestätigen, dass Ihr Clientknoten jetzt als Zielknoten auf den Server zugreift:

- Öffnen Sie das Baumstrukturfenster und überprüfen Sie, ob der Zielknotenname, der im Feld **Wie Knotenname** angegeben ist, angezeigt wird.
- Bestätigen Sie den Zielknotenamen im Feld **Zugriff als Knoten** im Fenster **Verbindungsinformationen**.

Um zur Operation mit Einzelknoten zurückzukehren, löschen Sie **Wie Knotenname** im Feld **Zugriff als Knoten** auf der Registerkarte **Allgemein > Vorgaben**.

Verschlüsselung definieren

In diesem Abschnitt sind die Schritte aufgelistet, die Sie ausführen müssen, um die Verschlüsselung mit der Option `encryptkey` einzurichten.

Vorgehensweise

1. Geben Sie **encryptkey=save** in der Optionsdatei an.
2. Sichern Sie mindestens eine Datei mit **asnode=ProxyNodeName**, um auf jedem Agentenknoten in der Mehrfachknotenumgebung einen lokalen Verschlüsselungsschlüssel zu erstellen.

Ergebnisse

Führen Sie die folgenden Schritte aus, um mit der Option **encryptkey=prompt** die Verschlüsselung zu definieren:

1. Geben Sie **encryptkey=prompt** in der Optionsdatei an.
2. Stellen Sie sicher, dass die Benutzer der Agentenknoten in der Mehrfachknotenumgebung denselben Verschlüsselungsschlüssel verwenden.

Wichtig:

- Wenn Sie den Verschlüsselungsschlüssel ändern, müssen Sie die vorherigen Schritte wiederholen.
- Verwenden Sie denselben Verschlüsselungsschlüssel für alle Dateien, die in der gemeinsam genutzten Knotenumgebung gesichert wurden.

Sicherungen mit der Unterstützung für den Clientknoten-Proxy planen

Es können mehrere Knoten verwendet werden, um Sicherungsoperationen mithilfe des Schedulers auszuführen.

Informationen zu diesem Vorgang

Wenn Sie den Agentenknoten Proxy-Berechtigung erteilen, führen diese geplante Sicherungsoperationen für den Zielknoten aus. Jeder Agentenknoten muss die Option **asnodename** innerhalb seines Zeitplans verwenden, um eine Mehrfachknotensicherung für den Agentenknoten auszuführen.

Starten Sie die Zeitpläne mit dem Clientbefehl **dsmc sched**:

Die folgenden Beispiele zeigen die Client/Server-Verwaltungsbefehle unter Verwendung des Schedulers auf mehreren Knoten.

- Der Administrator registriert alle zu verwendenden Knoten, indem er die folgenden Befehle ausgibt:
 - `register node NODE-A`
 - `register node NODE-B`
 - `register node NODE-C`
- Der Administrator erteilt mithilfe der folgenden Befehle jedem Agentenknoten Proxy-Berechtigung:
 - `grant proxynode target=NODE-Z agent=NODE-A`
 - `grant proxynode target=NODE-Z agent=NODE-B`
 - `grant proxynode target=NODE-Z agent=NODE-C`
- Der Administrator definiert die Zeitpläne mithilfe der folgenden Befehle:
 - `define schedule standard proxy1 description="NODE-A proxy schedule" action=incremental options="-asnode=NODE-Z" objects=/Volumes/Xsan1 startdate=05/21/2005 starttime=01:00`

- define schedule standard proxy2 description="NODE-B proxy schedule" action=incremental options="-asnode=NODE-Z" objects=/Volumes/Xsan2 startdate=05/21/2005 starttime=01:00
- define schedule standard proxy3 description="NODE-C proxy schedule" action=incremental options="-asnode=NODE-Z" objects=/Volumes/Xsan3 startdate=05/21/2005 starttime=01:00

Anmerkung: Fügen Sie die Option `asnodename` nur in die Zeitplandefinition ein. Fügen Sie sie nicht in die Clientoptionsdatei, in die Befehlszeile oder an einer anderen Position ein.

Sie können auch den Clientakzeptordämon (**dsmcad**) verwenden, wenn `managedservices` in der Systemoptionsdatei auf **schedule** gesetzt ist.

Anmerkung:

- Jeder Zeitplan kann von einer anderen Workstation oder logischen Partition gestartet werden.
- Nachdem die Zeitpläne ausgeführt worden sind, kann jeder Proxy-Client alle gesicherten Daten abfragen und zurückschreiben.
- Eine Proxy-Operation verwendet die Einstellungen für den Zielknoten (beispielsweise **maxnummp** und **deduplication**) sowie Zeitpläne, die auf dem IBM Spectrum Protect-Server definiert sind. Die Einstellungen und Zeitpläne für den Agentenknoten auf dem IBM Spectrum Protect-Server werden ignoriert.

Zugehörige Verweise:

„Asnodename“ auf Seite 359

„Sitzungseinstellungen und Zeitpläne für eine Proxy-Operation“ auf Seite 360

 Befehl `DEFINE SCHEDULE`

Beispiele für die Planung einer Sicherung eines IBM PowerHA SystemMirror-Clusters

Dieser Abschnitt enthält einige Beispiele für das Sichern eines IBM PowerHA SystemMirror-Clusters.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um die Zeitplanung mehrerer Knoten zu aktivieren:

1. Stellen Sie sicher, dass alle Agentenknoten Proxy-Berechtigung über einen gemeinsamen Zielknoten haben
2. Stellen Sie sicher, dass alle Agentenknoten einen Zeitplan auf dem Server definiert haben:

```
def sched domain_name sched_name options='-asnode=target'
```
3. Stellen Sie sicher, dass jeder Agentenknoten seinen Zeitplan einem Knoten zugeordnet hat:

```
def association domain_name schedule_name <Name des Agentenknotens>
```

In den folgenden Beispielen ist IBM PowerHA SystemMirror für zwei AIX-Hosts konfiguriert, `host_a` und `host_b`. Neben ihren eigenen lokalen Daten nutzen die Hosts Plattenspeicher gemeinsam, der über zwei Dateibereiche verfügt: `/disk1` und `/disk2`.

Das Beispiel mit `CLUSTERNODE` zeigt, wie die Option `clusternode` in einer aktuellen IBM PowerHA SystemMirror-Umgebung verwendet wird.

- Der Administrator definiert 3 Knoten auf dem IBM Spectrum Protect-Server: host_a, host_b, cluster_group. Hierzu werden die folgenden Befehle verwendet: (1) REGISTER NODE host_a mysecretpa5s, (2) REGISTER NODE host_b mysecretpa5s, (3) REGISTER NODE cluster_group mysecretpa5s.
- Der Administrator definiert eine Datei dsm.opt auf host_a und host_b (beachten Sie, dass sich die opt-Dateien auf den Hosts unterscheiden). Dazu verwendet er die folgenden Befehle: (1) NODENAME host_a (Standardwert der Option kann verwendet werden), (2) DOMAIN /home /usr ... etc..
- Der Administrator definiert die Datei dsm.opt, die sich auf einer der Clusterplatzengruppen befindet, beispielsweise /disk1/tsm/dsm.opt. Dazu verwendet er die folgenden Befehle: (1) NODENAME cluster_group, (2) DOMAIN /disk1 /disk2, (3) CLUSTERNODE YES.
- Der Administrator definiert mit dem folgenden Befehl einen Zeitplan auf dem IBM Spectrum Protect-Server: DEFINE SCHEDULE STANDARD CLUSTER_BACKUP.
- Der Administrator definiert mit dem folgenden Befehl Zuordnungen für jeden der 3 Knoten: DEFINE ASSOC STANDARD CLUSTER_BACKUP host_a,host_b,cluster_group. Es werden jeweils drei Instanzen des Schedulers des Clients für Sichern/Archivieren ausgeführt. (Dabei ist der Scheduler für cluster_group Teil der Clusterressourcen, für die eine Übernahme erfolgt, wenn für die Plattenressourcen der Clustergruppe eine Übernahme erfolgt. Somit würde er entweder auf host_a oder auf host_b, aber nicht auf beiden gleichzeitig ausgeführt werden.)
- Alle drei Knotennamen enthalten Daten auf dem IBM Spectrum Protect-Server.

Das Beispiel mit ASNODE zeigt eine generische Lösung, die für nicht unterstützte UNIX-Clusterlösungen angewendet werden könnte, z. B. Veritas Cluster Server für Solaris.

- Der Administrator definiert 3 Knoten auf dem IBM Spectrum Protect-Server, host_a, host_b, cluster_group:
REGISTER NODE host_a mysecretpa5s
REGISTER NODE host_b mysecretpa5s
REGISTER NODE cluster_group mysecretpa5s
- Der Administrator definiert eine Proxy-Knotenbeziehung von host_a und host_b zu hacmp_cluster:
GRANT PROXYNODE TARGET=cluster_group AGENT=host_a,host_b
- Der Administrator definiert eine Datei dsm.opt auf host_a und host_b, um die lokalen Dateisysteme zu verarbeiten:
NODENAME host_a (Standardwert der Option kann verwendet werden)
DOMAIN /home /usr ... etc.
NODENAME host_b (Standardwert der Option kann verwendet werden)
DOMAIN /home /usr ... etc.
- Der Administrator definiert eine Datei dsm.opt auf der Clusterressource, um die Sicherung der Clusterressourcen zu verarbeiten, z. B. /disk1/tsm/dsmcluster.opt (der Knotenname ist der Standardknotenname, der entweder host_a oder host_b lautet, abhängig davon, welche Workstation zu dem jeweiligen Zeitpunkt die Clustergruppe enthält):
DOMAIN /disk1 /disk2
ASNODE cluster_group
- Der Administrator definiert einen Zeitplan auf dem IBM Spectrum Protect-Server:
DEFINE SCHEDULE STANDARD CLUSTER_BACKUP
- Der Administrator definiert Zuordnungen für alle 3 Knoten:
DEFINE ASSOC STANDARD CLUSTER_BACKUP host_a,host_b,cluster_group

- Es werden jeweils drei Instanzen des Schedulers des Clients für Sichern/ Archivieren ausgeführt. Dabei wird der Scheduler für den Knoten `hacmp_cluster` entweder auf `host_a` oder auf `host_b`, aber nicht auf beiden ausgeführt (er ist in den Clusterressourcen enthalten, für die eine Übernahme erfolgen würde). Dieser Scheduler würde auf die Datei `dsmcluster.opt` zeigen, die auf jedem Host definiert ist. Die drei Instanzen würden folgendermaßen gestartet werden:

```
[host_a]      dsmc sched
[host_b]      dsmc sched
[cluster_group] dsmc sched -optfile=/disk/tsm/dsmcluster.opt
```

- Alle drei Knotennamen enthalten Daten auf dem IBM Spectrum Protect-Server.

Weitere Informationen zu den Server-Schedulerbefehlen enthält die Dokumentation zum Server.

Sicherung eines GPFS-Dateisystems planen

Sie sichern ein GPFS-Dateisystem mithilfe des Schedulers und der Proxy-Beziehungen.

Informationen zu diesem Vorgang

Es wird vorausgesetzt, dass drei Knoten in einem GPFS-Cluster an der Sicherungsoperation beteiligt sind. Die Knoten `node_1`, `node_2` und `node_3` werden nur für die Authentifizierung verwendet. Die Objekte werden in Dateibereichen gesichert, die zum Knoten `node_gpfs` gehören.

Vorgehensweise

1. Definieren Sie vier Knoten auf dem IBM Spectrum Protect-Server.

```
REGISTER NODE node_1 mysecretpa5s
REGISTER NODE node_2 mysecretpa5s
REGISTER NODE node_3 mysecretpa5s
REGISTER NODE node_gpfs mysecretpa5s
```
2. Definieren Sie eine Proxy-Beziehung zwischen den Knoten.

```
GRANT PROXYNODE TARGET=node_gpfs AGENT=node_1, node_2, node_3
```
3. Definieren Sie einen Zeitplan.

```
DEFINE SCHEDULE STANDARD GPFS_SCHEDULE ACTION=incremental
OBJECTS="/gpfs"
DEFINE ASSOCIATION STANDARD GPFS_SCHEDULE node_gpfs
```
4. Wählen Sie eines der GPFS-Systeme für die Ausführung des Zeitplans aus. Geben Sie die Optionen **nodename** und **asnodename** in der Optionsdatei `dsm.sys` auf allen Systemen in dem GPFS-Cluster an. Der Wert für die Option **asnodename** muss auf allen Systemen identisch sein.

Definitionen in der Optionsdatei `dsm.sys` auf node 1:

```
nodename node_1
asnodename node_gpfs
```

Definitionen in der Optionsdatei `dsm.sys` auf node 2:

```
nodename node_2
asnodename node_gpfs
```




Definitionen in der Optionsdatei `dsm.sys` auf node 3:

```
nodename node_3
asnodename node_gpfs
```

5. Starten Sie den Scheduler auf dem System, das für die Ausführung des Zeitplans ausgewählt wurde.

```
DSMC SCHED
```

Zugehörige Informationen:

-  Befehl 'mmbackup': IBM Spectrum Protect-Voraussetzungen
-  Anleitung für die Integration von IBM Spectrum Scale AFM mit IBM Spectrum Protect
-  Hinweise zur Verwendung der Einschluss- und Ausschlussoptionen von IBM Spectrum Protect in Verbindung mit dem IBM Spectrum Scale-Befehl 'mmbackup'

Lokale Momentaufnahme einem Serverdateibereich zuordnen (UNIX und Linux)

Verwenden Sie die Option `snapshotroot` in den Befehlen **incremental** und **selective** in Verbindung mit einer Anwendung eines anderen Herstellers zur Erstellung einer Momentaufnahme eines logischen Datenträgers, um die Daten in der lokalen Momentaufnahme den realen Dateibereichsdaten zuzuordnen, die auf dem IBM Spectrum Protect-Server gespeichert sind.

Die Option `snapshotroot` bietet keine Funktionen zur Erstellung einer Datenträgermomentaufnahme, sondern ausschließlich Funktionen zur Verwaltung von Daten, die durch Erstellen einer Datenträgermomentaufnahme generiert werden.

Zugehörige Verweise:

„Snapshotroot“ auf Seite 593

Imagesicherung

Von Ihrer lokalen Workstation aus können Sie einen logischen Datenträger als einzelnes Objekt auf Ihrem System sichern (Imagesicherung).

Die traditionelle statische Imagesicherung verhindert während der Operation den Schreibzugriff auf den Datenträger durch andere Systemanwendungen.

Sie müssen Root sein, um diese Task auszuführen, und die Imagesicherung gilt nicht für Mac OS X.

Eine Imagesicherung bietet die folgenden Vorteile:

- Schnellere Sicherung von Dateisystemen, die eine große Anzahl Dateien enthalten, im Vergleich zu einer Teilsicherung des gesamten Dateisystems.
- Verbesserung der Geschwindigkeit, mit der der Client Dateisysteme zurückschreibt, die viele kleine Dateien enthalten.
- Ressourceneinsparung auf dem Server während der Sicherung, da für ein Image nur ein Eintrag erforderlich ist.
- Bereitstellung eines Bildes Ihres logischen Datenträgers zu einem bestimmten Zeitpunkt, das im Bedarfsfall abgerufen werden kann.
- Zurückschreibung eines beschädigten Dateisystems oder unformatierten logischen Datenträgers. Nach dem Zurückschreiben haben die Daten denselben Status wie bei der letzten Sicherung des logischen Datenträgers.

Die traditionelle statische Imagesicherung verhindert während der Operation den Schreibzugriff auf den Datenträger durch andere Systemanwendungen. Verwenden Sie die Option `dynamicimage`, um den Datenträger im aktuellen Status ohne erneutes Anhängen mit Lesezugriff zu sichern. Die Sicherung kann beschädigt werden, wenn Anwendungen auch während der Ausführung der Sicherung weiter auf den Datenträger schreiben. Wird während der Ausführung einer Imagesicherung auf ei-

nen Datenträger geschrieben, kann es nach einer Zurückschreibungsoperation zu Dateninkonsistenzen und Datenverlust kommen. Die Option `dynamicimage` überschreibt den Kopiennummerierungswert in der Verwaltungsklasse bei der Durchführung von Imagesicherungen. Führen Sie nach dem Zurückschreiben einer Imagesicherung, die mit der Option `dynamicimage` erfolgt ist, immer das Dienstprogramm `chkdsk` aus.

Um eine Imagesicherung eines Datenträgers zurückschreiben zu können, muss der Client für Sichern/Archivieren eine exklusive Sperre des Datenträgers erlangen können, der gerade zurückgeschrieben wird.

Einschränkung: Verwenden Sie dynamische Imagesicherungen nicht für Dateisysteme, da das Dateisystem möglicherweise selbst dann inkonsistente Daten bereitstellt, wenn keine Schreibaktivität stattfindet. Die dynamische Imagesicherung kann außerdem zu einem nicht exakten Image führen, das bei der Zurückschreibung möglicherweise ungültig oder unvollständig ist.

Wenn der Client für Sichern/Archivieren das Dateisystem nach dem Zurückschreiben eines Image nicht anhängen kann, führen Sie `fsck` aus. Das Ausführen von `fsck` kann sich jedoch auf die Integrität großer Datenvolumen auswirken. Verwenden Sie die dynamische Imagesicherung nicht für JFS2-Dateisysteme unter AIX. Der Client lässt dynamische Imagesicherungen für JFS2-Dateisysteme unter AIX nicht zu. Wenn Sie `dynamicimage=yes` für ein JFS2-Dateisystem angeben, führt der Client eine momentaufnahmebasierte Imagesicherung aus. Wenn die Momentaufnahme aus irgendeinem Grund nicht erstellt werden kann, führt der Client stattdessen eine statische Imagesicherung aus.

Achtung: Um Datenverluste zu verhindern, sollten Sie die Verwendung der Option `dynamicimage` vermeiden und sicherstellen, dass keine Schreibaktivität auf dem Datenträger stattfindet, während die Sicherung ausgeführt wird.

Für AIX JFS2-Dateisysteme wird das Datenvolumen reduziert, das bei einer statischen Imagesicherung oder einer Momentaufnahmeimagesicherung auf dem IBM Spectrum Protect-Server gesichert wird, indem nur diejenigen Blöcke gesichert werden, die vom Dateisystem verwendet werden oder kleiner als der Wert der Option `imagegapsize` sind. Diese Methode der Datensicherung verbessert die Leistung der Imagesicherung. Weitere Informationen siehe „Imagegapsize“ auf Seite 469.

Nur für AIX-Clients: Standardmäßig führt der Client eine Onlinemomentaufnahmeimagesicherung der JFS2-Dateisysteme aus, während der der Datenträger für andere Systemanwendungen verfügbar ist.

Nur für Linux-Clients: Standardmäßig führt der Client eine Momentaufnahmeimagesicherung der Dateisysteme auf einem logischen Datenträger aus, der von Linux Logical Volume Manager erstellt wurde. Der Datenträger steht anderen Systemanwendungen zur Verfügung, während die Momentaufnahmeimagesicherung ausgeführt wird.

Für Linux-Clients: Die Imagesicherung von DASD-Einheiten mit dem Modus `'raw_track_access'` unter Linux on z Systems wird nicht unterstützt.

Die Imagesicherungsoperation wird auf Partitionen, die sich auf einer Multipath-Einheit befinden, nicht unterstützt.

Achtung: Von IBM Spectrum Protect for Space Management verwaltete Dateisysteme sind nicht für die Imagesicherung aktiviert.

Zugehörige Tasks:

„Momentaufnahmebasierte Dateisicherung und -archivierung und momentaufnahmebasierte Imagesicherung“ auf Seite 215

Vorausgesetzte Tasks vor der Erstellung einer Imagesicherung ausführen

In diesem Abschnitt sind einige Punkte aufgelistet, die zu berücksichtigen sind, bevor Sie eine Imagesicherung ausführen.

Informationen zu diesem Vorgang

Die folgenden Hinweise sind für Imagesicherungen zu beachten.

- Stellen Sie sicher, dass keine andere Anwendung den Datenträger verwendet, wenn Sie eine statische Imagesicherung ausführen. Um während der Sicherungsverarbeitung ein konsistentes Image sicherzustellen, hängt der Client den Datenträger ab und schreibgeschützt wieder an, sodass keine andere Anwendung auf den Datenträger schreiben kann, wenn ein Dateibereich auf dem Datenträger festgestellt wird. Ist der Datenträger im Gebrauch, wenn der Client versucht, ihn abzuhängen, schlägt die Sicherung fehl. Wenn der Client den Datenträger nicht abhängen und schreibgeschützt wieder anhängen kann, da dieser in Gebrauch ist, und keine Momentaufnahmeimagesicherung verfügbar ist, können Sie die Option `dynamicimage` verwenden. Damit können Sie den Client zwingen, eine Imagesicherung auszuführen, ohne den Datenträger abzuhängen und im schreibgeschützten Modus wieder anzuhängen. Setzen Sie in einer Anweisung `include.image` oder in der Befehlszeile die Option `dynamicimage`. Die Sicherung kann beschädigt werden, wenn Anwendungen auf den Datenträger schreiben, während die Sicherung gerade ausgeführt wird. Dieses Problem kann durch Ausführen von `fsck` nach dem Zurückschreiben behoben werden, um eventuell beschädigte Blöcke zu reparieren.

Wenn auf dem zu sichernden Datenträger kein Dateisystem erkannt wird, stellen Sie sicher, dass alle Anwendungen, die auf die Datenträger schreiben, stillgelegt werden. Der Client für Sichern/Archivieren verwendet die Dateisystemtabelle und die Ladetabelle, um die unterstützten Dateisysteme zu ermitteln.

Schließen Sie *keine* Systemdateien in eine Imagesicherung ein, da aktiv verwendete Dateisysteme nicht abgehängt werden können.

Nur für AIX und Linux: Wenn Sie eine Imagesicherung eines angehängten Dateisystems ausführen, das an einen anderen Mountpunkt angehängt und in der Dateisystemtabelle angegeben ist, gehen nach Durchführung der Imagesicherung alle Mountoptionen für dieses Dateisystem außer dem Lese- oder Schreibstatus verloren.

Wichtig: Verfügt ein angehängtes Dateisystem über verschachtelte Mountpunkte, müssen diese vor dem Versuch einer Sicherung abgehängt werden. Andernfalls kann der Client die Bereitstellung des Datenträgers nicht aufheben. Das Dateisystem wird als *aktiv* angesehen, wenn es angehängt ist.

- Verwenden Sie die Option `include.image`, um dem Datenträgerimage eine Verwaltungsklasse zuzuordnen. Wenn Sie keine Verwaltungsklasse zuordnen, wird die Standardverwaltungsklasse für das Image verwendet.
- Über die Option `exclude.image` können Sie einen Datenträger von der Imagesicherung ausschließen.
- Sie müssen den Mountpunkt für den Dateisystemdatenträger verwenden, für den eine Imagesicherung ausgeführt werden soll. Der Client sichert keinen Dateisystemdatenträger ohne die Verwendung eines Mountpunkts. Sichern Sie Dateisysteme mithilfe des Mountnamens. Beispiel: Ist `/dev/lv01` als Dateisystem

formatiert, das an /home angehängt ist, geben Sie den folgenden Befehl ein, um eine Imagesicherung dieses Datenträgers auszuführen:

```
dsmc backup image /home
```

Sichern Sie unformatierte Datenträger mithilfe des Einheitennamens. Beispiel: Wenn /dev/lv02 ein unformatierter Datenträger ist, geben Sie den folgenden Befehl ein, um eine Imagesicherung dieses Datenträgers durchzuführen:

```
dsmc backup image /dev/lv02
```

Wenn Sie einen unformatierten Datenträger sichern, der als Dateisystem formatiert ist, stellen Sie sicher, dass das Dateisystem nicht angehängt ist und keinen Eintrag in /etc/filesystems hat.

Zugehörige Konzepte:

Kapitel 9, „Speicherverwaltungsmaßnahmen“, auf Seite 309

Zugehörige Verweise:

„Exclude-Optionen“ auf Seite 438

„Include-Optionen“ auf Seite 473

Unterstützung für eine Imagesicherung nach Einheitentyp des Datenträgers

In diesem Abschnitt sind einige Einheiten aufgelistet, die vom Befehl **backup image** unterstützt werden.

Die folgende Tabelle enthält eine Liste der Einheiten, die vom Befehl **backup image** unterstützt werden. Bei einer unformatierten Einheit kann es sich um einen Plattensektor, eine Partition oder einen logischen Datenträger handeln.

Tabelle 37. Unterstützung für eine Imagesicherung nach Einheitentyp des Datenträgers

Verwaltungsprogramm des logischen Datenträgers	Typ der unformatierten Einheiten	Beispieleinheitenname	Unterstützung für Befehl backup image
AIX Logical Volume Mgr	Logische Datenträger	/dev/lv00	AIX
Sun Solstice DiskSuite Volume Manager	Metaeinheiten	/dev/md/dsk/dl	Solaris
Solaris Volume Manager	Metaeinheiten	/dev/md/dsk/dl	Solaris
Veritas Volume Mgr	Logische Datenträger	/dev/vx/dsk/rootdg/vol01 - AIX /dev/vg00/lvol01 - Solaris	Solaris AIX
Unformatierte Platten	Partitionen	/dev/hda1, /dev/sda3	Linux x86_64, Linux on POWER
Unformatierte Platten	Platteneinheiten	/dev/sda /dev/mapper/mpathX	Linux x86_64
Unformatierte Platten	Partitionen	/dev/dasdx	Linux on System z
Linux Logical Volume Mgr	Logische Datenträger	/dev/myvolgroup/ myvolume	Alle Linux
Unformatierte Platten	Plattensektoren	/dev/dsk/c0tld0s0	Solaris

Bei Roheinheiten sichert der Client für Sichern/Archivieren den Datenträger unverändert. Das heißt, es werden keine Momentaufnahmen erstellt und Anwendungen können weiter auf den Datenträger schreiben, während er gesichert wird. IBM Spectrum Protect kann die Konsistenz der Daten bei einer Sicherung auf der Ebene

physischer Platten nicht garantieren. Eine Beschädigung kann auftreten, wenn sich die Daten auf dem Datenträger ändern, während die Sicherung gerade ausgeführt wird.

Der Client muss den unformatierten Einheitentyp auf der spezifischen Plattform unterstützen, damit eine Imagesicherung einer unformatierten Einheit ausgeführt werden kann. Wenn Sie eine Imagesicherung für ein Dateisystem ausführen wollen, das auf einer unformatierten Einheit geladen ist, muss die unformatierte Einheit unterstützt werden. Unformatierte Einheiten müssen mit dem dazugehörigen Blockeinheitenamen angegeben werden.

Für die Linux-Clients: Imagesicherung wird nur auf Partitionen mit der ID 0x83 oder auf logischen Datenträgern unterstützt, die mit dem Linux Logical Volume Manager erstellt wurden. Beim Sichern anderer Partitionen, wie z. B. bei erweiterten Partitionen, die angehängte Dateisysteme oder Datenbankdaten enthalten, kann es zu inkonsistenten Sicherungsdaten kommen, wenn sich die Daten während der Imagesicherungsoperation ändern.

Für AIX und Solaris: Sie können Imageoperationen für Datenträger ausführen, die mit Veritas Volume Manager erstellt wurden. Der Client unterstützt anfänglich bei der Sicherung den Imagetyp 'Statisch' (Standardwert) und 'Dynamisch'.

Bei Solaris 10-Clients können Sie die Imagesicherung nur für Dateisysteme verwenden, die von der globalen Zone der nicht globalen Zone zugeordnet werden, indem die Einheit unter Angabe von 'add device' und 'set match' exportiert wird. Verwenden Sie die Imagesicherung nicht für andere Dateisysteme in nicht globalen Zonen, weil die nicht globale Zone keine Berechtigung zum Anhängen oder Abhängen des Dateisystems hat. Verwenden Sie bei Solaris 10-Clients außerdem nicht die die Überlappungseinheit der Rootplatte (c0t0d0s2) für eine Roheinheitensicherung. Vermeiden Sie die Verwendung dieses Features auf Platten oder Sektoren, die als Auslagerungseinheiten verwendet werden.

Von Veritas Volume Manager erstellte Metaeinheiten müssen einschließlich der Datenträgergruppe in /etc/vfstab aufgelistet werden, damit der Client für Sichern/Archivieren sie für eine Imagesicherung von Dateisystemen erkennt. Die Dateisysteme sollten abgehängt werden. Roheinheiten sollten nicht in /etc/vfstab aufgelistet werden. Der folgende Name ist z. B. der korrekte Metaeinheitenname, der in der Datei /etc/vfstab verwendet werden sollte:

```
/dev/vx/dsk/<Datenträgergruppe>/<Metaeinheitenname>
```

Die Angabe /dev/vx/dsk/ würde nicht richtig erkannt, und Sie würden einen Fehler empfangen (ANS1134E).

Plattensektoren, die Zylinder 0 enthalten, sollten nicht gesichert oder zurückschrieben werden. In diesem Fall wird das Datenträgerinhaltsverzeichnis (VTOC) überschrieben. Wenn Sie den ersten Plattensektor sichern müssen, schließen Sie Zylinder 0 aus, indem Sie den Plattensektor von Zylinder 1 starten (verwenden Sie das Dienstprogramm Formatieren). Der Client für Sichern/Archivieren überprüft nicht, ob Zylinder 0 in der Einheit enthalten ist, die bei einer Zurückschreibung überschrieben wird.

Verwendung von Imagesicherungen für die Ausführung von Dateisystemteilsicherungen

In diesem Abschnitt sind die Methoden und Schritte zum Ausführen effizienter Teilsicherungen Ihres Dateisystems mithilfe von Imagesicherungen aufgelistet.

Mithilfe dieser Sicherungsmethoden können Sie eine zeitpunktgesteuerte Zurückschreibung für Ihre Dateisysteme ausführen und den Durchsatz beim Sichern und Zurückschreiben verbessern. Sie können die Sicherung nur auf formatierten Datenträgern und nicht auf unformatierten logischen Datenträgern ausführen.

Verwenden Sie eine der folgenden Methoden, um Imagesicherungen für Datenträger mit angehängten Dateisystemen auszuführen.

Methode 1: Imagesicherungen mit Teilsicherungen des Dateisystems verwenden

In diesem Abschnitt sind die Schritte aufgelistet, die Sie durchführen müssen, um Imagesicherungen mit Teilsicherungen des Dateisystems auszuführen.

Informationen zu diesem Vorgang

Vorgehensweise

1. Führen Sie eine vollständige Teilsicherung des Dateisystems aus. Dies ist die Basis für die späteren Teilsicherungen.
2. Führen Sie eine Imagesicherung desselben Dateisystems aus, damit Imagezurückschreibungen möglich sind.
3. Führen Sie in regelmäßigen Abständen Teilsicherungen des Dateisystems aus, damit alle hinzugefügten und gelöschten Dateien auf dem Server aufgezeichnet werden.
4. Führen Sie in regelmäßigen Abständen eine Imagesicherung aus, um die Zurückschreibungszeit zu verkürzen.
5. Schreiben Sie Ihre Daten über eine Teilzurückschreibung zurück. Stellen Sie sicher, dass Sie **Image plus Teilsicherung von Verzeichnissen und Dateien** und **Inaktive Dateien von Lokal löschen** im Fenster für Zurückschreibungsoptionen ausgewählt haben, bevor Sie die Zurückschreibung starten. Während der Zurückschreibung führt der Client Folgendes durch:

Ergebnisse

- Er schreibt das neueste Image auf dem Server zurück.
- Er löscht alle im vorherigen Schritt zurückgeschriebenen Dateien, die auf dem Server inaktiv sind. Dies sind Dateien, die zum Zeitpunkt der Imagesicherung vorhanden waren, aber danach gelöscht und durch eine spätere Teilsicherung aufgezeichnet wurden.
- Er schreibt neue und geänderte Dateien aus den Teilsicherungen zurück.

Anmerkung: Wenn eine Teilsicherung nach der Sicherung eines Image mehrmals ausgeführt wird, müssen Sie sicherstellen, dass die Sicherungskopiengruppe des IBM Spectrum Protect-Servers über genügend Versionen für vorhandene und gelöschte Dateien auf dem Server verfügt, damit das nachfolgende Zurückschreibungsimage mit den Optionen `incremental` und `deletefiles` die Dateien ordnungsgemäß löschen kann.

Zugehörige Tasks:

„Daten über die Java-GUI sichern“ auf Seite 193

„Imagesicherung über die GUI ausführen“ auf Seite 213

„Image über die GUI zurückschreiben“ auf Seite 249

Methode 2: Imagesicherungen mit Imageteilsicherungen nach Datum verwenden

In diesem Abschnitt sind die Schritte aufgelistet, die Sie durchführen müssen, um Imagesicherungen mit Imageteilsicherungen nach Datum auszuführen.

Vorgehensweise

1. Führen Sie eine Imagesicherung des Dateisystems aus.
2. Führen Sie eine Imageteilsicherung nach Datum für das Dateisystem aus. Hierdurch werden nur die Dateien an den Server gesendet, die seit der letzten Imagesicherung hinzugefügt oder geändert wurden.
3. Führen Sie in regelmäßigen Abständen vollständige Imagesicherungen aus.
4. Schreiben Sie Ihren Datenträger über eine Teilzurückschreibung zurück. Stellen Sie sicher, dass Sie die Option **Image plus Teilsicherung von Verzeichnissen und Dateien** im Fenster für Zurückschreibungsoptionen ausgewählt haben, bevor Sie die Zurückschreibung starten. Damit werden zunächst das neueste Image und anschließend alle Teilsicherungen seit diesem Datum zurückgeschrieben.

Ergebnisse

Anmerkung: In den folgenden Fällen sollten Sie regelmäßige vollständige Imagesicherungen ausführen:

- Wenn der Änderungsumfang des Dateisystems hoch ist (mehr als 40 %), wie in Schritt 4 bei Methode 1 und Schritt 3 bei Methode 2 angegeben. Beim Zurückschreiben erhalten Sie auf diese Weise ein Dateisystemimage, das dem Image bei der letzten Teilsicherung nach Datum ähnlich ist; außerdem wird die Zurückschreibungsdauer verkürzt.
- Entsprechend den Anforderungen in Ihrer Umgebung.

Dadurch wird die Zurückschreibungszeit verbessert, da weniger Änderungen von Teilsicherungen angewendet werden.

Bei Verwendung von Methode 2 gelten folgende Einschränkungen:

- Das Dateisystem darf keine früheren vollständigen Teilsicherungen aufweisen.
- Durch eine Imageteilsicherung nach Datum werden Dateien auf dem Server nicht inaktiviert; demzufolge sind, wenn Sie ein Image mit der Option `incremental` zurückschreiben, Dateien vorhanden, die nach der ursprünglichen Imagesicherung gelöscht wurden.
- Bei der ersten Imagesicherung des Dateisystems wird eine vollständige Imagesicherung ausgeführt.
- Wenn die maximale Kapazität der Dateisysteme bereits oder fast erreicht ist, kann hierdurch eine Bedingung 'Zu wenig Speicherbereich' während der Zurückschreibung auftreten.

Zugehörige Tasks:

„Imagesicherung über die GUI ausführen“ auf Seite 213

„Image über die GUI zurückschreiben“ auf Seite 249

Vergleich der Methoden 1 und 2

Dieser Abschnitt enthält einen Vergleich der Methoden 1 und 2: (1) Imagesicherung mit Teilsicherungen des Dateisystems verwenden oder (2) Imagesicherung mit Imageteilsicherung nach Datum verwenden.

Als Hilfe bei der Entscheidung, welche Methode für Ihre Umgebung geeignet ist, enthält die folgende Tabelle einen Vergleich der Methoden 1 und 2.

Tabelle 38. Vergleich der Methoden zur Imageteilsicherung

Methode 1: Imagesicherung mit Teilsicherungen des Dateisystems verwenden	Methode 2: Imagesicherung mit Imageteilsicherung nach Datum verwenden
Dateien werden auf dem Server als verfallen gekennzeichnet, wenn sie aus dem Dateisystem gelöscht werden. Beim Zurückschreiben haben Sie die Möglichkeit, die auf dem Server verfallenen Dateien aus dem Image zu löschen.	Dateien werden auf dem Server nicht als verfallen gekennzeichnet. Nach der Imageteilzurückschreibung sind alle Dateien, die nach der Imagesicherung aus dem Dateisystem gelöscht wurden, wieder vorhanden. Wenn die maximale Kapazität der Dateisysteme bereits oder fast erreicht ist, kann hierdurch eine Bedingung 'Zu wenig Speicherbereich' auftreten.
Die für Teilsicherungen erforderliche Zeit entspricht der Zeit, die für normale Teilsicherungen erforderlich ist.	Die für Imageteilsicherungen erforderliche Zeit ist kürzer, da der Client nicht jede zu kopierende Datei beim Server abfragen muss.
Die Zurückschreibung erfolgt wesentlich schneller im Vergleich zu einer vollständigen Teilzurückschreibung des Dateisystems.	Die Zurückschreibung erfolgt wesentlich schneller im Vergleich zu einer vollständigen Teilzurückschreibung des Dateisystems.
Verzeichnisse, die nach der letzten Imagesicherung aus dem Dateisystem gelöscht wurden, sind nicht als verfallen gekennzeichnet.	Verzeichnisse und Dateien, die nach der letzten Imagegesamtsicherung aus dem Dateisystem gelöscht wurden, sind nicht als verfallen gekennzeichnet.

Imagesicherung über die GUI ausführen

Wenn die Imagesicherungsfunktion konfiguriert ist, können Sie eine Imagesicherung erstellen, während der der reale Datenträger für andere Systemanwendungen verfügbar ist.

Informationen zu diesem Vorgang

Während der Imagesicherung wird ein konsistentes Image des Datenträgers aufrechterhalten.

Wenn Sie eine Imagesicherung mit der Option `image backup` der GUI des Clients für Sichern/Archivieren ausführen, wird die Sicherungsoperation gemäß der Einstellung für die Option `snapshotproviderimage` ausgeführt. Der Standardwert für die Option `snapshotproviderimage` ist eine AIX JFS2-Momentaufnahme für AIX und eine Linux LVM-Momentaufnahme für Linux. Sie können den Standardwert auf der Registerkarte 'Momentaufnahme' unter den Vorgaben für Momentaufnahmeimage im Profileditor überschreiben.

Für Solaris-Clients: Bei Auswahl der Option `image backup` wird standardmäßig eine statische Imagesicherung ausgeführt. Bei der statischen Imagesicherung hängt der Client den Datenträger ab und schreibgeschützt wieder an, damit keine anderen Anwendungen auf ihn zugreifen können. Sie können den Standardwert überschreiben, indem Sie die Option `include.image` verwenden und `dynamicimage yes` auswählen. Bei der dynamischen Imagesicherung führt der Client die Imagesicherung aus, ohne das Dateisystem während der Sicherung schreibgeschützt zu machen.

Zur Erstellung einer Imagesicherung des Dateisystems oder des unformatierten logischen Datenträgers sind folgende Schritte auszuführen:

Vorgehensweise

1. Klicken Sie auf die Schaltfläche **Sichern** im IBM Spectrum Protect-Hauptfenster. Das Fenster 'Sichern' wird angezeigt.
2. Erweitern Sie die Verzeichnisstruktur und wählen Sie die zu sichernden Objekte aus. Zum Sichern eines unformatierten logischen Datenträgers das Objekt RAW in der Verzeichnisstruktur suchen und erweitern.
3. Klicken Sie auf **Sichern**. Im Fenster **Task-Liste** für die Sicherung wird der Verarbeitungsstatus der Sicherung angezeigt. Das Fenster 'Sicherungsbericht' zeigt einen ausführlichen Statusbericht an.

Ergebnisse

- Zum Ausführen einer statischen Imagesicherung wählen Sie **Imagesicherung** in der Dropdown-Liste aus.
- *Nur für AIX- und Linux-Clients:* Zum Ausführen einer Momentaufnahmeimagesicherung verwenden Sie die Option snapshotproviderimage.
- Zum Ausführen einer Imageteilsicherung nach Datum wählen Sie **Imageteilsicherung (nur Datum)** in der Dropdown-Liste aus.

Die folgenden Hinweise sind zu beachten, wenn Sie eine momentaufnahmebasierte Imagesicherung ausführen:

- Um bestimmte Sicherungsoptionen zu ändern, klicken Sie auf die Schaltfläche **Optionen**. Die ausgewählten Optionen sind nur während der aktuellen Sitzung wirksam.
- Um bestimmte Sicherungsoptionen zu ändern, klicken Sie auf die Schaltfläche **Optionen**. Die ausgewählten Optionen sind nur während der aktuellen Sitzung wirksam.

Nur für Linux: Der IBM Spectrum Protect-Client der Version 5.4 (und höher) erkennt keine LVM1-Datenträger für Imageoperationen. Er lässt jedoch zu, dass vorherige Imagesicherungen von LVM1-Datenträgern auf LVM2-Datenträger zurückgeschrieben werden. Tabelle 39 zeigt die Kombinationen, die die alten und neuen Versionen des Clients einbeziehen, die die LVM1- und LVM2-Datenträger für verschiedene Imageoperationen handhaben.

Tabelle 39. Vergleiche der LVM1- und LVM2-Imageoperationen

IBM Spectrum Protect-Clientversion	LVM1-Sicherung und -Zurückschreibung	LVM2-Sicherung und -Zurückschreibung	Gemischte Datenträger	
			Sicherung: LVM1, Zurückschreibung: LVM2	Sicherung: LVM2, Zurückschreibung: LVM1
V5.3 und früher	YES	Nur statisches Image für Dateisystem	NO	NEIN - unformatierte Datenträger werden nicht unterstützt
V5.4 und später	NEIN Fehlernachricht ANS1090E wird angezeigt	YES	JA Datenträger LVM1 muss einem früheren Client gesichert worden sein	NEIN Zurückschreibung auf Datenträger LVM1 schlägt fehl

Zugehörige Verweise:

„Snapshotproviderimage“ auf Seite 592

Imagesicherung über die Befehlszeile ausführen

Imagesicherungs- und -zurückschreibungsoperationen für einen einzelnen Datenträger werden mit dem Befehl **backup image** bzw. **restore image** ausgeführt.

Verwenden Sie die Option **mode** im Befehl **backup image**, um eine Imageteilsicherung nach Datum auszuführen, bei der nur die seit der letzten vollständigen Imagesicherung neu erstellten oder geänderten Dateien gesichert werden. Bei dieser Prozedur werden jedoch nur Dateien mit einem geänderten Datum gesichert, aber keine Dateien mit geänderten Berechtigungen.

Zugehörige Verweise:

„Backup Image“ auf Seite 702

„Mode“ auf Seite 509

„Restore Image“ auf Seite 786

Momentaufnahmebasierte Dateisicherung und -archivierung und momentaufnahmebasierte Imagesicherung

Für Clients für Sichern/Archivieren, die als Rootbenutzer auf JFS2-Dateisystemen unter AIX 5.3 oder höher ausgeführt werden, werden standardmäßig momentaufnahmebasierte Imagesicherungen mithilfe von Momentaufnahmen erstellt.

Informationen zu diesem Vorgang

Wahlweise können Sie momentaufnahmebasierte Sicherungs- und Archivierungsoperationen auf Dateiebene aktivieren, indem Sie die Option **snapshotproviderfs** angeben. Falls aus irgendeinem Grund keine Momentaufnahme erstellt werden kann, versucht der Client, eine statische Imagesicherung oder eine normale Dateisicherung auszuführen.

Um eine momentaufnahmebasierte Dateisicherung und -archivierung anzugeben, setzen Sie die Option **snapshotproviderfs** auf JFS2. Dies ist auf alle JFS2-Dateisysteme für diesen Client anwendbar.

Wichtig: Verwenden Sie die momentaufnahmebasierte Dateisicherung und -archivierung und die momentaufnahmebasierte Imagesicherung für alle Ihre JFS2-Dateisysteme unter AIX.

Beispiel: Geben Sie Folgendes in die Serverzeilengruppe in der Datei **dsm.sys** ein, um die momentaufnahmebasierte Dateisicherung und -archivierung für alle JFS2-Dateisysteme auf dem Client *einzuschalten*:

```
snapshotproviderfs JFS2
```

Geben Sie Folgendes in die Serverzeilengruppe in der Datei **dsm.sys** ein, um die momentaufnahmebasierte Dateisicherung und -archivierung für alle JFS2-Dateisysteme auf dem Client explizit *auszuschalten*:

```
snapshotproviderfs NONE
```

Geben Sie Folgendes in die Serverzeilengruppe in der Datei **dsm.sys** ein, um die momentaufnahmebasierte Dateisicherung und -archivierung für ein bestimmtes JFS2-Dateisystem auf dem Client *einzuschalten*:

```
snapshotproviderfs NONE
```

```
include.fs /kalafs1 snapshotproviderfs=JFS2
```

Geben Sie Folgendes in die Serverzeilengruppe in der Datei dsm.sys ein, um die momentaufnahmebasierte Dateisicherung und -archivierung für ein bestimmtes JFS2-Dateisystem auf dem Client *auszuschalten*:

```
snapshotproviderfs    JFS2  
  
include.fs    /kalafs2    snapshotproviderfs=NONE
```

Geben Sie Folgendes in der Befehlszeile ein, um die momentaufnahmebasierte Dateisicherung und -archivierung nur für eine bestimmte Operation auf dem Client *einzuschalten*:

```
dsmc incr    -snapshotproviderfs=JFS2    /kalafs1
```

Geben Sie Folgendes in der Befehlszeile ein, um die momentaufnahmebasierte Dateisicherung und -archivierung nur für eine bestimmte Operation auf dem Client *auszuschalten*:

```
snapshotproviderfs    JFS2
```

Führen Sie dann den Sicherungsbefehl aus. Zum Beispiel:

```
dsmc incr -snapshotproviderfs=NONE /kalafs2
```

Zugehörige Verweise:

„Snapshotproviderfs“ auf Seite 591

Btrfs-Dateisysteme schützen

Btrfs-Dateisysteme können als Dateispezifikationen für Sicherungs- und Zurückschreibungsbefehle, Archivierungs- und Abrufbefehle und in den Befehlen **backup image** und **restore image** angegeben werden. Außerdem können Sie Btrfs-Unterdatenträger als Dateispezifikation in den Sicherungs- und Zurückschreibungsfunktionen und in den Archivierungs- und Abruffunktionen angeben. Die Imagesicherungs- oder Imagezurückschreibungsbefehle des Clients für Sichern/Archivieren können Sie für einen Btrfs-Unterdatenträger nicht verwenden.

Btrfs-Dateisysteme werden unter SLES 11 SP2 oder höher, unter IBMSystem x, System p und System z unterstützt.

Wenn Sie eine statische Imagesicherung des gesamten Btrfs-Dateisystems erstellen wollen, müssen Sie alle Unterdatenträger abhängen, damit der Client für Sichern/Archivieren das Btrfs-Dateisystem während des Sicherungsprozesses ab- oder anhängen kann. Sie können die Anforderungen für das An- und Abhängen vermeiden, wenn Sie anstelle einer statischen Imagesicherung eine momentaufnahmebasierte Imagesicherung des Btrfs-Dateisystems ausführen.

Die Imagesicherungs- und Imagezurückschreibungsfunktionalität steht für Btrfs-Unterdatenträger nicht zur Verfügung. Wenn Sie versuchen, einen Unterdatenträger mit dem Befehl **image backup** zu sichern, wird die folgende Nachricht angezeigt:

```
ANS1162E Dateisystem konnte nicht angehängt werden
```

Sie können einen Btrfs-Unterdatenträger entweder mithilfe des Unterdatenträgernamens oder der Unterdatenträger-ID anhängen.

Auf Btrfs-Dateisystemen kann die Journalsicherung sowohl auf Dateisystemebene als auch auf Unterdatenträgerebene ausgeführt werden. Wenn Sie die journalbasierte Sicherung für ein Btrfs-Dateisystem ausführen, gilt das erstellte Journal für das gesamte Dateisystem; es gibt kein separates Journal für jeden Unterdatenträger.

Einschränkung: Auf Linux-Systemen verwenden einige Dateisysteme (z. B. ext2, ext3, ext4, btrfs und xfs) eine UUID (Universally Unique Identifier), um sich selbst im Betriebssystem zu identifizieren. Wenn Sie eine Imagesicherung eines solchen Datenträgers erstellen und an eine andere Position zurückschreiben, kann es sein, dass es zwei Datenträger mit derselben UUID gibt. Wenn Sie Ihre Dateisysteme mit einer UUID in /etc/fstab definieren, denken Sie daran, dass der Client für Sichern/Archivieren das zurückgeschriebene Dateisystem unter Umständen wegen eines UUID-Konflikts nicht korrekt anhängen kann. Um diese Situation zu vermeiden, sollten Sie das Image an seine ursprüngliche Position zurückschreiben. Wenn Sie es an eine andere Position zurückschreiben müssen, ändern Sie die UUID des ursprünglichen oder des zurückgeschriebenen Datenträgers, bevor Sie das zurückgeschriebene Dateisystem anhängen. Informationen zur Änderung einer UUID finden Sie in der Linux-Dokumentation. Möglicherweise müssen Sie auch die Datei /etc/fstab manuell bearbeiten, damit der ursprüngliche Datenträger und/oder der zurückgeschriebene Datenträger angehängt werden können.

Btrfs-Dateisysteme sichern und zurückschreiben

Sie können Btrfs-Dateisysteme mit den Befehlen **incremental**, **selective**, **restore**, **archive** und **retrieve** des Clients für Sichern/Archivieren sichern, zurückschreiben, archivieren und abrufen.

Informationen zu diesem Vorgang

Beim Sichern eines Btrfs-Dateisystems mit einer Version des Clients für Sichern/Archivieren vor Version 7.1 wurde der Dateisystemtyp in der GUI und Befehlsausgabe des IBM Spectrum Protect-Servers als Unbekannt aufgelistet. Der Dateisystemtyp Unbekannt wird angezeigt, weil Btrfs-Dateisysteme vor IBM Spectrum Protect Version 7.1 offiziell nicht unterstützt wurden. Wenn Sie dasselbe Btrfs-Dateisystem mit einem Client für Sichern/Archivieren der Version 7.1 (oder höher) sichern, werden alle Dateien, die über Zugriffssteuerungslisten (ACLs) und erweiterte Attribute (XATTRs) verfügen, selbst dann erneut gesichert, wenn sich ihr Inhalt seit der letzten Sicherung, die mit der früheren Clientversion erstellt wurde, nicht geändert hat. Außerdem wird nach der Sicherung eines Btrfs-Dateisystems mit dem Client der Version 7.1 (oder höher) der Dateisystemtyp in der GUI und Befehlsausgabe des IBM Spectrum Protect-Servers korrekt als Btrfs angezeigt.

Auch bei einem Client der Version 7.1 oder höher kann es dazu kommen, dass eine Datei in der nächsten Sicherungsoperation enthalten ist, wenn die Datei in einem Btrfs-Dateisystem kopiert wird. Wenn Sie eine Datei beispielsweise mit dem Befehl **cp** und der Option **-p** oder **-preserve** (Modus, Eigentumsrecht und Zeitmarken beibehalten) kopieren und wenn sich die Attribute der Datei ändern, wird das erweiterte Attribut für die Zugriffs-ACL (system.posix_acl_access) geändert. Da sich ein erweitertes Attribut ändert, sichert der Client die gesamte Datei und aktualisiert nicht nur die Attribute für die Datei.

Vorgehensweise

1. Hängen Sie das Dateisystem an, das Sie schützen oder wiederherstellen wollen. Das folgende Beispiel zeigt die Syntax zum Anhängen eines Dateisystems:
`mount /dev/sdb1 on /btreesfs1 type btrfs (rw)`
2. Führen Sie eine der folgenden Operationen aus, um das Dateisystem zu schützen oder wiederherzustellen:

Operation	Befehl
Dateisystem sichern	<code>dsmc incr /btreesfs1</code>

Operation	Befehl
Dateisystem zurückschreiben	dsmc restore /btreefs1/ -subdir=yes -replace=yes
Dateisystem archivieren	dsmc archive /btreefs1/ -subdir=yes
Dateisystem abrufen	dsmc retrieve /btreefs1/ -subdir=yes -replace=yes
Dateisystemmomentaufnahme sichern	<p>Erstellen Sie die Dateisystemmomentaufnahme. Verwenden Sie den Befehl btrfs subvolume snapshot. In diesem Beispiel wird das Verzeichnis btreefs1_snap in dem Dateisystem /btreefs1 als Momentaufnahmeverzeichnis angegeben.</p> <pre>btrfs subvolume snapshot /btreefs1/ /btreefs1/btreefs1_snap</pre> <p>Geben Sie den Befehl incremental des Clients für Sichern/Archivieren aus. Geben Sie die Option snapshotroot und die Position der Btrfs-Momentaufnahme an.</p> <pre>\$DSM_DIR/dsmc incr /btreefs1 -snapshotroot=/btreefs1/btreefs1_snap</pre>
Imagesicherung ausführen	<p>Bevor Sie eine Imagesicherung erstellen, müssen alle Unterdatenträger abgehängt werden.</p> <pre>dsmc backup image /btreefs1 -snapshotproviderimage=none</pre> <p>Um zu vermeiden, dass die Unterdatenträger abgehängt werden müssen, erstellen Sie eine momentaufnahmebasierte Imagesicherung.</p> <pre>dsmc backup image /btreefs1</pre>
Imagesicherung zurückschreiben	<p>Bevor Sie eine Imagesicherung zurückschreiben, müssen alle Unterdatenträger abgehängt werden.</p> <pre>dsmc restore image /btreefs1</pre>

Btrfs-Unterdatenträger sichern und zurückschreiben

Sie können Btrfs-Unterdatenträger mit den Befehlen **incremental**, **selective**, **restore**, **archive** und **retrieve** des Clients für Sichern/Archivieren sichern, zurückschreiben, archivieren und abrufen.

Vorgehensweise

1. Listen Sie die Unterdatenträger auf und ermitteln Sie ihre IDs.

```
btrfs subvolume list /btreefs1  
ID 256 top level 5 path @  
ID 262 top level 5 path @/btreefs1_sub1
```
2. Erstellen Sie das Verzeichnis, das als Mountpunkt für den Unterdatenträger verwendet werden soll.

```
mkdir /btreefs1_sub1
```

3. Hängen Sie den Unterdatenträger an. Verwenden Sie beispielsweise die folgende Syntax, um den Unterdatenträger auf der Einheit sdb1 bei /btreefs1_sub1 anzuhängen: `mount -t btrfs -o subvolid=262 /dev/sdb1 /btreefs1_sub1`
- Führen Sie eine oder mehrere der folgenden Operationen aus, um den Unterdatenträger zu schützen bzw. wiederherzustellen:

Operation	Befehl
Unterdatenträger sichern	Sowohl Teilsicherungen als auch selektive Sicherungen werden unterstützt. <code>dsmc incr /btreefs1_sub1</code> <code>dsmc sel /btreefs1_sub1/ -subdir=yes</code>
Unterdatenträger zurückschreiben	<code>dsmc restore /btreefs1_sub1/</code> <code>-subdir=yes -replace=yes</code>
Unterdatenträger archivieren	<code>dsmc archive /btreefs1_sub1/</code> <code>-subdir=yes</code>
Unterdatenträger abrufen	<code>dsmc retrieve /btreefs1_sub1/</code> <code>-subdir=yes -replace=yes</code>
Momentaufnahme eines Btrfs-Unterdatenträgers sichern	Erstellen Sie die Unterdatenträgermomentaufnahme. Verwenden Sie den Befehl btrfs subvolume snapshot . In diesem Beispiel wird das Verzeichnis /btreefs1/btreefs1_sub1_snap für den Unterdatenträger mit dem Namen btreefs1_sub1 als Momentaufnahmeverzeichnis angegeben. <code>btrfs subvolume snapshot</code> <code>/btreefs1/btreefs1_sub1</code> <code>/btreefs1/btreefs1_sub1_snap</code> Geben Sie den Befehl incremental des Clients für Sichern/Archivieren aus. Geben Sie die Option snapshotroot und die Position der Btrfs-Momentaufnahme an. <code>dsmc incr /btreefs1_sub1</code> <code>-snapshotroot=/btreefs1</code> <code>/btreefs1_sub1_snap</code>

NAS-Dateisysteme mit Network Data Management Protocol sichern

Windows-, AIX- und Solaris-Clients für Sichern/Archivieren können Network Data Management Protocol (NDMP) verwenden, um NAS-Dateisystemimages (NAS = Network Attached Storage) effizient zu sichern und zurückzuschreiben. Die Dateisystemimages können auf automatisierten Bandlaufwerken oder Speicherarchiven, die lokal an Network Appliance- oder EMC Celerra-NAS-Dateiserver angeschlossen sind, oder auf Bandlaufwerken oder Speicherarchiven, die lokal an einen IBM Spectrum Protect-Server angeschlossen sind, gesichert und von diesen zurückgeschrieben werden.

NDMP-Unterstützung ist nur für IBM Spectrum Protect Extended Edition verfügbar.

Für Linux x86_64-Clients können auch Teilsicherungen verwendet werden, um NAS-Dateisysteme zu sichern. Weitere Informationen finden Sie in der Beschreibung des Befehls **incremental** und der Optionen **snapshotroot**, **snappdiff**, **createnewbase** und **diffsnapshot**.

Nach der Konfiguration der NDMP-Unterstützung stellt der Server eine Verbindung zu der NAS-Einheit her und verwendet NDMP, um jede Sicherungs- und Zurückschreibungsoperation einzuleiten, zu steuern und zu überwachen. Die NAS-Einheit führt die externe Datenübertragung zu und von dem NAS-Dateisystem zu einem lokal angeschlossenen Speicherarchiv durch.

Für NAS-Einheiten, die NDMP Version 4 unterstützen, ist die Datenübertragung vom Dateiserver zum Server verfügbar.

Zu den Vorteilen von Sicherungen mit NDMP gehören:

- LAN-unabhängige Datenübertragung.
- Hochleistungsfähige und skalierbare Sicherungen und Zurückschreibungen.
- Sicherung auf lokale Bandeinheiten ohne Datenaustausch auf dem Netz.

Die folgende Unterstützung wird zur Verfügung gestellt:

- Vollständige Dateisystemimagesicherung aller Dateien innerhalb eines NAS-Dateisystems.
- Differenzdateisystemimagesicherung aller Dateien, die sich seit der letzten vollständigen Imagesicherung geändert haben.
- Parallele Sicherungs- und Zurückschreibungsoperationen bei der Verarbeitung mehrerer NAS-Dateisysteme.
- Auswahl von Schnittstellen zum Einleiten, Überwachen oder Abbrechen von Sicherungs- und Zurückschreibungsoperationen:
 - GUI des Clients für Sichern/Archivieren
 - Die Befehlszeilenschnittstelle des Clients für Sichern/Archivieren ist nur für Verbindungen zu IBM Spectrum Protect-Servern der Version 8.1.1, 8.1.0 oder 7.1.7 oder früher verfügbar.
 - Befehlszeilenschnittstelle des Verwaltungsclients (Sicherungs- und Zurückschreibungsoperationen können mit dem Verwaltungsbefehlsscheduler geplant werden)
 - Web-Client für Verwaltung

Die folgenden Funktionen werden *nicht* unterstützt:

- Archivieren und Abrufen
- Clientzeitplanung. Verwenden Sie Serverbefehle zum Planen einer NAS-Sicherung.
- Erkennung von beschädigten Dateien.
- Datenübertragungsoperationen für NAS-Daten, die von IBM Spectrum Protect gespeichert werden:
 - Umlagerung
 - Wiederherstellung
 - Export
 - Generierung von Sicherungssätzen

Zugehörige Konzepte:

„Voraussetzungen für NDMP-Unterstützung (nur Extended Edition)“ auf Seite 10

„Verarbeitung von NAS-Dateisystemen“ auf Seite 479

Zugehörige Verweise:

„Diffsnapshot“ auf Seite 400

„**Incremental**“ auf Seite 732

„Snapdiff“ auf Seite 581

NAS-Dateisysteme mit der GUI des Clients für Sichern/Archivieren unter Verwendung des NDMP-Protokolls sichern

Sowohl für die GUI des Clients für Sichern/Archivieren als auch für die Clientbefehlszeilenschnittstelle müssen Sie `passwordaccess=generate` angeben und `set authentication=on` muss auf dem Server angegeben werden.

Sie werden immer zur Eingabe einer Benutzer-ID und eines Kennworts aufgefordert. Um NAS-Knoten anzuzeigen und NAS-Funktionen auszuführen, müssen Sie eine berechtigte Verwaltungsbenutzer-ID und das Kennwort eingeben. Die berechtigte Benutzer-ID mit Administratorberechtigung sollte mindestens über Clienteigenerberechtigung sowohl für den NAS-Knoten als auch für den Client-Workstation-Knoten verfügen, die entweder über die Befehlszeile oder die GUI des Clients für Sichern/Archivieren verwendet werden. Der IBM Spectrum Protect-Server muss gemäß Konfiguration dem Clientknoten die Berechtigung für NAS-Sicherungs- und -Zurückschreibungsoperationen erteilen.

Sie können die Option `toc` zusammen mit der Option `include.fs.nas` in der Clientoptionsdatei verwenden, um anzugeben, ob der Client für jede Dateisystemsicherung Inhaltsverzeichnisinformationen (TOC-Informationen) speichert. Wenn Sie TOC-Informationen speichern, können Sie die GUI des Windows-Clients für Sichern/Archivieren verwenden, um die gesamte Baumstruktur des Dateisystems zu überprüfen und zurückzuschreibende Dateien und Verzeichnisse auszuwählen. Die Erstellung eines Inhaltsverzeichnisses erfordert, dass Sie das Attribut `TOCDestination` in der Sicherungskopiengruppe für die Verwaltungsklasse definieren, an die dieses Sicherungsbild gebunden wird. Beachten Sie, dass die TOC-Erstellung während der Sicherungsoperation eine zusätzliche Verarbeitung, zusätzliche Netzressourcen, zusätzlichen Speicherpoolspeicher und möglicherweise einen zusätzlichen Mountpunkt erfordert.

Um NAS-Dateisysteme mit der GUI des Clients für Sichern/Archivieren zu sichern, gehen Sie wie folgt vor:

1. Klicken Sie auf **Sichern** im Hauptfenster. Das Fenster **Sichern** wird angezeigt.
2. Falls erforderlich, erweitern Sie die Verzeichnisbaumstruktur.

Anmerkung:

- a. Der Anfangsknoten mit dem Namen **Knoten** ist nicht auswählbar. Dieser Knoten wird nur angezeigt, wenn ein NAS-Plug-in auf der Client-Workstation vorhanden ist.
 - b. NAS-Knoten werden auf derselben Stufe wie der Knoten der Client-Workstation angezeigt. Es werden nur Knoten angezeigt, für die der Administrator berechtigt ist.
 - c. Sie können NAS-Knoten erweitern, um Dateibereiche offen zu legen, aber eine darüber hinaus gehende Erweiterung ist nicht verfügbar (keine Dateinamen).
3. Klicken Sie auf die Auswahlfelder neben den Knoten oder den Dateisystemen, die Sie sichern wollen.
 4. Klicken Sie im Pulldown-Menü für die Sicherungsart die Art der Sicherung an, die ausgeführt werden soll. Die Liste 'NAS-Sicherungsart' ist nur aktiv, wenn Sie zuerst NAS-Sicherungsobjekte auswählen. Bei einer **Gesamtsicherung** wird das gesamte Dateisystem gesichert. Bei einer **Differenzsicherung** werden die Änderungen seit der jüngsten Gesamtsicherung gesichert.

5. Klicken Sie auf **Sichern**. Im Fenster **Task-Liste** für die NAS-Sicherung werden der Bearbeitungsstatus der Sicherung und die Statusleiste angezeigt. Die Zahl neben der Statusleiste gibt die Anzahl Byte an, die bisher gesichert wurden. Nachdem die Sicherung beendet ist, werden im Fenster mit dem NAS-Sicherungsbericht Verarbeitungsdetails, einschließlich der tatsächlichen Größe der Sicherung und der Summe der gesicherten Byte, angezeigt.

Anmerkung: Wenn die Sitzung der GUI des Clients für Sichern/Archivieren geschlossen werden muss, werden aktuelle NAS-Operationen nach der Trennung der Verbindung fortgesetzt. Sie können die Schaltfläche **Verlassen** im Fenster **Task-Liste** für die NAS-Sicherung verwenden, um die Verarbeitungsüberwachung zu verlassen, ohne die aktuelle Operation zu beenden.

6. (Optional) Um die Verarbeitung einer Operation vom Hauptfenster der grafischen Benutzerschnittstelle aus zu überwachen, öffnen Sie das Menü **Aktionen** und wählen Sie **IBM Spectrum Protect-Aktivitäten** aus. Während einer Sicherung zeigt die Statusleiste den Bearbeitungsstatus an. Eine prozentuale Schätzung wird für Differenzsicherungen nicht angezeigt.

Beachten Sie beim Sichern von NAS-Dateisystemen mit der GUI des Clients für Sichern/Archivieren Folgendes:

- Workstationsicherungen und ferne Sicherungen (NAS-Sicherungen) schließen sich in einem Sicherungsfenster gegenseitig aus. Wenn ein Element für die Sicherung ausgewählt wurde, muss das nächste Element, das Sie auswählen, denselben Typ aufweisen (entweder NAS oder Nicht-NAS).
- Für NAS-Knoten oder Dateisysteme werden keine Details auf der rechten Seite des Fensters **Sichern** angezeigt. Um Informationen zu Objekten in einem NAS-Knoten anzuzeigen, heben Sie das Objekt hervor und wählen Sie **Anzeigen > Dateiinformationen** im Menü aus.
- Um NAS-Dateibereiche zu löschen, wählen Sie **Dienstprogramme > Dateibereiche löschen** aus.
- Die Sicherungsoptionen gelten nicht für NAS-Dateibereiche und werden während einer NAS-Sicherungsoperation ignoriert.

Zugehörige Konzepte:

„Verarbeitung von NAS-Dateisystemen“ auf Seite 479

„NAS-Dateisysteme zurückschreiben“ auf Seite 264

Zugehörige Verweise:

„Toc“ auf Seite 619

Zugehörige Informationen:

 Server konfigurieren, um einem Clientknoten für NAS-Sicherungs- und -Zurückschreibungsoperationen Berechtigung zu erteilen

NAS-Dateisysteme über die Befehlszeile sichern

Sie können die Befehlszeile verwenden, um NAS-Dateisystemimages zu sichern.

Sie können den Befehlszeilenclient nur verwenden, wenn Sie eine Verbindung zu einem Server mit IBM Spectrum Protect Version 8.1.1, 8.1.0, 7.1.7 oder früher herstellen. Für Server mit IBM Spectrum Protect Version 8.1.2 oder höher verwenden Sie Serverbefehle im Verwaltungsbefehlszeilenclient (**dsmadm**).

In Tabelle 40 auf Seite 223 sind die Befehle und Optionen aufgelistet, die Sie zum Sichern von NAS-Dateisystemimages über die Befehlszeile verwenden können.

Tabelle 40. NAS-Optionen und -Befehle

Option oder Befehl	Definition	Seite
<code>domain.nas</code>	Mit der Option <code>domain.nas</code> geben Sie die Datenträger an, die für NAS-Sicherungen in Ihre Standarddomäne einbezogen werden sollen.	„Domain.nas“ auf Seite 413
<code>exclude.fs.nas</code>	Mit der Option <code>exclude.fs.nas</code> schließen Sie Dateisysteme auf dem NAS-Dateiserver von einer Imagesicherung aus, wenn sie zusammen mit dem Befehl backup nas verwendet wird. Diese Option ist <i>nur</i> für AIX- und Solaris-Clients gültig.	„Exclude-Optionen“ auf Seite 438
<code>include.fs.nas</code>	Verwenden Sie die Option <code>include.fs.nas</code> , um eine Verwaltungsklasse an NAS-Dateisysteme zu binden. Sie können auch angeben, ob während einer Imagesicherung des NAS-Dateisystems Inhaltsverzeichnisinformationen (TOC-Informationen) unter Verwendung der Option toc mit der Option <code>include.fs.nas</code> in Ihrer Clientoptionsdatei gespeichert werden. Diese Option ist <i>nur</i> für AIX- und Solaris-Clients gültig.	„Include-Optionen“ auf Seite 473
query node	Mit dem Befehl query node können Sie alle Knoten anzeigen, für die eine bestimmte Verwaltungenbenutzer-ID die Berechtigung zum Ausführen von Operationen hat. Die Verwaltungenbenutzer-ID sollte mindestens die Clientegnernberechtigung sowohl über den NAS-Knoten als auch den Client-Workstationknoten, die verwendet werden, besitzen.	„Query Node“ auf Seite 762
backup nas	Mit dem Befehl backup nas können Sie eine Imagesicherung eines oder mehrerer Dateisysteme, die zu einem NAS-Dateiserver gehören, erstellen.	„Backup NAS“ auf Seite 708
toc	Verwenden Sie die Option toc im Befehl backup nas oder mit der Option <code>include.fs.nas</code> , um anzugeben, ob für jede Dateisystemsicherung Inhaltsverzeichnisinformationen (TOC-Informationen) gespeichert werden.	„Toc“ auf Seite 619
monitor process	Mit dem Befehl monitor process können Sie aktuelle Sicherungs- und Zurückschreibungsprozesse für alle NAS-Knoten anzeigen, für die ein Benutzer mit Verwaltungsaufgaben berechtigt ist. Der Benutzer mit Verwaltungsaufgaben kann dann einen Prozess für die Überwachung auswählen.	„Monitor Process“ auf Seite 742

Tabelle 40. NAS-Optionen und -Befehle (Forts.)

Option oder Befehl	Definition	Seite
cancel process	Mit dem Befehl cancel process können Sie aktuelle Sicherungs- und Zurückschreibungsprozesse für alle NAS-Knoten anzeigen, für die ein Benutzer mit Verwaltungsaufgaben berechtigt ist. In der Anzeige kann der Benutzer mit Verwaltungsaufgaben einen Prozess zum Abbrechen auswählen.	„Cancel Process“ auf Seite 719
query backup	Verwenden Sie den Befehl query backup mit der Option class , um Informationen zu den Dateisystemimages anzuzeigen, die für einen NAS-Dateiserver gesichert wurden.	„Query Backup“ auf Seite 748
query filesystem	Verwenden Sie den Befehl query filesystem mit der Option class , um eine Liste der Dateibereiche anzuzeigen, die zu einem NAS-Knoten gehören.	„Query Filespace“ auf Seite 754
delete filesystem	Verwenden Sie den Befehl delete filesystem mit der Option class , um eine Liste der Dateibereiche anzuzeigen, die zu einem NAS-Knoten gehören. In dieser Liste können Sie einen Dateibereich zum Löschen auswählen.	„Delete Filespace“ auf Seite 727

- NAS-Knoten stellen eine neue Knotenart dar. Der Name des NAS-Knotens identifiziert einen NAS-Dateiserver und seine Daten eindeutig für IBM Spectrum Protect. Sie können den NAS-Knotennamen als Präfix vor die Dateispezifikation setzen, um den Dateiserver anzugeben, für den die Include-Anweisung gilt. Wenn Sie keinen NAS-Knotennamen angeben, gilt das angegebene Dateisystem für alle NAS-Dateiserver.
- Unabhängig von der Clientplattform wird in NAS-Dateisystemspezifikationen der Schrägstrich (/) als Trennzeichen verwendet. Zum Beispiel: /vol1/vol0.

Anmerkung: Wird eine NAS-Sicherungsoperation mithilfe der Befehlszeilenschnittstelle des Clients, der Client-GUI oder des Web-Clients eingeleitet, startet der Server einen Prozess, um die Operation einzuleiten, zu steuern und zu überwachen. Der Fortschritt in der Befehlszeilenschnittstelle des Clients lässt sich erst nach kurzer Zeit feststellen, da der Server eine Ladeoperation und andere erforderliche Tasks ausführen muss, bevor die Datenversetzung erfolgt.

Zugehörige Verweise:

„Toc“ auf Seite 619

NFS-Dateien sichern

Sie können den Client für Sichern/Archivieren zum Schützen von Dateien konfigurieren, auf die mit dem NFS-Protokoll (NFS = Network File System) oder dem CIFS-Protokoll (CIFS = Common Internet File System) zugegriffen wird.

Die Sicherungsleistung ist besser, wenn Sie den Client für Sichern/Archivieren an der Position installieren, an der das Dateisystem physisch vorhanden ist. Manchmal ist es jedoch notwendig, zum Sichern oder Wiederherstellen von Daten auf gemeinsam genutzten fernen Laufwerken mithilfe von NFS oder CIFS auf Dateisysteme zuzugreifen. Der Client für Sichern/Archivieren unter AIX-, Linux-, Mac OS X- und Solaris-Betriebssystemen kann Dateidaten auf einem über NFS oder CIFS an-

gehängten gemeinsam genutzten Laufwerk sichern, archivieren, zurückschreiben und abrufen. Die Operationen sind bei allen Versionen des NFS-Protokolls gültig, einschließlich NFS Version 2, NFS Version 3 und NFS Version 4.

Der Client für Sichern/Archivieren kann Zugriffssteuerungslisten sichern und zurückschreiben, wenn er für die Verwendung von NFS Version 4 konfiguriert ist.

Die folgenden Einschränkungen gelten, wenn der Client für Sichern/Archivieren Daten auf NFS-Datenträgern schützt:

- Clients für Sichern/Archivieren können keine Imagesicherungen von NFS-Datenträgern ausführen.
- Clients für Sichern/Archivieren unter AIX können auf NFS-Datenträgern keine momentaufnahmebasierten Dateisicherungen ausführen oder Dateien archivieren.
- Clients für Sichern/Archivieren können keine journalbasierten Sicherungen von NFS-Datenträgern ausführen.
- Clients für Sichern/Archivieren können möglicherweise keine NetApp-Datenträgermomentaufnahmen sichern, wenn über das NFS-Protokoll auf sie zugegriffen wird. Wenn der NetApp-Dateiserver für seine Datenträgermomentaufnahmen unterschiedliche Einheitenkennungen bereitstellt, werden diese Momentaufnahmen möglicherweise von Sicherungen ausgeschlossen. Das Verhalten ist von der Betriebssystemversion, von der Version des NetApp-Dateiservers und von den Einstellungen abhängig.

NFS-Dateisysteme mit der globalen Namensbereichsfunktion sichern

NFS-V4-Clients können NFS-Dateisysteme sichern, die mithilfe der globalen Namensbereichsfunktion (als *Linktechnik* bezeichnet) angehängt wurden. Alle Dateisysteme im globalen Namensbereich werden unter einem einzigen Dateibereich gesichert.

Die folgenden Beispiele zeigen die Dateisysteme im globalen Namensbereich, die unter einem einzigen Dateibereich gesichert werden:

```
Der Server 'publications' verfügt über das Dateisystem /doc
Der Server 'projects' verfügt über das Dateisystem /projects
Der Server 'data' verfügt über das Dateisystem /data
```

Der Server 'account1' ist der NFS-Hauptserver, der alle diese Dateisysteme mithilfe der Linktechnik exportiert, und er ist der Server, den alle Clients kennen. Das Verzeichnis /etc/exports auf 'account1' sieht wie folgt aus:

```
/doc -vers=4,refer=/doc@publications
/projects -vers=4,refer=/projects@projects
/data -vers=4,refer=/data@data
```

Der Client 'payroll' hängt Verzeichnisse vom Server 'account1' an und kann auf alle drei Dateisysteme zugreifen:

```
payroll:/#mount -o vers=4 account1:/ /mnt
payroll:/#ls /mnt
doc/ projects/ data/
```

Der Client 'payroll' kann die Datei /mnt als ein einziges NFS-Dateisystem sichern, wodurch alle anderen Dateisysteme gesichert werden.

Wichtig: Die Verwendung der Option `virtualmountpoint` kann die Systemleistung erhöhen, wenn Sie NFSV4-Dateisysteme mithilfe des globalen Namensbereichs si-

chern. Fügen Sie einer Zeilengruppe in dsm.sys die folgenden Einträge hinzu, um jedes angehängte Verzeichnis als separaten Dateibereich zu sichern:

```
VIRTUALMOUNTPOINT /doc
VIRTUALMOUNTPOINT /projects
VIRTUALMOUNTPOINT /data
```

AIX-Workloadpartitionsdateisysteme sichern

Mit dem Client für Sichern/Archivieren unter AIX können Sie Dateidaten lokaler Partitionen innerhalb der globalen Partition mithilfe des Namensbereichs der lokalen Partition innerhalb der globalen Partition sichern und zurückschreiben.

Jede Workloadpartition (WPAR) verfügt über ihre eigene Sicherheitsdomäne, so dass nur der globale Root einen garantierten Zugriff auf alle Daten hat.

Die Workloadpartitionen sind Partitionen, die innerhalb eines einzelnen AIX-Systemimages vollständig in Software erstellt werden und folgende Attribute aufweisen:

- Normalerweise erscheint die Workloadpartition als vollständiges und eigenständiges AIX-System.
- Es gibt keinen Hardwareassistenten und keine Konfiguration.

Workloadpartitionen stellen eine gesicherte und isolierte Umgebung für Unternehmensanwendungen in Bezug auf Verarbeitung, Signalgebung und Dateisystemspeicherbereich zur Verfügung. Software, die im Kontext einer Workloadpartition ausgeführt wird, erscheint, als ob sie ihre eigene separate Instanz von AIX hätte.

Das folgende Beispiel zeigt eine WPAR-Konfiguration innerhalb der globalen Workloadpartition:

Globale Partition:

```
Systemname: shimla
Dateisystem: /home /opt
```

WPAR #1-Konfiguration:

```
Name: wpar1
Dateisystem: /home; Name in globaler WPAR: /wpars/wpar1/home
```

WPAR #2-Konfiguration:

```
Name: wpar2
Dateisystem: /data; Name in globaler WPAR: /wpars/wpar2/data
```

Es gibt - wie folgt - zwei Arten, WPAR-Daten zu sichern:

- Alle WPAR-Dateisysteme als Dateibereiche innerhalb der globalen Partition sichern. Mit dem Namen des Dateibereichs muss die Workloadpartition identifiziert werden, zu der der Dateibereich gehört. Alle Daten werden mithilfe eines einzigen Zeitplans auf einem einzigen Knoten verwaltet. Unter Verwendung der Beispielkonfiguration zeigt das folgende Beispiel eine Musterdatei dsm.sys mit einer Serverzeilengruppe für alle Systeme, sowohl global als auch lokal:

```
SErvername shimla
TCPPort 1500
TCPSeveraddress server.example.com
nodename shimla
PasswordAccess generate
Domain /wpars/wpar1/home /wpars/wpar2/data /home /opt
```

- Jedes einzelne WPAR-Dateisystem unter einem anderen Knotennamen sichern. Bei dieser Methode wird für jede Workloadpartition eine Dateibereichsna-

menstrennung bereitgestellt. Jede Workloadpartition muss einen separaten Knotennamen und einen Scheduler haben, der innerhalb der globalen Partition ausgeführt wird. Außerdem müssen drei Scheduler-Services definiert werden, wobei jeder Service entsprechend dem Namen der Serverzeilengruppe eine andere Datei `dsm.opt` verwendet. Diese Methode ermöglicht, dass jede WPAR-Sicherungsoperation unabhängig von den anderen verwaltet wird. Unter Verwendung der Beispielkonfiguration zeigt das folgende Beispiel eine Musterdatei `dsm.sys` mit drei Serverzeilengruppen: eine für `wpar1`, eine für `wpar2` und eine für die globale Partition `shimla`:

```
SErvername  shimla_wpar1
TCPport    1500
TCPserveraddress  server.example.com
nodename    wpar1
PasswordAccess  generate
Domain      /wpars/wpar1/home

SErvername  shimla_wpar2
TCPport    1500
TCPserveraddress  server.example.com
nodename    wpar2
PasswordAccess  generate
Domain      /wpars/wpar2/data

SErvername  shimla
TCPport    1500
TCPserveraddress  server.example.com
nodename    shimla
PasswordAccess  generate
Domain      /home /opt
```

Solaris Zettabyte-Dateisysteme (ZFS) sichern

Auf Solaris SPARC- und Solaris x86-Systemen können Sie ZFS-Dateisysteme (Zettabyte File System) mithilfe von ZFS-Momentaufnahmen sichern. Der Vorteil dieser Methode im Vergleich zu einer normalen Teilsicherung oder selektiven Sicherung besteht darin, dass sich die Dateien und Ordner in einer Momentaufnahme immer im Lesezugriffsmodus befinden und daher während einer Sicherung nicht geändert werden können.

Informationen zu diesem Vorgang

Eine ZFS-Momentaufnahme erstellen Sie mithilfe von Oracle Solaris-ZFS-Befehlen. Beispiel:

```
zfs snapshot tank/myZFS@mySnapshot
```

In diesem Beispiel lautet der ZFS-Poolname `tank` und der Name des ZFS-Dateisystems ist `myZFS`. Dateien, die zu dieser ZFS-Momentaufnahme gehören, befinden sich in dem Unterverzeichnis `tank/myZFS/.zfs/snapshot/mySnapshot/`.

Vorgehensweise

Verwenden Sie eine dieser beiden Methoden, um eine ZFS-Momentaufnahme zu sichern.

- Sichern Sie jede Datei der Momentaufnahme mithilfe der Option `snapshotroot`. Beispiel:

```
dsmc inc -snapshotroot=/tank/myZFS/.zfs/snapshot/mySnapshot /tank/myZFS
```

Mit dieser Option kann der Administrator den aktuellen Momentaufnahme Pfad durch den ZFS-Dateisystem Pfad ersetzen, so dass die Dateien und Ordner mit dem ursprünglichen Dateisystem gesichert werden.

- Sichern Sie die vollständige Momentaufnahme mithilfe von Oracle Solaris-ZFS-Befehlen. Beispiel:

```
zfs send tank/myZFS@mySnapshot > /tmpdir/mySnapshotFile
```

Der Vorteil des Sicherns der vollständigen Momentaufnahme liegt darin, dass im Notfall das gesamte Dateisystem zurückgeschrieben werden kann.

Zugehörige Konzepte:

„Solaris Zettabyte-Dateisysteme (ZFS) zurückschreiben“ auf Seite 273

Zugehörige Verweise:

„Snapshotroot“ auf Seite 593

Verschlüsseltes AIX JFS2-Dateisystem sichern

Verwenden Sie das AIX JFS2-EFS-System (EFS = Encrypted File System - Verschlüsseltes Dateisystem), um Dateien entweder im Klartext oder im unformatierten Format zu sichern. Beim Format Klartext wird die Datei von EFS beim Lesen entschlüsselt. Beim unformatierten Format werden die Daten nicht entschlüsselt. Standardwert ist das unformatierte Format, aber wenn Sie die Option `efsdecrypt` auf `yes` setzen, erhalten Sie Sicherungen im Klartext.

Informationen zu diesem Vorgang

Wichtig: Immer, wenn Sie eine Sicherung ausführen, die auf einem EFS verschlüsselte Dateien einschließt, müssen Sie sicherstellen, dass Sie die korrekte Spezifikation der Option `efsdecrypt` verwenden. Falls sich der Optionswert `efsdecrypt` zwischen zwei Teilsicherungen ändert, werden alle verschlüsselten Dateien auf EFS-Dateisystemen erneut gesichert, selbst wenn sie sich seit der letzten Sicherung nicht geändert haben. Wenn Sie z. B. eine Teilsicherung verschlüsselter Dateien ausführen, die zuvor als unformatiert gesichert wurden, müssen Sie sicherstellen, dass `efsdecrypt` auf `no` gesetzt wird. Wenn Sie `efsdecrypt` in `yes` ändern, werden alle Dateien im Klartext erneut gesichert, selbst wenn sie unverändert sind. Stellen Sie deshalb sicher, dass Sie diese Option mit Vorsicht verwenden.

Wenn Sie versuchen, eine verschlüsselte Datei entweder auf eine Workstation, die EFS nicht unterstützt, oder in ein Dateisystem, in dem EFS nicht aktiv ist, zurückzuschreiben, wird eine Fehlermeldung geschrieben und die Datei wird übersprungen.

Einige Gründe für das Sichern von EFS mit der Verschlüsselung im Klartext:

- Diese Entschlüsselungsart ist nützlich, wenn Sie die Verschlüsselung des IBM Spectrum Protect-Clients für Sichern/Archivieren oder eine andere Art von Hardwareverschlüsselung (z. B. für Bandsysteme) verwenden wollen.
- Sie können Klartext für eine langfristige Archivierung von Daten verwenden, da die Daten unabhängig von der Plattform oder dem Verschlüsselungsschema gespeichert werden.

Nachfolgend einige Dinge, die zu beachten sind, wenn Sie eine Datei im Klartext sichern:

- Der Benutzer, von dem der Client für Sichern/Archivieren aufgerufen wurde, muss die Datei entschlüsseln können.

- Der Benutzer kann Lesezugriff auf eine Datei, aber keinen Zugriff auf den Schlüssel haben.

In den folgenden Szenarios wird eine Fehlermeldung ausgegeben:

Vorgehensweise

1. Der Benutzer wird im Modus Rootwächter ausgeführt, und EFS verfügt über das Konzept von zwei Roottypen. Rootadministrator ist der traditionelle Modus. Ein Root im Wächtermodus hat keinen Zugriff auf die unverschlüsselten Daten, es sei denn, der Benutzer ist der Eigner oder ein Mitglied der Dateigruppe.
2. Der Benutzer wird mit einer Nicht-Rootbenutzer-ID ausgeführt und versucht die Archivierung einer Datei, auf die er Lesezugriff hat, aber der Benutzer ist nicht der Eigner oder ein Mitglied der Dateigruppe. EFS wird es nicht zulassen, dass die Daten entschlüsselt werden.

Ergebnisse

Nachfolgend einige Hinweise zum Sichern von unformatierten EFS-Daten:

- Die Clientverschlüsselungseinstellung, die eine doppelte Verschlüsselung verhindert (dies aber nur auf dem Client), wird vom Client für Sichern/Archivieren nicht berücksichtigt. Der Server weiß nicht, dass die Daten verschlüsselt sind; dies bedeutet, dass eine Verschlüsselung, die z. B. von einem Bandlaufwerk erfolgt, trotzdem vorkommen kann.
- Die Komprimierungseinstellung wird vom Client nicht berücksichtigt, sodass der Client gar nicht erst versuchen wird, die Daten zu komprimieren.
- Die Schlüsselspeicherdatei wird vom Client nicht automatisch gesichert oder zurückgeschrieben. Wenn Sie verschlüsselte Dateien zurückschreiben, müssen Sie unter Umständen auch die Schlüsselspeicherdateien zurückschreiben, damit die Daten entschlüsselt werden können.

Tipps:

1. Stellen Sie zum Schutz des Schlüsselspeichers sicher, dass der Inhalt von `/var/efs` in Ihre regelmäßigen Sicherungen eingeschlossen wird.
 2. Für die Schlüsselspeicherdaten verwenden Sie die IBM Spectrum Protect-Speichermaßnahme mit einer unbegrenzten Anzahl Versionen.
- EFS-Dateien, die im unformatierten Modus (Standardwert) gesichert wurden, können nicht von einem Client für Sichern/Archivieren vor Version 5.5 oder einem Client auf einer anderen UNIX-Plattform zurückgeschrieben werden.

Erweiterte AIX JFS2-Attribute sichern

AIX Enhanced Journal File System (JFS2) bietet Sicherungsverarbeitung für benannte erweiterte Attribute für alle Dateisysteme, die benannte erweiterte Attribute unterstützen.

Diese erweiterten Attribute werden automatisch mit jedem Objekt gesichert, das Daten mit erweiterten Attributen enthält, und es ist keine weitere Aktion erforderlich.

Ist das Dateisystem mit dem V2-Format definiert, ist JFS2 das einzige Dateisystem, das erweiterte Attribute unterstützt. Sie können JFS2 für erweiterte Attribute bei Dateien und Verzeichnissen verwenden; Sie können JFS2 jedoch nicht für erweiterte Attribute bei symbolischen Verbindungen verwenden.

Virtuelle VMware-Maschinen sichern

Sie können mithilfe des Clients für Sichern/Archivieren eine virtuelle VMware-Maschine sichern und zurückschreiben. Gesamtsicherungen der virtuellen Maschine werden auf Plattenimageebene ausgeführt. Bei Teilsicherungen werden nur die Daten gesichert, die sich seit der vorherigen Gesamtsicherung geändert haben.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Tabelle 41 enthält die Sicherungs- und Zurückschreibungsfunktionalität für virtuelle VMware-Maschinen, die der Client für Sichern/Archivieren auf Linux-Plattformen implementieren kann.

Tabelle 41. Sicherungs- und Zurückschreibungsfunktionalität für virtuelle VMware-Maschinen auf Linux-Plattformen

Funktion	Kommentar
Immer inkrementelle VM-Gesamtsicherung:	<p>Eine VM-Gesamtsicherung ist erforderlich, bevor Sie Teilsicherungen erstellen können. Wenn Sie immer inkrementelle Sicherungen planen, wird dieser Sicherungstyp automatisch für die erste Sicherung ausgewählt, wenn noch keine Gesamtsicherung erstellt wurde. Daten aus Teilsicherungen werden mit Daten aus der Gesamtsicherung kombiniert, um daraus ein synthetisches Gesamtsicherungsimage zu erstellen. Bei nachfolgenden immer inkrementellen VM-Gesamtsicherungen werden alle verwendeten Blöcke gelesen und auf den IBM Spectrum Protect-Server kopiert. Bei jeder immer inkrementellen VM-Gesamtsicherung werden alle verwendeten Blöcke, unabhängig davon, ob die Blöcke seit der letzten Sicherung geändert wurden oder nicht, gelesen und kopiert. Sie können weiterhin eine VM-Gesamtsicherung planen, obwohl eine Gesamtsicherung nicht mehr erforderlich ist. Sie können beispielsweise eine VM-Gesamtsicherung ausführen, um eine Sicherung für einen anderen Knotennamen mit anderen Aufbewahrungseinstellungen zu erstellen.</p> <p>Sie können diesen Sicherungsmodus nicht für die Sicherung einer virtuellen VMware-Maschine verwenden, wenn die Verschlüsselung der Sicherungsdaten auf dem Client konfiguriert ist.</p>

Tabelle 41. Sicherungs- und Zurückschreibungsfunktionalität für virtuelle VMware-Maschinen auf Linux-Plattformen (Forts.)

Funktion	Kommentar
Immer inkrementelle VM-Teilsicherung:	<p>Sie müssen nur einmal eine VM-Gesamtsicherung erstellen. Bei der VM-Gesamtsicherung werden alle verwendeten Plattenblöcke, deren Eigner eine virtuelle Maschine ist, auf den IBM Spectrum Protect-Server kopiert. Nach dem Abschluss der ersten Gesamtsicherung sind alle nachfolgenden Sicherungen der virtuellen Maschine immer inkrementelle Teilsicherungen. Bei jeder immer inkrementellen Teilsicherung werden nur die Blöcke kopiert, die seit der letzten Sicherung geändert wurden, unabhängig vom Typ der letzten Sicherung. Der Server verwendet eine Gruppierungstechnologie, mit der die geänderten Blöcke aus der neuesten Sicherung den Daten zugeordnet werden, die bereits aus vorherigen Sicherungen auf dem Server gespeichert sind. Eine neue vollständige Sicherung wird dann jedes Mal effektiv erstellt, wenn bei einer immer inkrementellen Teilsicherung geänderte Blöcke auf den Server kopiert werden.</p> <p>Der Sicherungsmodus für immer inkrementelle Teilsicherungen bietet die folgenden Vorteile:</p> <ul style="list-style-type: none"> • Verbessert die Effizienz beim Sichern virtueller Maschinen. • Vereinfacht Datenzurückschreibungsoperationen. • Optimiert Datenzurückschreibungsoperationen. <p>Bei einer Zurückschreibungsoperation können Sie für die Wiederherstellung von Daten Optionen für den Zeitpunkt und das Datum angeben. Die Daten werden aus der ursprünglichen vollständigen Sicherung und allen geänderten Blöcken zurückgeschrieben, die den Daten zugeordnet sind.</p> <p>Sie können diesen Sicherungsmodus nicht für die Sicherung einer virtuellen VMware-Maschine verwenden, wenn die Verschlüsselung der Sicherungsdaten auf dem Client konfiguriert ist.</p>
Wiederherstellung von Objekten für Dateien und Ordner aus einer vollständigen Sicherung der virtuellen Maschine:	Ermöglicht das Wiederherstellen von Dateien und Ordnern aus einer vollständigen Sicherung einer virtuellen Maschine. Die Wiederherstellung von Elementen ist nur mit IBM Spectrum Protect Recovery Agent verfügbar.
Vollständige Zurückschreibung der virtuellen Maschine:	Schreibt alle Dateisysteme, virtuellen Platten und die Konfiguration der virtuellen Maschine zurück.

Zugehörige Konzepte:

„Parallele Sicherungen virtueller Maschinen“ auf Seite 234

Zugehörige Tasks:

„Umgebung für Gesamtsicherungen virtueller VMware-Maschinen vorbereiten“

„Gesamtsicherungen für virtuelle VMware-Maschinen erstellen“ auf Seite 233

Umgebung für Gesamtsicherungen virtueller VMware-Maschinen vorbereiten

Zur Vorbereitung der VMware-Umgebung auf die Sicherung vollständiger virtueller VMware-Maschinen führen Sie die folgenden Schritte aus. Auf dem vStorage-Sicherungsserver kann entweder ein Windows- oder ein Linux-Client ausgeführt werden.

Vorbereitende Schritte



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Vorgehensweise

1. Gehen Sie wie folgt vor, um die Speicherumgebung für die Sicherung zu konfigurieren:
 - a. Konfigurieren Sie Ihre Speicherumgebung so, dass der vStorage-Sicherungs-
server auf die Speicherdatenträger zugreifen kann, die sich in Ihrer ESX-
Server-Farm befinden.
 - b. Wenn Sie NAS (Network-Attached Storage) oder DAS (Direct-Attached Sto-
rage) verwenden, stellen Sie sicher, dass der vStorage-Sicherungs-
server mit einer netzbasierten Transportmethode auf die Datenträger zugreift.
 - c. Optional: Nehmen Sie für den Datenzugriff die folgenden Einstellungen vor:
 - Erstellen Sie SAN-Zonen, mit denen Ihr vStorage-Sicherungs-
server auf die logischen Speichereinheiten zugreifen kann, in denen sich Ihre VMware-
Datenspeicher befinden (SAN - storage area network, Speicherbereichs-
netz).
 - Konfigurieren Sie die Hostzuordnungen des Plattensubsystems, so dass
alle ESX-Server und der Sicherungs-Proxy auf dieselben Plattendaten-
träger zugreifen können.
2. Gehen Sie wie folgt vor, um den vStorage-Sicherungs-
server zu konfigurieren:
 - a. Legen Sie die Umgebungsvariable **LD_LIBRARY_PATH** so fest, dass sie auf das
Clientinstallationsverzeichnis verweist, und exportieren Sie die Umgebungs-
variable. Beispiel:
export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
 - b. Fügen Sie das Clientinstallationsverzeichnis zum Pfad jedes Konto hinzu,
das Befehle des Clients für Sichern/Archivieren verwendet, z. B. **dsmc**,
dsmcad oder **dsmj**.
3. Gehen Sie wie folgt vor, um IBM Spectrum Protect zu ändern:
 - a. Greifen Sie auf die Verwaltungsbefehlszeile des Clients für Sichern/
Archivieren zu.
 - b. Führen Sie im Client für Sichern/Archivieren auf dem vStorage-Sicherungs-
server den folgenden Befehl aus, um den Knoten zu registrieren:
register node Servername Kennwort

Dabei gibt *Servername* den vollständigen Computernamen des vStorage-Si-
cherungsservers und *Kennwort* das Kennwort für den Zugriff auf den Server
an.

Zugehörige Tasks:

„Gesamtsicherungen für virtuelle VMware-Maschinen erstellen“ auf Seite 233

Zugehörige Verweise:

„Backup VM“ auf Seite 710

„Query VM“ auf Seite 768

„Restore VM“ auf Seite 791

„Vmchost“ auf Seite 637

„Vmcpw“ auf Seite 638

„Vmcuser“ auf Seite 640

Gesamtsicherungen für virtuelle VMware-Maschinen erstellen

Bei einer Gesamtsicherung einer virtuellen VMware-Maschine wird die gesamte virtuelle Maschine, einschließlich der virtuellen Platten und der Konfigurationsdatei der virtuellen Maschine, gesichert. Dieser Sicherungstyp ähnelt einer Imagesicherung. Für die Erstellung der Gesamtsicherung konfigurieren Sie den Client für Sichern/Archivieren auf dem vStorage-Sicherungsserver. Auf dem vStorage-Sicherungsserver muss ein Windows- oder Linux-Client ausgeführt werden.

Vorbereitende Schritte



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Vorgehensweise

1. Führen Sie die Schritte im folgenden Abschnitt aus, um die Umgebung vorzubereiten:
„Umgebung für Gesamtsicherungen virtueller VMware-Maschinen vorbereiten“ auf Seite 231
2. Gehen Sie wie folgt vor, um den Client für Sichern/Archivieren auf dem vStorage-Sicherungsserver zu konfigurieren:
 - a. Klicken Sie auf der Begrüßungsseite der GUI des Clients für Sichern/Archivieren auf **Editieren** > **Clientvorgaben**.
 - b. Wählen Sie die Registerkarte **VM-Sicherung** aus.
 - c. Wählen Sie **VMWare - Vollständige VM** aus.
 - d. Wählen Sie in der Liste **Sicherungstypen für Domäne** die Option **Vollständige VM-Sicherung für Domäne** aus.
 - e. Geben Sie in das Feld **Host** entweder den Hostnamen jedes ESX-Servers oder den Hostnamen des Virtual Center ein. Wenn Sie das Virtual Center angeben, können Sie virtuelle Maschinen auf allen VMware-Servern sichern, die vom Virtual Center verwaltet werden.
 - f. Geben Sie die Benutzer-ID und das Kennwort für den Host ein, den Sie im Feld **Host** angeben.
 - g. Optional: Falls Sie die Standardverwaltungs-klasse für Gesamtsicherungen von virtuellen Maschinen überschreiben wollen, geben Sie die Verwaltungs-klasse an, die verwendet werden soll.
 - h. Geben Sie in das Feld **Datenspeicherposition** den Pfad des Verzeichnisses ein, in dem die Dateien gespeichert werden.
 - i. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.
3. Gehen Sie wie folgt vor, um eine Sicherung einer der virtuellen Maschinen zu erstellen:
 - a. Führen Sie über die Befehlszeile des vStorage-Sicherungs-servers den folgenden Befehl aus:

```
dsmc backup vm Name_der_eigenen_VM -mode=ifull -vmbackuptype=fullvm
```


Dabei gibt *Name_der_eigenen_VM* den Namen der virtuellen Maschine an.
 - b. Überprüfen Sie, ob der Befehl fehlerfrei ausgeführt wurde. Die folgende Nachricht zeigt eine erfolgreiche Ausführung an:

```

Befehl 'Backup VM' ausgeführt
Gesamtzahl der erfolgreich gesicherten virtuellen Maschinen: 1
Virtuelle Maschine 'VM-Name' auf Knotenname NODE gesichert
Gesamtzahl der fehlgeschlagenen virtuellen Maschinen: 0
Gesamtzahl der verarbeiteten virtuellen Maschinen: 1

```

4. Gehen Sie wie folgt vor, um zu überprüfen, ob Sie die Dateien für die virtuelle Maschine zurückschreiben können:
 - a. Führen Sie über die Befehlszeilenschnittstelle des vStorage-Sicherungservers den folgenden Befehl aus:
`dsmc restore vm VM-Name`
 - b. Wenn während der Zurückschreibungsverarbeitung Fehler auftreten, suchen Sie im Clientfehlerprotokoll nach weiteren Informationen.

Tipp: Die Protokolldatei wird unter `/opt/ibm/Tivoli/TSM/baclient/dsmerror.log` gespeichert.

Zugehörige Konzepte:

„Parallele Sicherungen virtueller Maschinen“

Zugehörige Tasks:

„Umgebung für Gesamtsicherungen virtueller VMware-Maschinen vorbereiten“ auf Seite 231

Zugehörige Verweise:

„Backup VM“ auf Seite 710

„Domain.vmfull“ auf Seite 414

„Query VM“ auf Seite 768

„Restore VM“ auf Seite 791

„Mode“ auf Seite 509

„Vmchost“ auf Seite 637

„Vmcpw“ auf Seite 638

„Vmcuser“ auf Seite 640

„Vmmc“ auf Seite 659

„Vmvstortransport“ auf Seite 677

Parallele Sicherungen virtueller Maschinen

Bei der parallelen Sicherungsverarbeitung können Sie einen einzigen Knoten einer Einheit zum Versetzen von Daten verwenden, um mehrere virtuelle Maschinen (VMs) gleichzeitig zu sichern, um Ihre Sicherungsleistung zu optimieren.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Informationen zu parallelen Sicherungsoperationen finden Sie in Mehrere virtuelle Maschinen parallel sichern.

Tivoli Storage Manager FastBack-Daten sichern und archivieren

Verwenden Sie Tivoli Storage Manager FastBack, um die neuesten Momentaufnahmen für die kurzfristige Aufbewahrung zu sichern und zu archivieren.

Verwenden Sie die Befehle **archive fastback** und **backup fastback**, um Datenträger für die kurzfristige Aufbewahrung zu sichern und zu archivieren, die durch die Optionen `fbpolicyname`, `fbclientname` und `fbvolumename` angegeben sind.

Zugehörige Konzepte:

„Installationsvoraussetzungen für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Clientdaten“ auf Seite 10

„Client für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Daten konfigurieren“ auf Seite 106

Zugehörige Verweise:

„Fbclientname“ auf Seite 447

„Fbpolicyname“ auf Seite 448

„Fbvolumename“ auf Seite 452

Status der Sicherungsverarbeitung anzeigen

Während einer Sicherung zeigt der Client für Sichern/Archivieren standardmäßig den Status jeder Datei an, die er zu sichern versucht.

Der Client meldet die Größe, den Pfad, den Dateinamen sowie die Gesamtzahl übertragener Byte zurück und gibt an, ob der Sicherungsversuch für die Datei erfolgreich war. Diese Angaben werden außerdem in der Datei `dsmsched.log` für geplante Befehle aufgezeichnet.

Die Java-GUI des Web-Clients und des Clients für Sichern/Archivieren stellt das Fenster **Task-Liste** zur Verfügung, in dem Informationen zu gerade verarbeiteten Dateien angezeigt werden. Nach Beendigung einer Task werden im Fenster **Sicherungsbericht** die Verarbeitungsdetails angezeigt. Klicken Sie auf die Schaltfläche **Hilfe** im Fenster **Sicherungsbericht**, um hierzu den Hilfetext aufzurufen.

In der Befehlszeile des Clients für Sichern/Archivieren wird der Name jeder Datei angezeigt, nachdem sie zum Server gesendet wurde. Das Statusanzeigefeld zeigt den Gesamtfortschritt an.

In Tabelle 42 sind einige Informationsnachrichten mit ihrer Bedeutung aufgelistet.

Tabelle 42. Informationsnachrichten der Clientbefehlszeile

Informationsnachricht	Bedeutung
Verzeichnis-->	Gibt das Verzeichnis an, das gesichert wird.
Normale Datei-->.	Jede Datei, die weder ein Verzeichnis noch eine symbolische Verbindung noch eine Gerätedatei ist.
Gerätedatei-->	Gerätedateien definieren Einheiten für das System oder temporäre Dateien, die durch Prozesse erstellt werden. Es gibt drei Grundtypen der Gerätedateien: FIFO (First-In, First-Out), Block und Zeichen. FIFO-Dateien werden auch als Pipe bezeichnet. Pipes werden durch einen Prozess erstellt, um eine vorübergehende Kommunikation mit einem anderen Prozess zu ermöglichen. Diese Dateien sind nicht mehr vorhanden, wenn der erste Prozess beendet ist. Blockbelegungs- und Zeichendateien definieren Einheiten. Der Client verarbeitet nur einheiten- und benannte-Pipe-orientierte Gerätedateien. Socket-Gerätedateien werden nicht verarbeitet.
Symbolische Verbindung-->	Gibt an, dass der Client eine symbolische Verbindung sichert.
Aktualisieren-->	Gibt an, dass nur die Dateimetadaten gesendet werden und nicht die Daten selbst.

Tabelle 42. Informationsnachrichten der Clientbefehlszeile (Forts.)

Informationsnachricht	Bedeutung
Verfall-->	Gibt ein Objekt (Datei oder Verzeichnis) auf dem Server an, das auf dem Client nicht mehr vorhanden ist. Das Objekt ist verfallen und wird auf dem Server inaktiviert.
Gesamtanzahl geprüfter Objekte:	Wie angezeigt. Bei der journalbasierten Sicherung ist die Anzahl der geprüften Objekte möglicherweise kleiner als die der gesicherten Objekte. Bei Verwendung der Teilsicherung unter Verwendung der Momentaufnahmedifferenz beträgt die Anzahl der geprüften Objekte null. Die Anzahl beträgt null, weil der Client eine Teilsicherung der Dateien durchführt, die NetApp als geändert gemeldet hat. Der Client überprüft den Datenträger nicht auf Dateien, die sich geändert haben.
Gesamtanzahl gesicherter Objekte:	Wie angezeigt.
Gesamtzahl verschlüsselter Objekte:	Hierbei handelt es sich um die Anzahl der Objekte, die während der Sicherungs- oder Archivierungsverarbeitung verschlüsselt wurden.
Datenverschlüsselungstyp:	Gibt die Art des Verschlüsselungsalgorithmus (z. B. 256-Bit AES) an, wenn mindestens ein Objekt während der Sicherungs- oder Archivierungsverarbeitung verschlüsselt wird.
Gesamtanzahl aktualisierter Objekte:	Hierbei handelt es sich um Dateien, deren Attribute, wie z. B. Dateieigner oder Dateiberechtigungen, geändert wurden.
Gesamtanzahl erneut gebundener Objekte:	Weitere Informationen siehe „Verwaltungsklassen an Dateien binden“ auf Seite 318.
Gesamtanzahl gelöschter Objekte:	Hierbei handelt es sich um die Anzahl der Objekte, die von der Client-Workstation gelöscht wurden, nachdem sie erfolgreich auf dem Server archiviert wurden. Die Anzahl ist für alle Sicherungsbefehle null.
Gesamtanzahl verfallener Objekte:	Weitere Informationen enthält der Abschnitt über vollständige und partielle Teilsicherungen.
Gesamtanzahl fehlgeschlagener Objekte:	Objekte können aus verschiedenen Gründen fehlschlagen. Weitere Einzelheiten hierzu sind in der Datei dsmerror.log enthalten.
Gesamtzahl Momentaufnahmedifferenzobjekte	Bei Teilsicherungen unter Verwendung der Momentaufnahmedifferenz stellt dies die Gesamtzahl der gesicherten Objekte und die Gesamtzahl der verfallenen Objekte dar.
Gesamtzahl deduplizierter Objekte	Gibt die Anzahl der deduplizierten Dateien an.
Gesamtzahl der überprüften Byte:	Gibt die Summe der Größe der Dateien an, die für die Operation ausgewählt sind. Beispiel: Die Gesamtzahl der überprüften Byte für den folgenden Befehl ist die Anzahl der Byte, die auf dem Datenträger /Volumes/BUILD belegt sind: dsmc INCREMENTAL /Volumes/BUILD/* -SU=Yes
Gesamtzahl der Byte vor der Deduplizierung:	Gibt die Anzahl der Byte an, die an den IBM Spectrum Protect-Server gesendet werden sollen, wenn der Client redundante Daten nicht entfernt. Vergleichen Sie diesen Betrag mit Gesamtzahl der Byte nach der Deduplizierung. Beinhaltet die Metadatengröße und könnte größer sein als die Anzahl der überprüften Byte.
Gesamtzahl der Byte nach der Deduplizierung:	Gibt die Anzahl der Byte an, die nach der Deduplizierung der Dateien auf dem Client-Computer an den IBM Spectrum Protect-Server gesendet werden. Beinhaltet die Metadatengröße und könnte größer sein als die Anzahl der verarbeiteten Byte.
Gesamtzahl der verarbeiteten Byte:	Gibt die Summe der Größe der Dateien an, die für die Operation verarbeitet werden.

Tabelle 42. Informationsnachrichten der Clientbefehlszeile (Forts.)

Informationsnachricht	Bedeutung
Datenübertragungszeit:	<p>Die Summe der Zeiten, die jede Sicherungs-, Archivierungs-, Zurückschreibungs- oder Abrufsitzung benötigt, um Daten über das Netz zu senden. Dieser Wert umfasst weder die Zeit, die der Client benötigt, um die Daten von Platte zu lesen, bevor die Daten gesendet werden, noch die Zeit, die auf die Beendigung von Servertransaktionen gewartet werden muss.</p> <p>Dieser Wert kann größer als die abgelaufene Verarbeitungszeit sein, wenn die Operation für das Versetzen von Daten mehrere gleichzeitig ablaufende Sitzungen verwendet, wie beispielsweise Mehrfachsitzungssicherungs- und -zurückschreibungsoperationen.</p> <p>Dieser Wert umfasst die Zeit, die benötigt wird, um Daten aufgrund von Neuversuchen mehrmals zu senden, wenn sich beispielsweise eine Datei während einer Sicherungsoperation ändert.</p>
Datenübertragungsgeschwindigkeit im Netz:	Die Durchschnittsgeschwindigkeit, mit der im Netz Daten zwischen dem Client und dem Server übertragen werden. Dieser Statistikwert wird berechnet, indem die Gesamtzahl übertragener Byte durch die Zeit für die Übertragung der Daten über das Netz dividiert wird. Dieser Statistikwert umfasst weder die Zeit, die der Client benötigt, um die Daten von Platte zu lesen, bevor die Daten gesendet werden, noch die Zeit, die auf die Beendigung von Servertransaktionen gewartet werden muss.
Datenübertragungsgeschwindigkeit Gesamt:	Die Gesamtzahl Byte, die während einer Sicherungs-, Archivierungs-, Zurückschreibungs- oder Abrufoperation übertragen wurden, dividiert durch die abgelaufene Gesamtzeit der Operation.
Objekte komprimiert um:	Gibt den Prozentsatz der über das Netz gesendeten Daten an, geteilt durch die Originalgröße der Datei auf der Platte. Beispiel: Wenn die Netzdatenbyte 10 K betragen und die Datei 100 K groß ist, ist das Ergebnis für "Objekte komprimiert um": $== (1 - (10240/102400)) \times 100 == 90\%$.
Gesamtzahl größer gewordener Objekte:	Die Gesamtzahl Dateien, die infolge der Komprimierung größer wurden.
Reduzierung durch Deduplizierung:	Gibt die Größe der gefundenen doppelten Bereiche an, dividiert durch die ursprüngliche Dateigröße oder Datenmenge. Beispiel: Die ursprüngliche Objektgröße ist 100 MB und die Größe nach der Deduplizierung ist 25 MB. Die Reduzierung beträgt $(1 - 25/100) \times 100 = 75\%$.
Gesamtverhältnis der Datenreduktion:	Addiert die Auswirkungen der Teilsicherung und Komprimierung. Beispiel: Die Anzahl der überprüften Byte beträgt 100 MB und die Anzahl der gesendeten Byte beträgt 10 MB. Die Reduzierung beträgt $(1 - 10/100) \times 100 = 90\%$.
Verarbeitungszeit:	Die aktive Verarbeitungszeit für die Ausführung eines Befehls. Die Verarbeitungszeit wird berechnet, indem die Startzeit der Befehlsverarbeitung von der Endzeit der beendeten Befehlsverarbeitung abgezogen wird.
Gesamtanzahl übertragener Byte:	Die Gesamtzahl Byte, die während der Sicherungs-, Archivierungs-, Zurückschreibungs- oder Abrufoperation übertragen wurden. Dieser Wert umfasst Daten, die aufgrund von Neuversuchen mehrmals gesendet werden, wenn sich beispielsweise eine Datei während einer Sicherungsoperation ändert.
Übertragene LAN-unabhängige Byte:	Die Anzahl der Datenbyte, die bei einer LAN-unabhängigen Operation übertragen wurden. Ist die Option enablelanfree auf <i>no</i> gesetzt, wird diese Zeile nicht ausgegeben.
Gesamtzahl der überprüften Byte:	Die Summe der Größe der Dateien, die für die Operation ausgewählt sind.

Tabelle 42. Informationsnachrichten der Clientbefehlszeile (Forts.)

Informationsnachricht	Bedeutung
Gesamtzahl Neuversuche:	Die Gesamtzahl Neuversuche während einer Sicherungsoperation. Abhängig von den Einstellungen für das Nummerierungsattribut und der Option changingretries wird eine Datei, die von einem anderen Prozess geöffnet wird, möglicherweise beim ersten Sicherungsversuch nicht gesichert. Möglicherweise versucht der Client für Sichern/Archivieren während einer Sicherungsoperation mehrmals, eine Datei zu sichern. Diese Nachricht gibt die Gesamtzahl Neuversuche für alle Dateien an, die in die Sicherungsoperation eingeschlossen sind.

Sicherung (UNIX und Linux): Weitere Hinweise

Sie sollten einige besondere Situationen bedenken, bevor Sie Ihre Daten sichern.

Gespeicherte Dateien

Werden Dateien gesichert und archiviert, speichert IBM Spectrum Protect die Sicherungen und Archivierungen in einem Dateibereich im Speicher, der denselben Namen wie das Dateisystem oder der virtuelle Mountpunkt hat, aus dem die Dateien stammen.

Ist beispielsweise ein Dateisystem mit dem Namen `/home` vorhanden und wird eine Datei mit dem Namen `doc1` im Verzeichnis `/home/monnett` gesichert, speichert IBM Spectrum Protect die Datei in einem Dateibereich mit dem Namen `/home`. Wenn Sie `/home/monnett` später als virtuellen Mountpunkt definieren, werden alle Dateien, die aus dem Verzeichnis `/home/monnett` gesichert werden (z. B. `doc2`), in einem Dateibereich mit dem Namen `/home/monnett` gespeichert. Bei Eingabe des Befehls

```
dsmc query backup "/home/monnett/*"
```

sucht IBM Spectrum Protect nach Dateien in dem Dateibereich `/home/monnett`. Es wird immer nach einer Datei in dem Dateibereich mit dem längsten Namen gesucht, der mit der Dateispezifikation übereinstimmt, die in einem Befehl angegeben wird. Das Programm findet die Datei mit dem Namen `doc2`, die gesichert wurde, nachdem der virtuelle Mountpunkt definiert wurde. Die Datei `doc1` wird jedoch nicht gefunden, da diese Datei gesichert wurde, bevor der virtuelle Mountpunkt definiert wurde und die Sicherung in dem Dateibereich `/home` gespeichert wurde.

Um die Datei `doc1` mithilfe eines Befehls aufzulisten oder zurückzuschreiben, muss der Name des Dateibereichs explizit angegeben werden, indem er in geschweifte Klammern eingeschlossen wird. Beispiel:

```
dsmc query backup "{/home}/monnett/*"
dsmc restore {/home}/monnett/doc1
```

Wenn Sie anschließend den virtuellen Mountpunkt `/home/monnett` entfernen und dann weitere Dateien in dem Verzeichnis `/home/monnett` sichern, werden die Sicherungen erneut in dem Dateibereich `/home` gespeichert. Wird beispielsweise jetzt eine Datei mit dem Namen `doc3` im Verzeichnis `/home/monnett` gesichert, wird sie in dem Dateibereich `/home` gespeichert. Sie wird nicht in dem vorhandenen Dateibereich `/home/monnett` gespeichert.

Da jedoch der Dateibereich `/home/monnett` bei dem Versuch, die Datei `doc3` abzufragen oder zurückzuschreiben, bereits vorhanden ist, sucht IBM Spectrum Protect in dem Dateibereich `/home/monnett` nach der Datei, es sei denn, der korrekte Dateibereichsname wird angegeben. Zum Beispiel:

```
dsmc query backup "{/home}/monnett/*"  
dsmc restore {/home}/monnett/doc2
```

Anmerkung: Der Dateibereichsname muss nur dann explizit angegeben werden, wenn die eingegebene Dateispezifikation mehrere Auflösungen zulässt.

Sind z. B. die Dateibereiche

```
/home  
/home/monnett  
/home/monnett/project1  
/home/monnett/project1/planning
```

im Speicher vorhanden, Folgendes eingeben:

```
dsmc query backup "/home/monnett/project1/planning/*"
```

IBM Spectrum Protect sucht nur in dem Dateibereich `/home/monnett/project1/planning` nach Dateien, auch wenn einer oder mehrere der anderen Dateibereiche einen Pfad mit demselben Namen enthalten. Wird aber einer der folgenden Befehle eingegeben:

```
dsmc query backup "{/home}/monnett/project1/planning/*"  
dsmc query backup "{/home/monnett}/project1/planning/*"  
dsmc query backup "{/home/monnett/project1}/planning/*"
```

sucht IBM Spectrum Protect nur im Dateibereich `/home`, im Dateibereich `/home/monnett` oder im Dateibereich `/home/monnett/project1` nach Dateien, je nach verwendeter Form.

Spezielle Dateisysteme

Spezielle Dateisysteme enthalten dynamische Informationen, die vom Betriebssystem generiert werden; sie enthalten jedoch keine Daten oder Dateien. Der Client für Sichern/Archivieren ignoriert spezielle Dateisysteme und ihren Inhalt.

Spezielle Dateisysteme umfassen Folgendes:

- Das Dateisystem `/proc` auf den meisten UNIX-Plattformen
- Das Dateisystem `/dev/fd` unter Solaris
- `/dev/pts` unter Linux

NFS- oder virtuelle Mountpunkte

Wenn Dateien von einem Dateisystem oder virtuellen Mountpunkt gesichert und archiviert werden, folgt der Client nicht den verschachtelten NFS- oder virtuellen Mountpunkten (sofern derartige Mountpunkte in einem Dateisystem definiert sind). Die verschachtelten NFS- oder virtuellen Mountpunkte werden nicht gesichert oder archiviert.

Verwaltungsklassen

IBM Spectrum Protect bestimmt mithilfe von Verwaltungsklassen, wie die Sicherungen auf dem Server verwaltet werden.

Bei jeder Sicherung einer Datei wird ihr eine Verwaltungsklasse zugeordnet. Bei der verwendeten Verwaltungsklasse kann es sich um die Standardverwaltungs-k-lasse handeln oder um eine Verwaltungsklasse, die der Datei mit der Option `include` in der Einschluss-/Ausschlussoptionsliste zugeordnet wird. Die ausgewählte Verwaltungsklasse muss eine Sicherungskopiengruppe enthalten, damit die Datei gesichert wird.

Wählen Sie **Dienstprogramme** → **Maßnahmeninformationen anzeigen** in der GUI des Clients für Sichern/Archivieren aus, um die Sicherungsmaßnahmen anzuzeigen, die vom IBM Spectrum Protect-Server für Ihren Clientknoten definiert wurden.

Zugehörige Konzepte:

Kapitel 9, „Speicherverwaltungsmaßnahmen“, auf Seite 309

Symbolische Verbindungen sichern

Der Client für Sichern/Archivieren verfährt beim Sichern symbolischer Verbindungen anders als bei regulären Dateien und Verzeichnissen.

Wie der Client symbolische Verbindungen sichert, ist von Optionseinstellungen, von der Verfügbarkeit des Zielverzeichnisses und von der Angabe der Objekte abhängig.

Eine *symbolische Verbindung* ist unter *UNIX* eine Datei, die einen Zeiger auf eine andere Datei oder ein anderes Verzeichnis enthält. Das Objekt, auf das die symbolische Verbindung zeigt, wird als Zielobjekt bezeichnet.

Eine symbolische Verbindung kann entweder als Pfadangabe für das Zielverzeichnis oder als Verzeichnis gesichert werden. Wird die symbolische Verbindung als Verzeichnis gesichert, können auch die Dateien und Ordner im Zielverzeichnis gesichert werden.

Anmerkung: Die hier beschriebene Verarbeitung symbolischer Verbindungen gilt nicht für Mac OS X. Symbolische Verbindungen werden immer als Dateien gesichert und den Zeigern wird nicht gefolgt.

Zugehörige Verweise:

„Archsymlinkasfile“ auf Seite 358

„Followsymbolic“ auf Seite 458

„Virtualmountpoint“ auf Seite 630

Beispiele: Teilsicherung oder selektive Sicherung von symbolischen Verbindungen

Wie der Client eine symbolische Verbindung sichert, ist davon abhängig, ob das Ziel der symbolischen Verbindung eine Datei oder ein Verzeichnis ist und wie Sie die symbolische Verbindung in dem Befehl für die Teilsicherung oder selektive Sicherung angeben.

Wenn eine symbolische Verbindung auf eine Datei zeigt, sichert der Client nur die Pfadangabe. Der Client sichert keine Datei, die das Ziel einer symbolischen Verbindung ist.

Wenn eine symbolische Verbindung auf ein Verzeichnis zeigt, ist die Sicherung davon abhängig, wie das Verzeichnis im Befehl angegeben ist.

Wird ein Verzeichnis in einem Befehl für selektive Sicherung oder Teilsicherung mit einem abschließenden Schrägstrich angegeben, sichert der Client die symbolische Verbindung als Verzeichnis und sichert den Inhalt des Zielverzeichnisses.

Wird die symbolische Verbindung ohne abschließenden Schrägstrich eingegeben oder wird eine symbolische Verbindung nicht explizit in einer Dateispezifikation für die Sicherung angegeben, sichert der Client nur die Pfadangabe für das Zielverzeichnis. Der Inhalt des Zielverzeichnisses wird nicht gesichert.

Für die folgenden Beispiele wird angenommen, dass `symdir` eine symbolische Verbindung zu dem Zielverzeichnis `/fs1/guest/` ist. `/fs1/guest/` enthält die folgenden Objekte:

```
/fs1/guest/file (eine Datei)
/fs1/guest/dir1 (ein Verzeichnis)
/fs1/guest/dir1/file1 (eine Datei)
```

Beispiel 1

```
dsmc incr /home/gillis/symdir/
```

In diesem Beispiel sichert der Client die symbolische Verbindung als Verzeichnis und sichert den Inhalt des Zielverzeichnisses `/fs1/guest/`. Wenn Sie die Option `subdir=yes` angeben, sichert der Client die Unterverzeichnisse von `/fs1/guest/`.

Beispiel 2

```
dsmc incr /home/gillis/symdir/dir1
```

Beispiel 3

```
dsmc incr /home/gillis/symdir/dir1/
```

In den Beispielen 2 und 3 sichert der Client die symbolische Verbindung als Verzeichnis und sichert das Unterverzeichnis `/dir1/` des Zielverzeichnisses. Die Angabe des abschließenden Schrägstrichs spielt nur für die symbolische Verbindung eine Rolle; sie ist bei den Unterverzeichnissen der symbolischen Verbindung nicht relevant. Wenn Sie die Option `subdir=yes` angeben, sichert der Client die Unterverzeichnisse von `/fs1/guest/dir1`. Auf dem IBM Spectrum Protect-Server gespeicherte Sicherungskopien haben einen Pfad wie `/home/gillis/symdir/dir1/file1`.

Beispiel 4

```
dsmc incr /home/gillis/symdir
```

In Beispiel 4 sichert der Client nur den Pfad zu dem Zielverzeichnis, da die symbolische Verbindung keinen abschließenden Schrägstrich enthält. Der Client sichert die symbolische Verbindung nicht als Verzeichnis und sichert keine Dateien oder Ordner im Zielverzeichnis.

Beispiel 5

```
dsmc incr /home/gillis/
```

In Beispiel 5 sichert der Client nur den Pfad zu dem Zielverzeichnis, da die symbolische Verbindung nicht explizit in der Dateispezifikation für die Sicherung angegeben ist. Der Client sichert die symbolische Verbindung nicht als Verzeichnis und sichert keine Dateien oder Ordner im Zielverzeichnis.

Einschränkung: Wenn Sie eine symbolische Verbindung als Verzeichnis sichern, in einer zukünftigen Teilsicherung diese symbolische Verbindung jedoch nicht als Verzeichnis sichern, verfallen diese als Verzeichnis gesicherte symbolische Verbindung sowie die Dateien und Verzeichnisse in diesem Verzeichnis.

Beispiel: Angenommen, Sie sichern die symbolische Verbindung `symdir` zunächst als Verzeichnis und sichern den Inhalt des Zielverzeichnisses. Der in Beispiel 1 angegebene Befehl führt diese Operation aus. Der Client erstellt Sicherungskopien mit dem übergeordneten Pfad `/home/gillis/symdir/`. In diesem Beispiel erstellt der Client Sicherungskopien mit den folgenden Pfaden:

```
/home/gillis/symdir/
/home/gillis/symdir/file
/home/gillis/symdir/dir1
```

/home/gillis/symdir/dirl/file1

Der Inhalt von /home/gillis wird mit dem folgenden Befehl gesichert:

```
dsmc inc /home/gillis/ -subdir=yes
```

Dieser Befehl verarbeitet den Wert `symdir` als symbolische Verbindung und verarbeitet nicht die Objekte, auf die die symbolische Verbindung zeigt. Daher kennzeichnet der Client Sicherungskopien im Verzeichnis `/home/gillis/symdir/`, die in Beispiel 1 erstellt wurden, als verfallen.

Teilsicherung nur für eine Domäne

Der Client sichert eine symbolische Verbindung während einer Teilsicherung der Domäne, wenn die symbolische Verbindung als virtueller Mountpunkt definiert und die Option `followsymbolic` auf `yes` gesetzt ist.

Der Client sichert eine symbolische Verbindung und das Zielverzeichnis, wenn alle folgenden Bedingungen erfüllt sind:

- Der Client führt eine Teilsicherung der Domäne aus.
- Die symbolische Verbindung ist mit der Option `virtualmountpoint` als virtueller Mountpunkt definiert.
- `followsymbolic=yes`

Die Optionen `virtualmountpoint` und `followsymbolic` fügen der Domäne die symbolische Verbindung hinzu. Der Befehl **incremental** sichert die Domäne, die das Ziel der symbolischen Verbindung umfasst.

Zugehörige Verweise:

„Followsymbolic“ auf Seite 458

„Virtualmountpoint“ auf Seite 630

Feste Verbindungen

Wenn Sie Dateien sichern, die fest verbunden sind, sichert der Client für Sichern/Archivieren jede Instanz der fest verbundenen Datei.

Wenn Sie beispielsweise zwei Dateien sichern, die fest verbunden sind, sichert der Client die Dateidaten zweimal.

Wenn Sie fest verbundene Dateien zurückschreiben, versucht der Client, die Verbindungen wiederherzustellen. Hatten Sie beispielsweise ein Dateipaar mit fester Verbindung und ist nur eine der fest verbundenen Dateien auf Ihrer Workstation, werden beide Dateien beim Zurückschreiben fest verbunden. Werden beide Dateien zusammen mit einem einzigen Befehl zurückgeschrieben, werden die Dateien auch dann fest verbunden, wenn keine der Dateien zum Zeitpunkt der Zurückschreibung vorhanden ist. Bei diesem Verfahren gibt es eine Ausnahme, und zwar, wenn Sie zwei fest verbundene Dateien sichern und dann die Verbindung zwischen diesen Dateien auf der Workstation unterbrechen. Wenn Sie die beiden Dateien über den Standardzurückschreibungsprozess (oder klassischen Zurückschreibungsprozess) vom Server zurückschreiben, respektiert der Client das aktuelle Dateisystem und stellt die feste Verbindung nicht wieder her.

Wichtig: Wenn nicht alle fest verbundenen Dateien gleichzeitig gesichert oder zurückgeschrieben werden, können Probleme auftreten. Um sicherzustellen, dass fest verbundene Dateien synchronisiert bleiben, führen Sie die Sicherung und den Zurückschreibung fest verbundener Dateien immer gleichzeitig durch.

Dateien mit freien Bereichen

Dateien mit freien Bereichen haben keinen Plattenspeicherplatz für jeden Block im gesamten Adressraum zugeordnet, was zu freien Datenbereichen innerhalb der Datei führt. Freie Datenbereiche werden durch ihren Inhalt erkannt, der immer Null ist, und diese Nullen nehmen Speicherplatz ein.

Standardwert ist, die Datei mit freien Bereichen ohne die freien Datenbereiche zurückzuschreiben, was mehr freien Plattenspeicherplatz lassen würde. Der Client für Sichern/Archivieren erkennt Dateien mit freien Bereichen während einer Sicherungsoperation und markiert sie als solche auf dem IBM Spectrum Protect-Server.

Anmerkung: Dateien mit freien Bereichen gelten nicht für Mac OS X.

Der Client für Sichern/Archivieren sichert eine Datei mit freien Bereichen als reguläre Datei, wenn die Clientkomprimierung inaktiviert ist.

Zugehörige Verweise:

„Compression“ auf Seite 380

„Makesparsefile“ auf Seite 501

Absolute und bedingte NFS-Mounts

Wenn der Client für Sichern/Archivieren die Verbindung zu einem NFS-Dateisystem herstellt, kann entweder ein absoluter Mount oder ein bedingter Mount verwendet werden.

Der Client bestimmt mithilfe des Werts für die Option **nfsttimeout** die Wartezeit für eine Antwort auf einen NFS-Systemaufruf, bevor eine Zeitlimitüberschreitung auftritt; diese Einstellung gilt für absolute und bedingte Mounts. Der Standardwert ist 0 Sekunden. Dies bedeutet, dass der Client das Standardverhalten von NFS-Systemaufrufen verwendet.

Sie sollten sich über die Auswirkungen absoluter und bedingter Mounts im Klaren sein, falls der Mount nicht mehr aktuell ist (wenn beispielsweise der Server für das Dateisystem nicht mehr verfügbar ist).

Absoluter Mount

Bei einem NFS-Dateisystem mit absolutem Mount versuchen die NFS-Dämonen ständig, mit dem Server Verbindung aufzunehmen. Für die Neuversuche der NFS-Dämonen tritt keine Zeitlimitüberschreitung auf, sie beeinträchtigen die Systemleistung und der Benutzer kann sie nicht unterbrechen; die Steuerung wird jedoch an den Client zurückgegeben, wenn der Wert für **nfsttimeout** erreicht ist.

Bedingter Mount

Bei einem NFS-Dateisystem mit bedingtem Mount versucht NFS so lange mit dem Server Verbindung aufzunehmen, bis eine der folgenden Situationen eintritt:

- Eine Verbindung wird aufgebaut
- Die NFS-Wiederholungsschwelle wird erreicht
- Der Wert für **nfsttimeout** wird erreicht

Tritt eines dieser Ereignisse ein, wird die Steuerung an das aufrufende Programm zurückgegeben.

Anmerkung: Auf UNIX- und Linux-Systemen kann die Option **nfsttimeout** fehlschlagen, wenn der NFS-Mount ein absoluter Mount ist. Tritt eine Blo-

ckierung auf, müssen Sie die Option **nfstimeout** inaktivieren und das NFS-Dateisystem wie folgt mit einem bedingten Mount anhängen:

```
mount -o soft,timeo=5,retry=5 machine:/filesystem /mountpoint
```

Die Parameter sind wie folgt definiert:

soft Generiert einen bedingten Mount des NFS-Dateisystems. Tritt ein Fehler auf, gibt die Funktion **stat()** einen Fehler zurück. Wird die Option **hard** verwendet, gibt **stat()** erst dann einen Rückkehrcode aus, wenn das Dateisystem verfügbar ist.

timeo=n Setzt das Zeitlimitintervall für den Fehler eines bedingten Mounts auf *n* Zehntel einer Sekunde.

retry=n Legt die Anzahl der Mountversuche fest (hierbei ist *n* eine ganze Zahl). Der Standardwert ist 10000.

Gelöschte Dateisysteme

Wenn ein Dateisystem oder Laufwerk gelöscht wurde oder nicht mehr vom Client für Sichern/Archivieren gesichert wird, werden die vorhandenen Sicherungsversionen für jede Datei gemäß den folgenden Maßnahmenattributen verwaltet: Anzahl Tage für die Aufbewahrung inaktiver Sicherungsversionen und Anzahl Tage für die Aufbewahrung der letzten Sicherungsversion (falls keine aktive Version vorhanden ist).

Wenn Sie nichts weiter unternehmen, verbleiben aktive Sicherungsversionen unbegrenzt. Falls Sie die aktiven Versionen nicht unbegrenzt aufbewahren müssen, können Sie mit dem Befehl **expire** die aktiven Versionen inaktivieren.

Wenn Sie keine der aktiven Versionen aufbewahren müssen, können Sie mit dem Befehl **delete backup** alle Sicherungsversionen im Dateibereich löschen. Ihr IBM Spectrum Protect-Serveradministrator muss Ihnen die Berechtigung zur Verwendung dieses Befehls geben. Mithilfe des Befehls **query session** können Sie feststellen, ob Sie die Berechtigung "delete backup" besitzen. Alternativ dazu können Sie Ihren IBM Spectrum Protect-Serveradministrator bitten, den Dateibereich für Sie zu löschen.

Zugehörige Konzepte:

Kapitel 9, „Speicherverwaltungsmaßnahmen“, auf Seite 309

Geöffnete Dateien

Der Client für Sichern/Archivieren sucht nach Dateien, die sich zwischen dem Start und dem Ende der Dateisicherung geändert haben.

Einige Dateien auf Ihrem System sind möglicherweise im Gebrauch oder geöffnet, wenn Sie versuchen, sie zu sichern. Da sich eine offene Datei ändern kann, spiegelt eine Sicherungsaktion den Inhalt der Datei zu einem bestimmten Zeitpunkt nicht korrekt wider.

Überlegen Sie, ob die Datei wichtig ist und ob sie sie erneut erstellen können. Wenn die Datei nicht wichtig ist, ist eine Sicherung eventuell nicht erforderlich. Wenn die Datei wichtig ist, kann ein Root auf Ihrer Workstation sicherstellen, dass die Datei vor dem Sichern geschlossen wird.

Werden die Sicherungen nach einem Zeitplan ausgeführt, kann ein Root mit der Option `preschedulecmd` einen Befehl eingeben, der die Datei schließt. Handelt es sich bei der offenen Datei beispielsweise um eine Datenbank, verwenden Sie den Befehl **quiesce** der Datenbank, um sie zu beenden. Nach Beendigung der Sicherung kann ein Root die Anwendung, die die Datei verwendet, mit der Option `postschedulecmd` erneut starten. Wird kein Zeitplan für die Sicherung verwendet, muss die Anwendung, die die Datei verwendet, vor Beginn der Sicherung geschlossen werden.

Der Client kann die Datei selbst dann sichern, wenn sie während der Sicherung offen ist und geändert wird. Dies ist nur sinnvoll, wenn die Datei noch verwendbar ist, auch wenn sie sich während der Sicherung ändert. Damit diese Dateien gesichert werden, muss ihnen eine Verwaltungsklasse mit der Durchnummerierung *Dynamisch* oder *Gemeinsam dynamisch* zugeordnet werden.

Zugehörige Konzepte:

„Informationen zu Verwaltungsklassen und Kopiengruppen anzeigen“ auf Seite 311

„Verwaltungsklasse für Dateien auswählen“ auf Seite 315

Platzhalterzeichen

Beim Client für Sichern/Archivieren können die Platzhalterzeichen des Betriebssystems in Dateispezifikationen verwendet werden. Mithilfe dieser Zeichen können Gruppen von Dateien mit ähnlichen Namen ausgewählt werden.

In einem Befehl können Platzhalterzeichen nur innerhalb des Dateinamens oder innerhalb der Erweiterung verwendet werden. Sie können nicht für Zieldateien, Dateisysteme oder Verzeichnisse angegeben werden. Werden Platzhalterzeichen in einem anderen Modus als dem Schleifenmodus verwendet, wie z. B. in `dsmc sel "/home/ledger.*"`, muss der Parameter, der den Stern enthält, in Anführungszeichen gesetzt werden, um sicherzustellen, dass das System das Platzhalterzeichen nicht interpretiert und unerwartete Ergebnisse liefert. Die folgende Tabelle enthält Informationen über Platzhalterzeichen.

Wichtig: Verwenden Sie einen Stern (*) statt eines Fragezeichens (?) als Platzhalterzeichen, wenn Sie nach einer Übereinstimmung mit einem Muster in einer Mehrfachbyte-Codepage suchen, um unerwartete Ergebnisse zu verhindern.

Die folgende Tabelle zeigt einige Platzhalterzeichenmuster und ihre Angabe.

<i>* (Stern)</i>	Null oder mehr Zeichen, die Dateien mit folgenden Merkmalen entsprechen:
*.cpp	Dateinamen mit der Erweiterung <code>cpp</code>
hm*.*	Dateinamen, die mit <code>hm</code> beginnen und eine beliebige Erweiterung haben, aber das Zeichen <code>'.'</code> aufweisen müssen
hm*	Dateinamen, die mit <code>hm</code> beginnen und eine Erweiterung haben können oder nicht
h.*	Dateinamen mit einem <code>h</code> an einer beliebigen Position im Dateinamen und mit einer beliebigen Erweiterung, die aber einen <code>.</code> aufweisen müssen
<i>? (Fragezeichen)</i>	Ein Zeichen, das Dateien mit folgenden Merkmalen entspricht:
?cpp	Dateinamen mit der Erweiterung <code>cpp</code> , die aus nur einem einzigen Zeichen bestehen

<i>? (Fragezeichen)</i>	Ein Zeichen, das Dateien mit folgenden Merkmalen entspricht:
hm?.cpp	Dreistellige Dateinamen, die mit hm beginnen und die Erweiterung cpp haben
<i>* ? (Stern und Fragezeichen)</i>	Kombinationen aus Stern und Fragezeichen, die Dateien mit folgenden Merkmalen entsprechen:
??hm.*	Vierstellige Dateinamen, die mit hm. enden und eine beliebige Erweiterung haben

In einem Pfadnamen für eine Dateispezifikation kann kein Verzeichnis angegeben werden, dessen Name einen Stern (*) oder ein Fragezeichen (?) enthält. Der Client erkennt diese Zeichen nur als Platzhalterzeichen.

Kapitel 5. Daten zurückschreiben

Mit IBM Spectrum Protect können Sicherungsversionen bestimmter Dateien, einer Gruppe von Dateien mit ähnlichen Namen oder vollständiger Verzeichnisse zurückgeschrieben werden.

Sie können diese Sicherungsversionen zurückschreiben, wenn die ursprünglichen Dateien verloren gegangen oder beschädigt sind. Wählen Sie die zurückzuschreibenden Dateien mithilfe einer Dateispezifikation (Pfad, Name und Erweiterung der Datei), einer Verzeichnisliste oder mithilfe eines Unterverzeichnispfads zu einem Verzeichnis und seinen Unterverzeichnissen aus.

Alle Sicherungs- und Zurückschreibungsprozeduren des Clients, auf die in diesem Abschnitt verwiesen wird, gelten auch für den Web-Client. Der Web-Client verfügt jedoch über keinen Profileditor, mit dem Clientoptionen definiert werden können.

Achtung: Schreiben Sie keine Betriebssystemdateien, wie z. B. Basissystemverzeichnisse, Kernelmodule oder Programmkorrekturen, an ihre ursprüngliche Position zurück, während das Dateisystem ausgeführt wird. Das Betriebssystem könnte blockieren oder ausfallen.

Die folgenden Tasks sind die primären Zurückschreibungstasks:

- „Image zurückschreiben“
- „Daten über die grafische Benutzerschnittstelle zurückschreiben“ auf Seite 267
- „Beispiele für Zurückschreibungsbefehle“ auf Seite 268
- „Daten aus einem Sicherungssatz zurückschreiben“ auf Seite 250
- „Daten nach Zeitpunkt zurückschreiben“ auf Seite 260
- „NAS-Dateisysteme zurückschreiben“ auf Seite 264
- „Einen anderen Benutzer zum Zurückschreiben und Abrufen Ihrer Dateien berechtigen“ auf Seite 274
- „Dateien von einem anderen Clientknoten zurückschreiben oder abrufen“ auf Seite 275
- „Dateien auf eine andere Workstation zurückschreiben oder abrufen“ auf Seite 276
- „Platte nach Plattenverlust zurückschreiben“ auf Seite 277
- „Dateibereiche löschen“ auf Seite 277

Die Veröffentlichung *IBM Spectrum Protect for Space Management for UNIX and Linux* enthält Details über das Zurückschreiben umgelagerter Dateien und die Option `restoremigstate`.

Zugehörige Tasks:

„Web-Client-Sitzung starten“ auf Seite 158

Image zurückschreiben

Einige Punkte sind zu berücksichtigen, bevor Sie mit der Zurückschreibung von Images auf Ihr System beginnen.

Damit Sie eine Imagezurückschreibung (offline oder online) ausführen können, benötigen Sie die Administratorberechtigung auf dem System.

Beachten Sie die folgende Liste von Hinweisen, bevor Sie ein Image zurückschreiben:

- Durch das Zurückschreiben des Image eines Datenträgers werden die Daten in denselben Zustand zurückgeschrieben, den sie hatten, als die letzte Imagesicherung ausgeführt wurde. Sie müssen absolut sicher sein, dass Sie ein Image zurückschreiben müssen, da Ihr gesamtes aktuelles Dateisystem oder der unformatierte Datenträger durch das Image auf dem Server ersetzt wird.
- Stellen Sie sicher, dass der Datenträger, auf den Sie das Image zurückschreiben, mindestens so groß ist wie das Image, das zurückgeschrieben wird.
- Auf Linux-Systemen verwenden einige Dateisysteme (z. B. ext2, ext3, ext4, btrfs und xfs) eine UUID (Universally Unique Identifier), um sich selbst im Betriebssystem zu identifizieren. Wenn Sie eine Imagesicherung eines solchen Datenträgers erstellen und an eine andere Position zurückschreiben, kann es sein, dass es zwei Datenträger mit derselben UUID gibt. Wenn Sie Ihre Dateisysteme mit einer UUID in /etc/fstab definieren, denken Sie daran, dass der Client für Sichern/Archivieren das zurückgeschriebene Dateisystem unter Umständen wegen eines UUID-Konflikts nicht korrekt anhängen kann. Um diese Situation zu vermeiden, sollten Sie das Image an seine ursprüngliche Position zurückschreiben. Wenn Sie es an eine andere Position zurückschreiben müssen, ändern Sie die UUID des ursprünglichen oder des zurückgeschriebenen Datenträgers, bevor Sie das zurückgeschriebene Dateisystem anhängen. Informationen zur Änderung einer UUID finden Sie in der Linux-Dokumentation. Möglicherweise müssen Sie auch die Datei /etc/fstab manuell bearbeiten, damit der ursprüngliche Datenträger und/oder der zurückgeschriebene Datenträger angehängt werden können.
- Das Dateisystem oder der Datenträger, in das bzw. auf den zurückgeschrieben wird, muss denselben Typ wie das Original haben.
- Stellen Sie sicher, dass der Zieldatenträger für die Zurückschreibung nicht im Gebrauch ist. Der Client sperrt den Datenträger, bevor die Zurückschreibung gestartet wird. Der Client entsperrt den Datenträger, wenn die Zurückschreibung beendet ist. Wird der Datenträger verwendet, wenn der Client versucht, das Dateisystem zu sperren, schlägt die Zurückschreibung fehl.
- Sie können ein Image nicht an eine Position zurückschreiben, auf der das IBM Spectrum Protect-Clientprogramm installiert ist.
- Wurden fortlaufende Teilsicherungen *und* Imagesicherungen des Dateisystems ausgeführt, können Sie eine Imageteilzurückschreibung des Dateisystems ausführen. Bei dem Prozess werden einzelne Dateien zurückgeschrieben, nachdem das vollständige Image zurückgeschrieben wurde. Die einzelnen zurückgeschriebenen Dateien sind die Dateien, die nach dem ursprünglichen Image gesichert wurden. Wurden Dateien nach der ursprünglichen Sicherung gelöscht, können diese Dateien bei der Teilzurückschreibung wahlweise aus dem Basisimage gelöscht werden.

Das Löschen von Dateien wird ordnungsgemäß ausgeführt, wenn die Sicherungskopiengruppe des IBM Spectrum Protect-Servers über genügend Versionen für vorhandene und gelöschte Dateien verfügt. Teilsicherungen und -zurückschreibungen können nur für angehängte Dateisysteme und nicht für unformatierte logische Datenträger ausgeführt werden.

- Sollte ein zurückgeschriebenes Image aus irgendeinem Grund beschädigt sein, können Sie versuchen, es mit dem Tool fsck zu reparieren.

Sie können die Option `verifyimage` im Befehl **restore image** verwenden, um anzugeben, dass die Feststellung von defekten Sektoren auf dem Zieldatenträger

aktiviert werden soll. Werden defekte Sektoren auf dem Zieldatenträger festgestellt, gibt der Client eine Warnung auf der Konsole und im Fehlerprotokoll aus. Befinden sich defekte Sektoren auf dem Zieldatenträger, können Sie die Option **imagetofile** im Befehl **restore image** verwenden, um anzugeben, dass das Quellenimage in eine Datei zurückgeschrieben werden soll. Später können Sie ein Datenkopierprogramm Ihrer Wahl verwenden, um das Image von der Datei auf einen Plattendatenträger zu übertragen.

Zugehörige Verweise:

„Imagetofile“ auf Seite 470

„Verifyimage“ auf Seite 629

Image über die GUI zurückschreiben

Sie können die GUI verwenden, um ein Image Ihres Dateisystems oder unformatierten logischen Datenträgers zurückzuschreiben.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um ein Image Ihres Dateisystems oder unformatierten logischen Datenträgers zurückzuschreiben:

Vorgehensweise

1. Klicken Sie auf **Zurückschreiben** im Hauptfenster. Das Fenster 'Zurückschreiben' wird angezeigt.
2. Verzeichnisebenen der Verzeichnisbaumstruktur einblenden.
3. Lokalisieren Sie das Objekt in der Baumstruktur mit dem Namen **Image** und erweitern Sie das Objekt. Klicken Sie auf das Auswahlfeld neben dem Image, das Sie zurückschreiben wollen. Detaillierte Informationen über das Objekt erhalten Sie, wenn Sie das Objekt hervorheben und **Sicht → Dateiinformationen...** im Hauptfenster auswählen oder auf die Schaltfläche **Dateiinformationen anzeigen** klicken.
4. **(Optional)** Zum Ausführen einer Imageteilzurückschreibung klicken Sie auf die Schaltfläche **Optionen**, um das Fenster für Zurückschreibungsoptionen aufzurufen. Wählen Sie dann die Option **Image plus Teilsicherung von Verzeichnissen und Dateien** aus. Möchten Sie inaktive Dateien aus Ihrem lokalen Dateisystem löschen, wählen Sie das Kontrollkästchen **Inaktive Dateien von Lokal löschen** aus. Klicken Sie auf die Schaltfläche **OK**.
5. Klicken Sie auf **Zurückschreiben**. Das Fenster 'Zurückschreibungsziel' wird angezeigt. Das Image kann auf den Datenträger mit dem Mountpunkt zurückgeschrieben werden, von dem es ursprünglich gesichert wurde. Alternativ kann ein anderer Datenträger als Zurückschreibungsziel ausgewählt werden.
6. Klicken Sie auf die Schaltfläche **Zurückschreiben**, um die Zurückschreibung zu starten. Das Fenster **Taskliste** erscheint, das den Fortschritt der Zurückschreibung anzeigt. Das Fenster 'Zurückschreibungsbericht' zeigt einen ausführlichen Statusbericht an.

Ergebnisse

Die folgenden Hinweise sind zu beachten, wenn Sie eine Imagezurückschreibung über die GUI ausführen:

- Sie können **Sicht → Dateiinformationen** im Hauptfenster auswählen oder auf die Schaltfläche **Dateiinformationen anzeigen** klicken, um die folgenden Statistiken über Dateisystemimages anzuzeigen, die vom Client gesichert wurden:

- Imagegröße - Dies ist die Größe des Datenträgers, der gesichert wurde.
- Gespeicherte Größe - Dies ist die Größe des Image, das tatsächlich auf dem Server gespeichert wurde. Das auf dem IBM Spectrum Protect-Server gespeicherte Image hat dieselbe Größe wie der Datenträger.
- Dateisystemtyp
- Sicherungsdatum und -zeit
- Die der Imagesicherung zugeordnete Verwaltungsklasse
- Ob die Imagesicherung eine aktive oder inaktive Kopie ist
- Um bestimmte Zurückschreibungsoptionen zu ändern, klicken Sie auf die Schaltfläche **Optionen**. Die geänderten Optionen sind *nur* während der aktuellen Sitzung wirksam.
- Im Fenster für Zurückschreibungsoptionen können Sie auswählen, ob Sie nur das Image oder zusätzlich die über Teilsicherung gesicherten Verzeichnisse und Dateien zurückschreiben wollen. Wenn Sie **Nur Image** auswählen, wird nur das Image von Ihrer letzten Imagesicherung zurückgeschrieben. Dies ist der Standardwert.

Haben Sie jedoch Imageteilsicherung nach Datum für einen Datenträger oder Imagesicherungen auf einem über Teilsicherungen gesicherten Datenträger ausgeführt, können Sie die Option **Image plus Teilsicherung von Verzeichnissen und Dateien** auswählen. Wenn Sie **Image plus Teilsicherung von Verzeichnissen und Dateien** auswählen, können Sie auch **Inaktive Dateien von Lokal löschen** auswählen, um inaktive Dateien zu löschen, die in Ihr lokales Dateisystem zurückgeschrieben werden. Haben Sie für das Dateisystem als einzigen Teilsicherungstyp Imageteilsicherung nach Datum ausgeführt, werden keine Dateien gelöscht.

Wichtig: Sie müssen absolut sicher sein, dass Sie eine Teilzurückschreibung ausführen müssen, da Ihr gesamtes Dateisystem durch das Image auf dem Server ersetzt wird und anschließend die Dateien zurückgeschrieben werden, die Sie mit der Imageteilsicherungsoperation gesichert haben.

Image über die Befehlszeile zurückschreiben

Verwenden Sie den Befehl **restore image**, um ein Image über den IBM Spectrum Protect-Befehlszeilenclient zurückzuschreiben.

Zugehörige Verweise:

„Imagetofile“ auf Seite 470

„Verifyimage“ auf Seite 629

Daten aus einem Sicherungssatz zurückschreiben

Ihr IBM Spectrum Protect-Administrator kann einen Sicherungssatz (d. h. eine Sammlung Ihrer Dateien, die sich auf dem Server befinden) auf Wechseldatenträgern generieren und diese auf einer Einheit mit einem Format erstellen, das mit der Clienteinheit kompatibel ist.

Sie können die Daten aus einem Sicherungssatz vom IBM Spectrum Protect-Server zurückschreiben oder aus einem Sicherungssatz, der lokal als Datei oder auf einer Bandeinheit verfügbar ist.

Sie können Sicherungssätze von folgenden Positionen zurückschreiben:

- Vom IBM Spectrum Protect-Server

- Von Wechseldatenträgern auf einer Einheit, die an Ihre Client-Workstation angeschlossen ist
- Von einer Sicherungssatzdatei auf Ihrer Client-Workstation

Sicherungssätze ermöglichen wie in der nachfolgenden Liste beschrieben die sofortige Archivierung und schnelle Wiederherstellung.

Sofortarchivierung

Diese Fähigkeit erlaubt es einem Administrator, eine Archivierungssammlung aus Sicherungsversionen zu erstellen, die bereits auf dem Server gespeichert sind.

Schnelle Wiederherstellung mit lokalen Sicherungssätzen

In der Regel werden Zurückschreibungen von normalen Dateisicherungen ausgeführt, die auf dem IBM Spectrum Protect-Server außerhalb von Sicherungssätzen gespeichert sind. Mit dieser Zurückschreibungsmethode können Sie die neueste Sicherungsversion jeder Datei zurückschreiben. Ein Sicherungssatz enthält möglicherweise nicht die neueste Sicherungsversion Ihrer Dateien.

In manchen Fällen stellt die Zurückschreibung von Daten aus einem Sicherungssatz eine bessere Option als die Zurückschreibung von Daten aus normalen Sicherungsdateien auf dem IBM Spectrum Protect-Server dar. Die Zurückschreibung aus einem Sicherungssatz kann aus folgenden Gründen eine bessere Option sein:

- Die Zurückschreibung aus einem Sicherungssatz kann schneller sein, da alle für die Zurückschreibung erforderlichen Dateien sich zusammen auf einer kleineren Anzahl von Speicherdatenträgern befinden.
- Ein Sicherungssatz stellt eine Sammlung von Dateien nach Zeitpunkt dar. Sie können eine zeitpunktgesteuerte Zurückschreibung ausführen, während Sie bei einer normalen Zurückschreibung auf Dateiebene vom Server den aktuellen Stand zurückschreiben.

Die Zurückschreibung eines Sicherungssatzes vom IBM Spectrum Protect-Server bietet mehr Zurückschreibungsoptionen als die Zurückschreibung von einem lokalen Sicherungssatz. Dennoch kann die Zurückschreibung aus einem lokalen Sicherungssatz in einigen Fällen Vorteile bieten:

- Eventuell müssen Sie Ihre Daten zurückschreiben, wenn keine Netzverbindung zum IBM Spectrum Protect-Server besteht. Dies ist bei einer Wiederherstellung nach einem Katastrophenfall möglich.
- Die lokale Zurückschreibung benötigt möglicherweise weniger Zeit als die Zurückschreibung über eine Netzverbindung zu Ihrem IBM Spectrum Protect-Server.

Ein Sicherungssatz kann vom IBM Spectrum Protect-Server zurückgeschrieben werden, während die Sicherungssatzdatenträger für den Server verfügbar sind, oder sie können für eine lokale Sicherungssatzzurückschreibung auf das Clientsystem übertragen werden. Ein Sicherungssatz kann mit oder ohne Inhaltsverzeichnis (table of contents - TOC) generiert werden und kann Dateidaten oder Imagedaten enthalten.

Ihre Möglichkeiten zum Zurückschreiben von Daten aus Sicherungssätzen sind von der Position des Sicherungssatzes und vom Typ der Daten im Sicherungssatz abhängig. Der Befehlszeilenclient kann einige Daten zurückschreiben, die die GUI nicht zurückschreiben kann. Die GUI ermöglicht Ihnen jedoch das Anzeigen und Auswählen der zurückzuschreibenden Objekte. Im Allgemeinen bieten Sicherungs-

sätze mit Inhaltsverzeichnis, die auf dem Server gespeichert sind, mehr Zurückschreibungsoptionen. In manchen Fällen bieten lokale Sicherungssätze jedoch nützlichere Optionen als die Zurückschreibung vom IBM Spectrum Protect-Server.

Die Einschränkungen, die für das Zurückschreiben von Daten aus Sicherungssätzen über die GUI gelten, sind in der folgenden Tabelle zusammengefasst. Jede innen liegende Zelle stellt eine Kombination aus Datentyp und Position des Sicherungssatzes dar. Für jede Situation gibt die Zelle an, ob Sie die GUI verwenden können, um nur den gesamten Sicherungssatz zurückzuschreiben bzw. um Objekte innerhalb des Sicherungssatzes auszuwählen oder ob Sie nicht die GUI verwenden können, um den Sicherungssatz zurückzuschreiben.

Tabelle 43. Einschränkungen beim Zurückschreiben von Sicherungssätzen über die GUI

Datentyp im Sicherungssatz	Position des Sicherungssatzes		
	Lokal location=file oder location=tape)	IBM Spectrum Protect-Server (TOC verfügbar)	IBM Spectrum Protect-Server (TOC nicht verfügbar)
Datei	Nur gesamten Sicherungssatz zurückschreiben	Gesamten Sicherungssatz oder ausgewählte Objekte im Sicherungssatz zurückschreiben	Nur gesamten Sicherungssatz zurückschreiben
Image	Zurückschreiben nicht möglich	Gesamten Sicherungssatz oder ausgewählte Objekte im Sicherungssatz zurückschreiben	Zurückschreiben nicht möglich
Systemstatus	Nur gesamten Sicherungssatz zurückschreiben	Gesamten Sicherungssatz oder ausgewählte Objekte im Sicherungssatz zurückschreiben	Nur gesamten Sicherungssatz zurückschreiben

Die Einschränkungen, die für das Zurückschreiben von Daten aus Sicherungssätzen über den Befehlszeilenclient gelten, sind in der folgenden Tabelle zusammengefasst. Jede innen liegende Zelle stellt eine Kombination aus Datentyp und Position des Sicherungssatzes dar. Für jede Situation listet die Zelle die Befehle zum Zurückschreiben auf, die verwendet werden können. Wenn nicht anders angegeben, können Sie bestimmte Objekte in einem Sicherungssatz sowie den gesamten Sicherungssatz zurückschreiben.

Tabelle 44. Einschränkungen beim Zurückschreiben von Sicherungssätzen über die Befehlszeile

Datentyp im Sicherungssatz	Position des Sicherungssatzes		
	Lokal location=file oder location=tape)	IBM Spectrum Protect-Server (TOC verfügbar)	IBM Spectrum Protect-Server (TOC nicht verfügbar)
Datei	Befehle: restore restore backupset	Befehle: restore restore backupset	Befehle: restore backupset
Image	Zurückschreiben nicht möglich	Befehl: restore image	Zurückschreiben nicht möglich
Systemstatus	Befehl: restore backupset	Befehle: restore backupset restore systemstate	Befehl: restore backupset

Einschränkung: Beim Zurückschreiben des Systemstatus mit dem Befehl **restore backupset** können Sie keine einzelnen Objekte angeben. Sie können nur den gesamten Systemstatus zurückschreiben.

Zugehörige Verweise:

„Localbackupset“ auf Seite 500

„Query Backupset“ auf Seite 751

„Query Image“ auf Seite 758

„Restore“ auf Seite 771

„Restore Backupset“ auf Seite 777

„Restore Image“ auf Seite 786

Sicherungssätze zurückschreiben: Hinweise und Einschränkungen

In diesem Abschnitt sind einige Hinweise und Einschränkungen aufgeführt, die Sie beim Zurückschreiben von Sicherungssätzen beachten müssen.

Hinweise für das Zurückschreiben von Sicherungssätzen

Beachten Sie beim Zurückschreiben von Sicherungssätzen die folgenden Hinweise:

- Wenn das zurückzuschreibende Objekt auf einem Clientknoten generiert wurde, dessen Name sich von Ihrem aktuellen Knotennamen unterscheidet, geben Sie in allen Zurückschreibungsbefehlen den ursprünglichen Knotennamen im Parameter **filespace** an.
- Ist das Zurückschreiben eines Sicherungssatzes von einem austauschbaren Datenträger nicht möglich, ist zusammen mit dem IBM Spectrum Protect-Administrator zu überprüfen, ob der austauschbare Datenträger auf einer Einheit erstellt wurde, auf der ein kompatibles Format verwendet wurde.
- Wenn Sie den Befehl **restore backupset** in der Anfangsbefehlszeile mit dem Parameter **-location=tape** oder **-location=file** verwenden, versucht der Client nicht, eine Verbindung zum IBM Spectrum Protect-Server herzustellen.
- Beim Zurückschreiben einer Gruppe aus einem Sicherungssatz:
 - Die gesamte Gruppe bzw. alle Gruppen im virtuellen Dateibereich werden zurückgeschrieben. Wenn sich in einem virtuellen Dateibereich mehrere Gruppen befinden, ist es nicht möglich, durch Angabe des Gruppennamens eine einzige Gruppe zurückzuschreiben. Es ist nicht möglich, durch Angabe eines Dateipfads eine Gruppe teilweise zurückzuschreiben.
 - Geben Sie eine Gruppe über einen der folgenden Werte an:
 - Geben Sie den Namen des virtuellen Dateibereichs mit dem Parameter **Dateibereichsname** an.
 - Verwenden Sie die Option **subdir**, um Unterverzeichnisse einzuschließen.
- Eine begrenzte Unterstützung wird für das Zurückschreiben von Sicherungssätzen auf Bandeinheiten bereitgestellt, die an das Clientsystem angeschlossen sind. Sie müssen immer einen nativen Einheitentreiber verwenden, der vom Hersteller der Einheit bereitgestellt wird. Der Einheitentreiber, der von IBM für die Verwendung mit dem IBM Spectrum Protect-Server bereitgestellt wird, kann nicht auf dem Clientsystem zum Zurückschreiben lokaler Sicherungssätze benutzt werden.
- Enthält ein Sicherungssatz Dateien von mehreren Eignern, ist der Sicherungssatz selbst Eigentum der Rootbenutzer-ID und er wird Benutzer-IDs ohne Rootberechtigung nicht angezeigt. In diesem Fall können Benutzer-IDs ohne Rootberechtigung ihre Dateien zurückschreiben, indem sie den Namen des Sicherungs-

satzes vom IBM Spectrum Protect-Administrator anfordern. Andere Benutzer als Root können nur eigene Dateien zurückschreiben.

- Soll die grafische Benutzerschnittstelle des Clients einen Sicherungssatz von einer lokalen Einheit zurückschreiben, ohne dass eine Serververbindung erforderlich ist, verwenden Sie die Option `localbackupset`.

Einschränkungen beim Zurückschreiben von Sicherungssätzen

Beachten Sie beim Zurückschreiben von Sicherungssätzen die folgenden Einschränkungen:

- Sicherungssatzdaten, die mit der API gesichert wurden, können weder zurückgeschrieben noch verwendet werden.
- Mit dem Befehl **restore backupset** können Sie keine Imagedaten aus einem Sicherungssatz zurückschreiben. Imagedaten aus einem Sicherungssatz können Sie nur mit dem Befehl **restore image** zurückschreiben.
- Sie können keine Imagedaten aus einem lokalen Sicherungssatz (`location=tape` oder `location=file`) zurückschreiben. Imagedaten aus einem Sicherungssatz können Sie nur vom IBM Spectrum Protect-Server zurückschreiben.

Zugehörige Verweise:

„Localbackupset“ auf Seite 500

„Restore“ auf Seite 771

„Restore Image“ auf Seite 786

„Restore Backupset“ auf Seite 777

Zurückschreibung von Sicherungssätzen

IBM Spectrum Protect betrachtet einen Sicherungssatz als ein Objekt, das die gesamte Dateistruktur enthält. Sie können den gesamten Sicherungssatz zurückschreiben oder in einigen Fällen Teile des Satzes auswählen. Die Sicherungssatzdatenträger sind selbstbeschreibend und enthalten alle Informationen, die für eine erfolgreiche Zurückschreibung erforderlich sind.

Wenn eine Verbindung zu dem Tivoli Storage Manager-Server der Version 5.4 oder höher besteht, kann Ihr Serveradministrator gestapelte Sicherungssätze erstellen. Diese Sicherungssätze können Daten mehrerer Clientknoten und verschiedene Datentypen für einen bestimmten Clientknoten enthalten. Bei den Datentypen kann es sich um Dateidaten oder Imagedaten handeln.

Einschränkung: Die Zurückschreibungsverarbeitung von Imagedaten und Anwendungsdaten ist nur verfügbar, wenn die Zurückschreibung vom Server erfolgt. Imagedaten und Anwendungsdaten können Sie nicht aus lokalen Sicherungssätzen auf dem Client zurückschreiben.

Wenn ein Sicherungssatz gestapelt ist, können Sie nur Daten für Ihren eigenen Knoten zurückschreiben. Die Daten aller anderen Knoten werden übersprungen. Wenn Daten aus einem gestapelten Sicherungssatz auf einer lokalen Einheit zurückgeschrieben werden, können Sie nur Daten auf Dateiebene für Ihren eigenen Clientknoten zurückschreiben. Es ist wichtig, dass die Option `nodename` so eingestellt ist, dass sie für einen der Knoten im Stapelspeicher dem Knotennamen entspricht, der zum Generieren des Sicherungssatzes verwendet wurde.

Wichtig: Aufgrund der Portierbarkeit lokaler Sicherungssätze müssen Sie Ihre lokalen Sicherungssätze auf Wechseldatenträgern durch zusätzliche Maßnahmen sichern. Die Datenträger für Sicherungssätze müssen physisch gesichert werden, weil

der Sicherungssatz ohne Authentifizierung beim Server lokal zurückgeschrieben werden kann. Jeder Benutzer hat Zugriff auf alle Daten in dem gestapelten Sicherungssatz; dies bedeutet, dass der Benutzer Zugriff auf Daten habt, die ihm nicht gehören, indem er den Knotennamen ändert oder den Sicherungssatz im unformatierten Format anzeigt. Verschlüsselung oder physischer Schutz der Datenträger sind die einzigen Möglichkeiten zum Schutz der Daten.

Wenn Sie Sicherungssatzdaten vom Server zurückschreiben, können einzelne Dateien, Verzeichnisse oder die gesamten Sicherungssatzdaten in einer einzigen Operation von der GUI oder der Befehlszeile zurückgeschrieben werden. Wenn Sie Sicherungssatzdaten lokal zurückschreiben, kann die GUI nur einen vollständigen Sicherungssatz anzeigen und zurückschreiben. Sie können die Befehlszeile verwenden, um einzelne Dateien oder Verzeichnisse zurückzuschreiben, die in einem Sicherungssatz lokal gespeichert sind.

Sicherungssätze über die GUI zurückschreiben

Die Client-GUI kann Daten aus einem Sicherungssatz auf dem Server, aus einer lokalen Datei oder von einer lokalen Bandeinheit zurückschreiben. Sie können die GUI verwenden, um einzelne Dateien aus einem Sicherungssatz mit einem Inhaltsverzeichnis vom IBM Spectrum Protect-Server zurückzuschreiben. Dies ist jedoch weder bei lokalen Sicherungssätzen noch bei Sicherungssätzen vom Server ohne Inhaltsverzeichnis möglich.

Informationen zu diesem Vorgang

Wichtig: Bevor Sie eine Zurückschreibungsoperation beginnen, beachten Sie, dass Sicherungssätze Daten für mehrere Dateibereiche enthalten können. Wenn Sie ein anderes Ziel als die ursprüngliche Position angeben, werden Daten aus *allen* Dateibereichen an die angegebenen Position zurückgeschrieben.

Führen Sie folgende Schritte aus, um einen Sicherungssatz über die GUI zurückzuschreiben:

1. Klicken Sie auf **Zurückschreiben** im GUI-Hauptfenster. Das Fenster 'Zurückschreiben' wird angezeigt.
2. Lokalisieren Sie das Objekt **Sicherungssätze** in der Verzeichnisbaumstruktur und erweitern Sie es, indem Sie auf das Pluszeichen (+) daneben klicken.
 - Soll der Sicherungssatz von einer lokalen Einheit zurückgeschrieben werden, erweitern Sie das Objekt **Lokal**. Das Fenster 'Position für Sicherungssatz angeben' wird angezeigt. Wählen Sie im Fenster **Dateiname:** oder **Bandname:** in der Liste aus und geben Sie die Position des Band- oder Dateinamens ein. Sie können auch auf die Schaltfläche **Durchsuchen** klicken, um ein Dateiauswahlfenster zu öffnen und einen Sicherungssatz auszuwählen.
 - Zum Zurückschreiben von Daten aus einem Sicherungssatz auf dem Server müssen Sie zuerst das Objekt **Server** und anschließend **Dateiebene** oder **Image** erweitern, je nachdem, welche Art der Zurückschreibung angefordert wird.
3. Klicken Sie auf das Auswahlfeld, das sich neben dem zurückzuschreibenden Sicherungssatz bzw. neben dem zurückzuschreibenden Verzeichnis oder der zurückzuschreibenden Datei innerhalb des Sicherungssatzes befindet.

Sie können Dateien innerhalb eines Sicherungssatzes auswählen, wenn der Sicherungssatz sich auf dem Server befindet und über ein Inhaltsverzeichnis verfügt.
4. Klicken Sie auf **Zurückschreiben**. Das Fenster 'Zurückschreibungsziel' wird angezeigt. Geben Sie die entsprechenden Informationen ein.

5. Klicken Sie auf **Zurückschreiben**. Im Fenster 'Task-Liste' wird der Verarbeitungsstatus der Zurückschreibung angezeigt.

Anmerkung:

- Wenn das Objekt, das Sie zurückschreiben wollen, Teil eines auf einem Knoten generierten Sicherungssatzes ist und der Knotenname auf dem Server geändert wird, stimmen keine Sicherungssatzobjekte, die vor der Namensänderung generiert wurden, mit dem neuen Knotennamen überein. Stellen Sie sicher, dass der Knotenname derselbe ist wie für den Knoten, für den der Sicherungssatz generiert wurde.
- Der Client kann verwendet werden, um einen Sicherungssatz auf einer angeschlossenen Einheit mit oder ohne Serververbindung zurückzuschreiben. Schlägt die Serververbindung fehl, wird eine Eingabeaufforderung angezeigt, um die Zurückschreibung des lokalen Sicherungssatzes fortzusetzen. Außerdem kann der Client über die Option `localbackupset` angewiesen werden, keine Verbindung zum Server herzustellen.
- Für bestimmte lokale Einheiten wie Bandeinheiten (Bandeinheiten gelten nicht für Mac OS X) müssen Einheitentreiber installiert werden, bevor eine Zurückschreibung ausgeführt werden kann. Das Handbuch zur Einheit bietet Unterstützung bei dieser Task. Sie müssen auch die Einheitenadresse kennen, um die Zurückschreibung ausführen zu können.
- Die folgenden Features einer Sicherungssatzzurückschreibung vom Server stehen bei einer lokalen Zurückschreibung nicht zur Verfügung:
 1. Imagezurückschreibung.
 2. Die GUI-Anzeige und -Zurückschreibung einzelner Dateien und Verzeichnisse. Die Befehlszeile kann verwendet werden, um ein einzelnes Verzeichnis oder eine einzelne Datei aus einem lokalen Sicherungssatz zurückzuschreiben.

Sicherungssätze mit der Befehlszeilenschnittstelle des Clients zurückschreiben

Die Befehlszeilenschnittstelle des Clients kann Daten aus einem Sicherungssatz auf dem Server, aus einer lokalen Datei oder von einer lokalen Bandeinheit zurückschreiben. Sie können mit der Befehlszeilenschnittstelle des Clients einzelne Dateien aus lokalen Sicherungssätzen und aus Sicherungssätzen ohne Inhaltsverzeichnis zurückschreiben.

Wenn Sie einen Sicherungssatz über die Befehlszeilenschnittstelle des Clients zurückschreiben wollen, verwenden Sie den Befehl **query backupset**, um die verfügbaren Sicherungssatzdaten anzuzeigen. Anschließend schreiben Sie die Daten mit Zurückschreibungsbefehlen zurück.

Mit den folgenden Befehlen können Sie Daten aus Sicherungssätzen zurückschreiben:

- **restore**
- **restore backupset**
- **restore image**

Verwenden Sie den korrekten Befehl für die Position des Sicherungssatzes und die Daten in dem Sicherungssatz. Weitere Informationen siehe Tabelle 44 auf Seite 252.

Zugehörige Verweise:

„Query Backupset“ auf Seite 751

„Query Image“ auf Seite 758
„Restore“ auf Seite 771
„Restore Backupset“ auf Seite 777
„Restore Image“ auf Seite 786

Daten während einer Übernahme zurückschreiben oder abrufen

Wenn eine Übernahme des Clients auf dem Sekundärserver stattfindet, können Sie replizierte Daten vom Sekundärserver zurückschreiben oder abrufen.

Vorbereitende Schritte

Bevor Sie mit dem Zurückschreiben bzw. Abrufen von Daten während einer Übernahme beginnen, müssen Sie Folgendes sicherstellen:

- Die automatisierte Clientübernahme ist auf dem Client konfiguriert.
- Es besteht eine Verbindung zu einem IBM Spectrum Protect-Server, der Clientknoten repliziert. Weitere Informationen zu Übernahmevoraussetzungen finden Sie in „Voraussetzungen für die automatisierte Clientübernahme“ auf Seite 99.

Einschränkung: Im Übernahmemodus können Sie keine Daten auf dem Sekundärserver sichern oder archivieren.

Vorgehensweise

Gehen Sie wie folgt vor, um Daten während einer Übernahme zurückzuschreiben oder abzurufen:

1. Überprüfen Sie den Replikationsstatus der Clientdaten auf dem Sekundärserver. Der Replikationsstatus zeigt an, ob die neueste Sicherung auf dem Sekundärserver repliziert wurde.
2. Führen Sie die Zurückschreibung bzw. den Abruf Ihrer Daten wie gewöhnlich mithilfe der Client-GUI oder der Befehlszeilenschnittstelle aus.

Tipp: Wiederanlauffähige Zurückschreibungsoperationen funktionieren erwartungsgemäß, wenn eine Verbindung zum Sekundärserver besteht. Jedoch können Zurückschreibungsoperationen, die unterbrochen werden, wenn der Primärserver ausfällt, nach der Übernahme des Clients nicht erneut gestartet werden. Sie müssen nach der Übernahme des Clients auf dem Sekundärserver die gesamte Zurückschreibungsoperation erneut ausführen.

Ergebnisse

Wenn die replizierten Daten auf dem Sekundärserver nicht aktuell sind, werden Sie aufgefordert, die Zurückschreibungs- bzw. Abrufoperation fortzusetzen oder zu stoppen.

Geben Sie beispielsweise den folgenden Befehl aus, um das Verzeichnis `build.sh` über die Befehlszeilenschnittstelle zurückzuschreiben:

```
dsmc res /build.sh
```

Die folgende Ausgabe wird angezeigt:

```
IBM Spectrum Protect
Befehlszeilenschnittstelle des Clients für Sichern/Archivieren
Clientversion 8, Release 1, Stufe 0.0
Clientdatum/-zeit: 16.11.2016 12:05:35
(c) Copyright IBM Corporation und andere 1990, 2016. Alle Rechte vorbehalten.

Knotenname: MY_NODE_NAME
ANS2106I Verbindung zum primären IBM Spectrum Protect-Server 192.0.2.1 ist
fehlgeschlagen.

ANS2107I Es wird versucht, eine Verbindung zum sekundären Server TARGET
unter 192.0.2.9 : 1501 herzustellen.

Knotenname: MY_NODE_NAME
Sitzung hergestellt mit Server TARGET: Windows
Serverversion 8, Release 1, Stufe 0.0
Serverdatum/-zeit: 16.11.2016 12:05:35  Letzter Zugriff: 15.11.2016 14:13:32

Sitzung im Übernahmemodus auf dem sekundären Server aufgebaut
ANS2108I Verbindung zum sekundären Server TARGET hergestellt.
Zurückschreibungsfunktion aufgerufen.

ANS2120W Das vom Server TARGET aufgelistete Datum der letzten Speicheroperation
(16.05.2013 22:38:23) stimmt nicht mit dem vom Client gespeicherten Datum
der letzten Speicheroperation (21.05.2013 21:32:20) überein.
Fortfahren? (Ja (J)/Nein (N))
```

Wenn Sie N auswählen, wird die folgende Nachricht angezeigt:

```
ANS1074W Die Operation wurde vom Benutzer gestoppt.
```

Wenn Sie J auswählen, wird die Zurückschreibungsverarbeitung normal fortgesetzt, aber die zurückgeschriebenen Daten sind möglicherweise nicht aktuell.

Zugehörige Konzepte:

„Konfiguration und Verwendung der automatisierten Clientübernahme“ auf Seite 98

Zugehörige Tasks:

„Status replizierter Clientdaten bestimmen“ auf Seite 104

Image in Datei zurückschreiben

Wenn Sie ein Image sichern, sichert der Client für Sichern/Archivieren den ersten Sektor des Datenträgers. Bei der Zurückschreibung der Daten wird der erste Sektor jedoch übersprungen, um den ursprünglichen Steuerblock des logischen Datenträgers des Zieldatenträgers beizubehalten.

Wenn Sie ein Image in eine Datei zurückschreiben, wird der vollständige Datenträgerinhalt einschließlich des ersten Sektors in die Datei zurückgeschrieben.

AIX LVM-Datenträger aus ursprünglichen Datenträgergruppen enthalten den Steuerblock des logischen Datenträgers (LVCB = Logical Volume Control Block) im ersten Sektor (512 Byte) des Datenträgers. Der LVCB enthält datenträgerspezifische Metadaten, die von den Anwendungen, die den Datenträger verwenden, beibehalten werden sollten.

Wenn Sie die Datei mit dem Image auf einen LVM-Datenträger aus der ursprünglichen Datenträgergruppe kopieren, müssen Sie den LVCB sowohl in der Datei als auch auf dem Zieldatenträger überspringen. Zu diesem Zweck können Sie den folgenden **dd**-Befehl verwenden.

```
dd if=<Dateiname> of=/dev/<Datenträger> bs=512 skip=1 seek=1
```

Der Befehl **dd** setzt die Blockgröße auf 512 Byte, wodurch das Kopieren sehr langsam wird. Es ist besser, einen Wert wie `bs=1m` oder Ähnliches zu verwenden. Alternativ können Imagedaten wie folgt kopiert werden:

1. Sichern Sie den ursprünglichen ersten Sektor in einer Datei:

```
dd if=/dev/<Datenträger> of=firstblk.tmp bs=512 count=1
```

2. Kopieren Sie das zurückgeschriebene Image:

```
dd if=<Dateiname> of=/dev/<Datenträger> bs=1m
```

3. Schreiben Sie den ursprünglichen ersten Sektor zurück:

```
dd if=firstblk.tmp of=/dev/<Datenträger> bs=512 count=1
```

Seit der Einführung großer und skalierbarer Datenträgergruppenformate unter AIX ist es möglich, dass der erste Sektor des logischen Datenträgers keinen LVCB enthält und für die Daten verfügbar ist. Wenn Sie auf Ihrem System große und skalierbare Datenträgergruppen verwenden und den gesamten Datenträger einschließlich des ersten Sektors zurückschreiben müssen, schreiben Sie den Datenträger in eine Datei zurück und kopieren Sie die Datei anschließend auf einen Zieldatenträger. Zu diesem Zweck können Sie den folgenden **dd**-Befehl verwenden.

```
dd if=<Dateiname> of=/dev/<Datenträger> bs=1m
```

Zugehörige Konzepte:

„Image über die Befehlszeile zurückschreiben“ auf Seite 250

Zugehörige Tasks:

„Image über die GUI zurückschreiben“ auf Seite 249

GPFS-Dateisystemdaten mit Speicherpools verwalten

Mithilfe der GPFS-Technologie (GPFS = Global Parallel File Systems) können Sie Ihre Daten mit Speicherpools verwalten. Ein Speicherpool ist eine Sammlung von Platten oder RAID-Arrays mit ähnlichen Eigenschaften, die als eine Gruppe zusammen verwaltet werden.

Die Gruppe, unter der die Speicherpools zusammen verwaltet werden, ist das Dateisystem. Die automatische Platzierung und Verwaltung von Dateien auf Speicherpoolebene wird von Maßnahmen ausgeführt. Eine Maßnahme ist eine Gruppe von Regeln, die auf der Basis der Dateiattributen den Lebenszyklus von Benutzerdaten beschreibt.

Wenn eine Datei erstellt wird, bestimmt die Platzierungsmaßnahme die ursprüngliche Position der Dateidaten und ordnet die Datei einem Speicherpool zu. Alle Daten, die in diese Datei geschrieben werden, werden in den zugeordneten Speicherpool gestellt. Die Verwaltungsmaßnahme bestimmt die Dateiverwaltungsoperation wie z. B. Migration und Löschung. Die Dateien innerhalb eines GPFS-Dateisystems werden in Abhängigkeit von den aktivierten Platzierungs- und Umlagerungsmaßnahmen über verschiedene Speicherpools verteilt.

Bei der Zurückschreibung werden die Dateien in den korrekten Speicherpool gestellt. Da der IBM Spectrum Protect-Server die Umlagerungen zwischen den Speicherpools nicht erkennt, werden die Dateien in den Speicherpool gestellt, in dem die Sicherung erfolgt ist. Die Maßnahmensteuerkomponente ersetzt die Dateien auf der Basis von Migrationsmaßnahmen.

Ist eine Speicherpool-ID in den erweiterten Attributen der Datei gespeichert und ist dieser Speicherpool verfügbar, wird die Datei immer in diesen Speicherpool ge-

stellt. Ist der Speicherpool nicht verfügbar, wird die Datei anhand der Platzierungsmaßnahme platziert. Stimmt die Platzierungsmaßnahme nicht mit der Datei überein, wird die Datei in den Systempool gestellt.

GPFS handhabt die Platzierung von Dateien nach einer Zurückschreibung wie folgt:

- Die Datei wird in den Pool gestellt, der ausgewählt werden kann, indem die gesicherten Dateiattribute mit einer Regel RESTORE in Einklang gebracht wird
- Die Datei wird in den Pool gestellt, in der sie war, als sie gesichert wurde
- Die Datei wird auf der Basis der aktuellen Platzierungsmaßnahme platziert
- Die Datei wird in den Systemspeicherpool gestellt

Mit der GPFS-Regel RESTORE können Sie Dateien in Übereinstimmung mit ihren gespeicherten Attributen und nicht mit den aktuellen Dateiattributen bringen. Wenn die Dateiattribute nicht übereinstimmen, versucht GPFS, die Datei bei ihrer Zurückschreibung in der oben beschriebenen Reihenfolge zu platzieren.


Weitere Informationen über die GPFS-Regel RESTORE enthalten die Abschnitte zu Maßnahmen und Regeln in der GPFS-Dokumentation.

Es gelten die folgenden Einschränkungen:


- Das Zurückschreiben von Stubdateien funktioniert nicht mit mehreren Speicherpools bzw. mit Dateien, die über ACLs verfügen
- Das Aufheben von Dateigruppenverbindungen ist nicht zulässig
- Die GPFS-Option ctime sollte auf no (den Standardwert) gesetzt werden, um zu verhindern, dass Dateien nach der GPFS-Dateiumlagerung in einen anderen Speicherpool gesichert werden.

Informationen zur Verwendung von Speicherpools finden Sie in der Dokumentation zum IBM Spectrum Protect-Server.


Zugehörige Verweise:

 [Datenspeicherung in Speicherpools](#)

Zugehörige Informationen:

 [Produktinformation zu IBM Spectrum Scale](#)

 [Befehl 'mmbackup': IBM Spectrum Protect-Voraussetzungen](#)

 [Hinweise zur Verwendung der Einschluss- und Ausschlussoptionen von IBM Spectrum Protect in Verbindung mit dem IBM Spectrum Scale-Befehl 'mmbackup'](#)

Daten nach Zeitpunkt zurückschreiben

Verwenden Sie eine Zurückschreibung *nach Zeitpunkt*, um Dateien mit dem Stand zurückzuschreiben, den sie an einem bestimmten Datum und zu einer bestimmten Uhrzeit hatten.

Informationen zu diesem Vorgang

Durch das Zurückschreiben nach Zeitpunkt können die Auswirkungen eines Datenverlusts beseitigt werden, indem die Daten von einem Zeitpunkt vor dem bekannten Datenverlust zurückgeschrieben werden, oder der frühere Status einer Basisconfiguration kann wiederhergestellt werden.

Sie können eine Zurückschreibung nach Zeitpunkt für einen Dateibereich, ein Verzeichnis oder eine Datei ausführen.

Sie können eine Zurückschreibung nach Zeitpunkt auch für Imagesicherungen ausführen.

Teilsicherungen sind durchzuführen, um eine Zurückschreibung nach Zeitpunkt zu unterstützen. Während einer Teilsicherung benachrichtigt der Client für Sichern/ Archivieren den Server, wenn Dateien aus einem Clientdateibereich oder Verzeichnis gelöscht werden. Bei selektiven Sicherungen und Teilsicherungen nach Datum erhält der Server keine Informationen über gelöschte Dateien. Teilsicherungen sollten den möglichen Zurückschreibungsanforderungen entsprechend häufig durchgeführt werden.

Wird eine Zurückschreibung nach Zeitpunkt mit einem Datum und einer Uhrzeit angefordert, die vor der ältesten vom IBM Spectrum Protect-Server verwalteten Version liegen, wird das Objekt nicht in Ihr System zurückgeschrieben. Dateien, die vor dem angegebenen Zeitpunkt von Ihrer Workstation gelöscht wurden, werden nicht zurückgeschrieben.

Anmerkung:

1. Ihr Administrator muss Kopiengruppeneinstellungen definieren, mit denen genügend inaktive Versionen einer Datei aufbewahrt werden, um sicherzustellen, dass diese Datei mit dem Stand eines bestimmten Datums und einer bestimmten Uhrzeit zurückgeschrieben werden kann. Wenn nicht genügend Versionen aufbewahrt werden, kann der Client unter Umständen nicht alle Objekte mit dem Stand des angegebenen Zeitpunkts zurückschreiben.
2. Wird eine Datei oder ein Verzeichnis gelöscht, wird die aktive Sicherungsversion bei der nächsten Ausführung einer Teilsicherung zu einer inaktiven Version, und die ältesten Versionen, die die mit dem Verwaltungsklassenattribut *Versions gelöschter Daten* angegebene Anzahl überschreiten, werden gelöscht.

Bei der Ausführung einer Zurückschreibung nach Zeitpunkt ist Folgendes zu beachten:

- Der Client schreibt Dateiversionen aus der neuesten Sicherung vor dem angegebenen Datum des Zeitpunkts zurück. Stellen Sie sicher, dass der angegebene Zeitpunkt nicht mit dem Datum und die Uhrzeit identisch ist, an dem bzw. zu der diese Sicherung ausgeführt wurde.
- Liegen das angegebene Datum und die angegebene Uhrzeit für das Objekt, das zurückgeschrieben werden soll, vor dem Datum und der Uhrzeit der ältesten Version, die auf dem Server vorhanden ist, kann der Client dieses Objekt nicht zurückschreiben.
- Bei einer Zurückschreibung nach Zeitpunkt werden Dateien zurückgeschrieben, die nach dem Datum des Zeitpunkts von der Client-Workstation gelöscht wurden, aber keine Dateien, die vor diesem Datum gelöscht wurden.
- Der Client kann keine Datei zurückschreiben, die nach dem Datum und der Uhrzeit des Zeitpunkts erstellt wurde. Wird ein Zurückschreiben nach Zeitpunkt durchgeführt, werden Dateien, die nach dem Datum für den Zeitpunkt auf dem Client erstellt wurden, nicht gelöscht.

Vorgehensweise

Gehen Sie wie folgt vor, um eine Zurückschreibung nach Zeitpunkt über die Client-GUI auszuführen:

1. Klicken Sie auf die Schaltfläche **Zurückschreiben** im Hauptfenster. Das Fenster **Zurückschreiben** wird angezeigt.
2. Klicken Sie auf die Schaltfläche **Zeitpunkt** im Fenster **Zurückschreiben**. Das Fenster **Zurückschreiben nach Zeitpunkt** wird angezeigt.
3. Wählen Sie das Auswahlfeld **Datum nach Zeitpunkt verwenden** aus. Wählen Sie das Datum und die Uhrzeit aus und klicken Sie auf **OK**. Der angegebene Zeitpunkt wird im Anzeigefeld **Zeitpunkt** im Fenster **Zurückschreiben** angezeigt.
4. Zeigen Sie die Objekte an, die zurückgeschrieben werden sollen. Sie können nach einem Objekt anhand des Namens suchen, die Verzeichnisbaumstruktur filtern oder mit den Verzeichnissen in der Verzeichnisbaumstruktur arbeiten.
5. Klicken Sie auf die Auswahlfelder neben den Objekten, die zurückgeschrieben werden sollen.
6. Klicken Sie auf die Schaltfläche **Zurückschreiben**. Das Fenster **Zurückschreibungsziel** wird angezeigt. Geben Sie die entsprechenden Informationen ein.
7. Klicken Sie auf die Schaltfläche **Zurückschreiben**, um die Zurückschreibung zu starten. Im Fenster **Task-Liste** für die Zurückschreibung wird der Verarbeitungsstatus der Zurückschreibung angezeigt.

Ergebnisse

Anmerkung: Sind keine Sicherungsversionen eines Verzeichnisses für den angegebenen Zeitpunkt vorhanden, können Dateien in diesem Verzeichnis nicht mit der GUI zurückgeschrieben werden. Sie können diese Dateien jedoch mithilfe der Befehlszeile zurückschreiben.

Sie können eine Zurückschreibung nach Zeitpunkt mit dem Befehlszeilenclient starten, indem Sie die Optionen `pitdate` und `pittime` in den Befehlen **query backup** und **restore** verwenden. Wenn Sie beispielsweise die Optionen `pitdate` und `pittime` im Befehl **query backup** verwenden, legen Sie den Zeitpunkt fest, für den Dateinformationen zurückgegeben werden. Wenn Sie `pitdate` und `pittime` im Befehl **restore** verwenden, legen die angegebenen Datums- und Zeitwerte den Zeitpunkt fest, für den Dateien zurückgegeben werden. Wird `pitdate` ohne einen Wert für `pittime` angegeben, nimmt `pittime` den Standardwert 23:59:59 an. Wird `pittime` ohne einen Wert für `pitdate` angegeben, wird die Option ignoriert.

Zugehörige Konzepte:

Kapitel 9, „Speicherverwaltungsmaßnahmen“, auf Seite 309

Zugehörige Verweise:

„Backup Image“ auf Seite 702

Verschlüsselte AIX-Dateien zurückschreiben

Wenn Dateien in unformatiertem Format von einem AIX JFS2 EFS (Verschlüsseltes AIX JFS2-Dateisystem) gesichert werden, können Sie sie nur in dasselbe oder in ein anderes JFS2 EFS zurückschreiben. Sie können nicht in ein anderes Dateisystem oder auf eine andere Plattform zurückgeschrieben werden.

Wenn EFS-Dateien im Klartext gesichert werden, können Sie sie standortunabhängig zurückschreiben. Wenn Sie sie in ein JFS2 EFS zurückschreiben, werden sie automatisch nur dann erneut verschlüsselt, wenn für das Verzeichnis, in das sie zurückgeschrieben werden, die AIX-Option "EFS-Vererbung" definiert ist.

Nach dem Zurückschreiben einer in unformatiertem Format gesicherten Datei stellen Sie unter Umständen fest, dass die Datei nicht entschlüsselt werden kann. Der ursprünglich für die Datei verwendete Verschlüsselungsschlüssel ist möglicherweise im Schlüsselspeicher des Benutzers nicht mehr verfügbar. In diesem Fall ist es erforderlich, den zum Zeitpunkt der Sicherung verwendeten Schlüsselspeicher zurückzuschreiben.

Informationen zum Sichern von EFS-Daten finden Sie in „Verschlüsseltes AIX JFS2-Dateisystem sichern“ auf Seite 228.

AIX-Workloadpartitionsdateisysteme zurückschreiben

Alle Dateien, die von der lokalen Workloadpartition (WPAR) erstellt und von dem in der globalen Workloadpartition installierten Client für Sichern/Archivieren gesichert wurden, können von dem in der globalen Workloadpartition installierten Client zurückgeschrieben werden.

Es folgen einige Konfigurationsbeispiele für die globale Partition und die Workloadpartition:

Globale Partition:

Systemname: shimla

Dateisystem: /home /opt

WPAR #1-Konfiguration:

Name: wpar1

Dateisystem: /home; Name in globaler WPAR: /wpars/wpar1/home

WPAR #2-Konfiguration:

Name: wpar2

Dateisystem: /data; Name in globaler WPAR: /wpars/wpar2/data

Es gibt zwei Möglichkeiten, die WPAR-Daten zurückzuschreiben, abhängig von der Methode, die zum Sichern der WPAR-Datendateien verwendet wurde:

- Alle WPAR-Dateisysteme als Dateibereiche innerhalb der globalen Partition zurückschreiben. Mit dem Namen des Dateibereichs muss die Workloadpartition identifiziert werden, zu der der Dateibereich gehört. Alle Daten werden mithilfe eines einzigen Zeitplans auf einem einzigen Knoten verwaltet. Unter Verwendung der zuvor erwähnten Beispielkonfiguration zeigt das folgende Beispiel eine Musterdatei dsm.sys mit einer Serverzeilengruppe für alle Systeme, sowohl global als auch lokal:

SErvername shimla

TCPPort 1500

TCPServeraddress server.example.com

nodename shimla

PasswordAccess generate

Domain /wpars/wpar1/home /wpars/wpar2/data /home /opt

Verwenden Sie den folgenden Befehl, um jeden einzelnen Dateibereich zurückzuschreiben:

```
dsmc restore /wpars/wpar1/home/*
dsmc restore /wpars/wpar2/data/*
dsmc restore /home/*
dsmc restore /opt/
```

- Jedes einzelne WPAR-Dateisystem von einem anderen Knotennamen zurückschreiben, wenn es unter einem anderen Knotennamen gesichert wurde. Jede Workloadpartition muss einen separaten Knotennamen und einen Scheduler haben, der innerhalb der globalen Partition ausgeführt wird. Außerdem müssen drei Scheduler-Services definiert werden, wobei jeder Service entsprechend dem Namen der Serverzeilengruppe eine andere Datei dsm.opt verwendet. Diese Methode ermöglicht, dass jede WPAR-Zurückschreibungsoperation unabhängig von den anderen verwaltet wird. Unter Verwendung der zuvor erwähnten Beispielkonfiguration zeigt das folgende Beispiel eine Musterdatei dsm.sys mit drei Serverzeilengruppen: eine für wpar1, eine für wpar2 und eine für die globale Partition shimla:

```
Servname shimla_wpar1
TCPport 1500
TCPserveraddress server.example.com
nodename wpar1
PasswordAccess generate
Domain /wpars/wpar1/home
```

```
Servname shimla_wpar2
TCPport 1500
TCPserveraddress server.example.com
nodename wpar2
PasswordAccess generate
Domain /wpars/wpar2/data
```

```
Servname shimla
TCPport 1500
TCPserveraddress server.example.com
nodename shimla
PasswordAccess generate
Domain /home /opt
```

Tabelle 45. Beispielbefehle zum Zurückschreiben von Workloadpartitionen mit der Datei dsm.opt

In der Datei dsm.opt	Beispielbefehl zum Zurückschreiben
servername shimla_wpar1	dsmc restore /wpars/wpar1/home/*
servername shimla_wpar2	dsmc restore /wpars/wpar2/data/*
servername shimla	dsmc restore /home/* dsmc restore /opt/*

NAS-Dateisysteme zurückschreiben

NAS-Dateisystemimages werden mithilfe der GUI des Clients für Sichern/Archivieren oder der Befehlszeilenschnittstelle zurückgeschrieben.

Sie können vollständige NAS-Dateisystemimages oder Differenzdateisystemimages zurückschreiben, die zuvor gesichert wurden. Wird ein Differenzimage zurückgeschrieben, schreibt IBM Spectrum Protect automatisch zuerst das vollständige Sicherungsimage und dann das Differenzimage zurück. Es ist nicht erforderlich, dass ein Clientknoten ein NAS-Dateisystem anhängt, um Sicherungs- oder Zurückschreibungsoperationen für dieses Dateisystem auszuführen.

Zugehörige Konzepte:

NAS-Dateisysteme mit der GUI des Clients für Sichern/Archivieren zurückschreiben

In diesem Abschnitt sind die Schritte aufgelistet, die Sie ausführen müssen, um NAS-Dateisysteme mit der GUI des Clients für Sichern/Archivieren zurückzuschreiben.

Vorgehensweise

1. Klicken Sie auf die Schaltfläche **Zurückschreiben** im Hauptfenster. Das Fenster 'Zurückschreiben' wird angezeigt.
2. Falls erforderlich, erweitern Sie die Verzeichnisbaumstruktur. Zum Erweitern eines Knotens in der Baumstruktur klicken Sie auf das Pluszeichen (+) neben einem Objekt in der Baumstruktur. Es werden die Knoten angezeigt, die gesichert wurden und für die Ihr Administrator berechtigt ist. Der Anfangsknoten mit dem Namen **Knoten** ist nicht auswählbar. Dieser Knoten wird nur angezeigt, wenn ein NAS-Plug-in auf der Client-Workstation vorhanden ist. NAS-Knoten werden auf derselben Stufe wie der Knoten der Client-Workstation angezeigt. Es werden nur Knoten angezeigt, für die der Administrator berechtigt ist.
3. Erweitern Sie den NAS-Knoten, um das Imageobjekt anzuzeigen.
4. Erweitern Sie das Imageobjekt, um Datenträger anzuzeigen, die Sie zurückschreiben können. Datenträgerobjekte können Sie nicht erweitern.
5. Wählen Sie die Auswahlfelder neben den Datenträgern unter dem Imageobjekt aus, die zurückgeschrieben werden sollen. Wenn Sie ein NAS-Image zurückschreiben wollen, das an einem bestimmten Datum gesichert wurde, klicken Sie auf die Schaltfläche **Nach Zeitpunkt**. Nach Auswahl eines Datums wird das letzte Objekt angezeigt, das an oder vor diesem Datum gesichert wurde, einschließlich eventueller inaktiver Objekte. Sollen vor der Auswahl von Objekten alle Images (einschließlich aktiver und inaktiver Images) angezeigt werden, wählen Sie in der Menüleiste **Sicht** → **Aktive/inaktive Dateien anzeigen** aus.
6. Klicken Sie auf **Zurückschreiben**. Das Fenster 'Zurückschreibungsziel' wird angezeigt. Geben Sie die Informationen in das Fenster 'Zurückschreibungsziel' ein. Wenn Sie ein anderes Ziel für die Zurückschreibung auswählen, können Sie jeweils nur einen Datenträger an ein anderes Ziel zurückschreiben. Sie können NAS-Dateisystemimages auf alle Datenträger auf dem NAS-Dateiserver zurückschreiben, von dem sie gesichert wurden. Sie können Images nicht auf einen anderen NAS-Dateiserver zurückschreiben.
7. Klicken Sie auf **Zurückschreiben**. Im Fenster **Task-Liste** für die NAS-Zurückschreibung werden der Verarbeitungsstatus der Zurückschreibung und die Statusleiste angezeigt. Eine Zahl neben der Statusleiste gibt, falls bekannt, die Größe der Zurückschreibung an. Nach Beendigung der Zurückschreibung zeigt das Fenster 'NAS-Zurückschreibungsbericht' Verarbeitungsdetails an. Wenn Sie die Sitzung der GUI des Clients für Sichern/Archivieren schließen müssen, werden aktuelle NAS-Operationen nach der Trennung der Verbindung fortgesetzt. Sie können die Schaltfläche **Verlassen** im Fenster **Task-Liste** für die NAS-Zurückschreibung verwenden, um die Verarbeitungsüberwachung zu verlassen, ohne die aktuelle Operation zu beenden.
8. (Optional) Um die Verarbeitung einer Operation zu überwachen, wählen Sie **Aktionen** > **IBM Spectrum Protect-Aktivitäten** im Hauptfenster aus.

Ergebnisse

Hinweise:

- Workstationsicherungen und ferne Sicherungen (NAS-Sicherungen) schließen sich in einem Zurückschreibungsfenster gegenseitig aus. Wenn ein Element für die Zurückschreibung ausgewählt wurde, muss das nächste Element, das Sie auswählen, denselben Typ aufweisen (entweder NAS oder Nicht-NAS).
- Für NAS-Knoten oder -Images werden keine Details auf der rechten Seite des Zurückschreibungsfensters angezeigt. Um Informationen zu einem NAS-Image anzuzeigen, heben Sie das NAS-Image hervor und wählen Sie **Anzeigen > Dateiinformationen** im Menü aus.
- Um NAS-Dateibereiche zu löschen, wählen Sie **Dienstprogramme > Dateibereiche löschen** aus. Sie können sowohl Workstationobjekte als auch ferne Objekte löschen.

Optionen und Befehle für die Zurückschreibung von NAS-Dateisystemen über die Befehlszeile

Dieser Abschnitt enthält einige Beispiele für Optionen und Befehle, die Sie zum Zurückschreiben von NAS-Dateisystemimages über die Befehlszeile verwenden können.

Tabelle 46. NAS-Optionen und -Befehle

Option oder Befehl	Definition	Seite
query node	Zeigt alle Knoten an, für die eine bestimmte Verwaltungsbenutzer-ID die Berechtigung zum Ausführen von Operationen hat. Die Verwaltungsbenutzer-ID sollte mindestens die Clienteignerberechtigung sowohl über den NAS-Knoten als auch den Client-Workstation-Knoten besitzen, der entweder von der Befehlszeile oder vom Web-Client aus verwendet wird.	„ Query Node “ auf Seite 762
query backup	Verwenden Sie den Befehl query backup mit der Option class , um Informationen zu den Dateisystemimages anzuzeigen, die für einen NAS-Dateiserver gesichert wurden.	„ Query Backup “ auf Seite 748
query filespace	Verwenden Sie den Befehl query filespace mit der Option class , um eine Liste der Dateibereiche anzuzeigen, die zu einem NAS-Knoten gehören.	„ Query Filespace “ auf Seite 754
restore nas	Schreibt das Image eines Dateisystems zurück, das zu einem NAS-Dateiserver gehört.	„ Restore NAS “ auf Seite 789
monitor process	Zeigt die aktuellen Sicherungs- und Zurückschreibungsprozesse für alle NAS-Knoten an, für die ein Benutzer mit Verwaltungsaufgaben die Berechtigung hat. Der Benutzer mit Verwaltungsaufgaben kann dann einen Prozess für die Überwachung auswählen.	„ Monitor Process “ auf Seite 742
cancel process	Zeigt die aktuellen Sicherungs- und Zurückschreibungsprozesse für alle NAS-Knoten an, für die ein Benutzer mit Verwaltungsaufgaben die Berechtigung hat. In der Anzeige kann der Benutzer mit Verwaltungsaufgaben einen Prozess zum Abbrechen auswählen.	„ Cancel Process “ auf Seite 719

Tabelle 46. NAS-Optionen und -Befehle (Forts.)

Option oder Befehl	Definition	Seite
delete filesystem	Verwenden Sie delete filesystem mit der Option <code>class</code> , um eine Liste der Dateibereiche anzuzeigen, die zu einem NAS-Knoten gehören. In dieser Liste können Sie einen Dateibereich zum Löschen auswählen.	„Delete Filespace“ auf Seite 727

Unabhängig von der Clientplattform wird in NAS-Dateisystemspezifikationen der Schrägstrich (/) als Trennzeichen verwendet. Zum Beispiel: /vol/vol0.

Anmerkung: Wird eine NAS-Zurückschreibungsoperation mithilfe des Befehlszeilenclients oder des Web-Clients eingeleitet, startet der Server einen Prozess, um die Operation einzuleiten, zu steuern und zu überwachen. Der Fortschritt in der Befehlszeilenschnittstelle des Clients lässt sich erst nach kurzer Zeit feststellen, da der Server eine Ladeoperation und andere erforderliche Tasks ausführen muss, bevor die Datenversetzung erfolgt. Der IBM Spectrum Protect-Befehlszeilenclient zeigt unter Umständen die Nachricht Unterbrochen... an, wenn der Ladevorgang erfolgt. Sie können diese Nachricht ignorieren.

Aktive oder inaktive Sicherungen zurückschreiben

Ihr Administrator legt fest, wie viele Sicherungsversionen IBM Spectrum Protect für jede Datei auf Ihrer Workstation aufbewahrt.

Sind mehrere Versionen einer Datei vorhanden, können ältere Versionen zurückgeschrieben werden, falls die aktuellste Sicherungsversion beschädigt ist. Die aktuellste Sicherungsversion ist die *aktive* Version. Jede andere Sicherungsversion ist eine *inaktive* Version.

Bei jeder Dateisicherung markiert IBM Spectrum Protect die neue Sicherungsversion als die aktive Sicherungsversion, und die letzte aktive Sicherungsversion wird zu einer inaktiven Version. Wenn die maximal zulässige Anzahl inaktiver Versionen erreicht ist, löscht IBM Spectrum Protect die älteste inaktive Version.

Soll eine inaktive Sicherungsversion zurückgeschrieben werden, müssen sowohl aktive als auch inaktive Versionen angezeigt werden. Klicken Sie dazu **Anzeigen** → **Aktive/inaktive Dateien anzeigen** an. Sollen nur die aktiven Versionen angezeigt werden (Standardwert), klicken Sie **Anzeigen** → **Nur aktive Dateien anzeigen** an. Wird versucht, mehrere Versionen einer Datei gleichzeitig zurückzuschreiben, wird nur die aktive Version zurückgeschrieben.

Verwenden Sie in der IBM Spectrum Protect-Befehlszeile die Option `inactive`, um sowohl aktive als auch inaktive Objekte anzuzeigen.

Zugehörige Verweise:

„Inactive“ auf Seite 471

Daten über die grafische Benutzerschnittstelle zurückschreiben

In diesem Abschnitt sind die Schritte aufgelistet, die Sie ausführen müssen, um Sicherungsversionen von einzelnen Dateien oder Unterverzeichnissen zurückzuschreiben.

Vorgehensweise

1. Klicken Sie auf **Zurückschreiben** im Hauptfenster. Das Fenster 'Zurückschreiben' wird angezeigt.
2. Erweitern Sie die Verzeichnisbaumstruktur. Wählen Sie die Auswahlfelder neben den Dateien oder Verzeichnissen, die zurückgeschrieben werden sollen, aus. Zum Suchen oder Filtern von Dateien klicken Sie auf das Symbol **Suchen** in der Funktionsleiste.
3. Die Suchkriterien in das Fenster 'Dateien suchen (Zurückschreiben)' eingeben.
4. Klicken Sie auf die Schaltfläche **Suchen**. Das Fenster 'Übereinstimmende Dateien (Zurückschreiben)' wird angezeigt.
5. Klicken Sie auf die Auswahlfelder neben den Dateien, die zurückgeschrieben werden sollen, und schließen Sie das Fenster 'Übereinstimmende Dateien (Zurückschreiben)'.
6. Die Filterkriterien in das Fenster 'Dateien suchen (Zurückschreiben)' eingeben.
7. Klicken Sie auf die Schaltfläche **Filter**. Das Fenster 'Zurückschreiben' zeigt die gefilterten Dateien an.
8. Klicken Sie auf die Auswahlfelder neben den gefilterten Dateien oder Verzeichnissen, die zurückgeschrieben werden sollen.
9. Um bestimmte Zurückschreibungsoptionen zu ändern, klicken Sie auf die Schaltfläche **Optionen**. Die geänderten Optionen sind *nur* während der aktuellen Sitzung wirksam.
10. Klicken Sie auf **Zurückschreiben**. Das Fenster 'Zurückschreibungsziel' wird angezeigt. Geben Sie die Informationen in das Fenster 'Zurückschreibungsziel' ein.
11. Klicken Sie auf **Zurückschreiben**. Im Fenster **Task-Liste** für die Zurückschreibung wird der Bearbeitungsstatus der Zurückschreibung angezeigt.

Ergebnisse

Anmerkung: Beachten Sie unter Mac OS X die folgenden Hinweise, wenn Sie Daten über die GUI zurückschreiben:

1. Wenn die **IBM Spectrum Protect-Tools für Administratoren** zum Starten des Clients verwendet werden, wird der Client mit der UID null ausgeführt. Dies bedeutet, dass der Root Eigner eines Ordners ist, den Sie als Ziel für die Zurückschreibung erstellen. Sie müssen die Berechtigungen des Ordners ändern, um auf die Dateien zugreifen zu können. Sie können den Eigner des Ordners in einem Terminalfenster mit dem sudo-Befehl **chown** ändern. Weitere Informationen zu dieser Task finden Sie in der Dokumentation zu Ihrem Betriebssystem.
2. Wenn Sie bei einer Dateizurückschreibung für die Option **replace** den Wert **no** angeben, werden vorhandene Dateien nicht überschrieben, aber vorhandene Verzeichnisse werden überschrieben. Sollen vorhandene Verzeichnisse während einer Zurückschreibungsoperation nicht überschrieben werden, wählen Sie die Schaltfläche **Optionen**, Dropdown-Menü **Alle ausgewählten Dateien und Verzeichnisse** => Option **Nur Dateien** aus.
3. Werden Ordner, die sich nur in der Groß-/Kleinschreibung unterscheiden, von einem UFS- oder HFSX-Dateisystem in ein HFS-Dateisystem zurückgeschrieben, schreibt der Client den Inhalt beider Ordner in einen einzigen Ordner zurück.

Beispiele für Zurückschreibungsbefehle

Dieser Abschnitt enthält einige Beispiele für Befehle **restore**, die für bestimmte Tasks verwendet werden müssen.

Die folgende Tabelle enthält Beispiele zur Verwendung des Befehls **restore** zum Zurückschreiben von Objekten aus dem IBM Spectrum Protect-Serverspeicher.

Tabelle 47. Beispiele für Zurückschreibungsbefehle

Task	Befehl	Hinweise
Die aktuellste Sicherungsversion der Datei /Users/monnett/Documents/h1.doc zurückschreiben, selbst wenn die Sicherung inaktiv ist.	<code>dsmc restore /Users/monnett/Documents/h1.doc -latest</code>	Ist die zurückzuschreibende Datei nicht mehr auf der Workstation des Benutzers vorhanden und wurde nach dem Löschen der Datei eine Teilsicherung ausgeführt, befindet sich keine aktive Sicherungsversion der Datei auf dem Server. In diesem Fall muss mit der Option <code>latest</code> die neueste Sicherungsversion zurückgeschrieben werden. IBM Spectrum Protect schreibt die aktuellste Sicherungsversion zurück, unabhängig davon, ob sie aktiv oder inaktiv ist. Weitere Informationen siehe „Latest“ auf Seite 499.
Eine Liste der aktiven und inaktiven Sicherungsversionen von Dateien anzeigen, aus der Sie die zurückzuschreibenden Versionen auswählen können.	<code>dsmc restore "/Users/monnett/Documents/*"-pick -inactive</code>	Wird versucht, eine aktive und eine inaktive Version einer Datei gleichzeitig zurückzuschreiben, wird nur die aktive Version zurückgeschrieben. „Pick“ auf Seite 528 und „Inactive“ auf Seite 471 enthalten weitere Informationen.
Die Datei /Users/monnett/Documents/h1.doc in ihr Ursprungsverzeichnis zurückschreiben.	<code>dsmc restore /Users/monnett/Documents/h1.doc</code>	Wird kein Ziel angegeben, werden die Dateien an ihre ursprüngliche Position zurückgeschrieben.
Die Datei /Users/monnett/Documents/h1.doc unter einem neuen Namen und in ein neues Verzeichnis zurückschreiben.	<code>dsmc restore /Users/monnett/Documents/h1.doc /Users/gordon/Documents/h2.doc</code>	Keine
Die Dateien im Verzeichnis /Users und in allen zugehörigen Unterverzeichnissen zurückschreiben.	<code>dsmc restore /Users/ -subdir=yes</code>	Beim Zurückschreiben eines bestimmten Pfads und einer bestimmten Datei führt IBM Spectrum Protect eine rekursive Zurückschreibung <i>aller</i> Unterverzeichnisse unter diesem Pfad und aller Instanzen der angegebenen Datei, die sich unter <i>jedem</i> dieser Unterverzeichnisse befinden, durch. Weitere Informationen zur Option subdir befinden sich im Abschnitt „Subdir“ auf Seite 605.
Alle Dateien im Verzeichnis /Users/gordon/Documents in ihrem Status am 17. August 2003 um 13:00 Uhr zurückschreiben.	<code>dsmc restore -pitd=8/17/2003 -pitt=13:00:00 /Users/gordon/Documents/</code>	Weitere Informationen zu den Optionen <code>pitdate</code> und <code>pittime</code> enthalten die Abschnitte „Pitdate“ auf Seite 529 und „Pittime“ auf Seite 530.

Tabelle 47. Beispiele für Zurückschreibungsbefehle (Forts.)

Task	Befehl	Hinweise
Alle Dateien aus dem Verzeichnis /Users/mike/Documents, die mit .bak enden, in das Verzeichnis /Users/mike/projectn/ zurückschreiben.	<code>dsmc restore "/Users/mike/Documents/*.bak" /Users/mike/projectn/</code>	Handelt es sich bei dem Ziel um ein Verzeichnis, muss der Begrenzer (/) als letztes Zeichen des Ziel angegeben werden. Wird der Begrenzer nicht angegeben und handelt es sich bei der angegebenen Quelle um ein Verzeichnis oder eine Dateispezifikation mit einem Platzhalterzeichen, wird ein Fehler angezeigt. Ist das Verzeichnis projectn nicht vorhanden, wird es erstellt.
Die in der Datei restorelist.txt angegebenen Dateien an eine andere Position zurückschreiben.	<code>dsmc restore -filelist=/Users/user2/Documents/restorelist.txt /Users/NewRestoreLocation/</code>	Weitere Informationen zum Zurückschreiben von Dateilisten befinden sich im Abschnitt „Filelist“ auf Seite 453.

Zugehörige Verweise:
„Restore“ auf Seite 771

Beispiele: Große Datenvolumen über die Befehlszeile zurückschreiben

Müssen sehr viele Dateien zurückgeschrieben werden, kann die Leistung verbessert werden, wenn anstelle der grafischen Benutzerschnittstelle der Befehl **restore** verwendet wird. Außerdem lässt sich die Leistung verbessern, wenn mehrere **restore**-Befehle gleichzeitig eingegeben werden.

Sollen beispielsweise alle Dateien im Dateisystem /home zurückgeschrieben werden, geben Sie Folgendes ein:

```
dsmc restore /home/ -subdir=yes -replace=all -tapeprompt=no
```

Werden jedoch mehrere Befehle für die Verzeichnisse im Dateibereich /home eingegeben, können die Dateien schneller zurückgeschrieben werden.

Es können beispielsweise folgende Befehle eingegeben werden:

```
dsmc restore /home/monnett/ -subdir=yes -replace=all -tapeprompt=no
dsmc restore /home/gillis/ -subdir=yes -replace=all -tapeprompt=no
dsmc restore /home/stewart/ -subdir=yes -replace=all -tapeprompt=no
```

Sie können auch die Option **quiet** in den **restore**-Befehlen verwenden, um Verarbeitungszeit einzusparen. Es werden jedoch keine Informationsnachrichten für einzelne Dateien angezeigt.

Anmerkung: Wenn Sie die geeigneten Werte für die Optionen **subdir**, **replace**, **tapeprompt** und **quiet** bereits in Ihrer Clientbenutzeroptionsdatei definiert haben, brauchen Sie diese Optionen nicht in die Befehle einzuschließen.

Werden mehrere Befehle zum Zurückschreiben von Dateien eingegeben, muss ein eindeutiger Teil des Dateibereichs in jedem Befehl **restore** angegeben werden. Es dürfen keine Überschneidungen bei den Dateispezifikationen in den Befehlen auftreten.

Mit dem Befehl **query backup** kann eine Liste der Verzeichnisse in einem Dateibereich angezeigt werden. Beispiel:

```
dsmc query backup -dirsonly -subdir=no /Users/
```

Im Allgemeinen können zwei bis vier **restore**-Befehle gleichzeitig eingegeben werden. Wie viele Befehle maximal gleichzeitig ausgeführt werden können, ohne die Leistung zu beeinträchtigen, ist abhängig von verschiedenen Faktoren, z. B. vom verfügbaren Speicher und von der Netzauslastung.

Mit welcher Geschwindigkeit Sie die Dateien zurückschreiben können, ist auch davon abhängig, wie viele Bandlaufwerke auf dem Server verfügbar sind und ob der Administrator die Kollokation verwendet, um Dateibereiche möglichst wenig Datenträgern zuzuordnen.

Befinden sich /Users/user1 und /Users/user2 beispielsweise auf demselben Band, muss das Zurückschreiben für /Users/user2 warten, bis das Zurückschreiben für /Users/user1 beendet ist. Befindet sich /Users/user3 jedoch auf einem anderen Band und stehen mindestens zwei Bandlaufwerke zur Verfügung, kann das Zurückschreiben für /Users/user3 und für /Users/user1 gleichzeitig beginnen.

Setzen Sie die ulimit-Systemwerte auf unbegrenzt (-1), wenn Sie sehr große Dateien (2 GB) mit HSM oder dem Client für Sichern/Archivieren zurückschreiben. Der Client kann diese großen Dateien mit ausreichenden Systemressourcen zurückschreiben. Wenn die ulimit-Werte auf niedrigere Werte gesetzt werden, könnten Zurückschreibungsfehler auftreten.

Standardzurückschreibung mit Abfrage, Zurückschreibung ohne Abfrage und wiederanlauffähige Zurückschreibung

In diesem Abschnitt werden die Standardzurückschreibung (klassische Zurückschreibung), die Zurückschreibung ohne Abfrage und die wiederanlauffähige Zurückschreibung beschrieben.

Standardzurückschreibungsprozess mit Abfrage

Der Standardzurückschreibungsprozess mit Abfrage ist auch als klassisches Zurückschreiben bekannt. In diesem Abschnitt wird die Standardzurückschreibung mit Abfrage beschrieben.

Die Standardzurückschreibung mit Abfrage arbeitet wie folgt:

- Der Client fragt den Server nach einer Liste mit Dateien ab, die für den Clientdateibereich gesichert wurden, der zurückgeschrieben werden soll.
- Der Server sendet eine Liste der gesicherten Dateien, die den Zurückschreibungsbedingungen entsprechen. Sollen sowohl aktive als auch inaktive Dateien zurückgeschrieben werden, sendet der Server Informationen zu allen gesicherten Dateien an den Client.
- Die vom Server ausgegebene Dateiliste wird im Clientspeicher sortiert, um die Zurückschreibungsreihenfolge der Dateien zu bestimmen und die für die Zurückschreibung erforderlichen Bandladevorgänge zu minimieren.
- Der Client teilt dem Server mit, Dateidaten und Verzeichnisobjekte zurückzuschreiben.
- Die Verzeichnisse und Dateien, die zurückgeschrieben werden sollen, werden vom Server an den Client gesendet.

Prozess für Zurückschreibung ohne Abfrage

Beim Zurückschreiben ohne Abfrage wird der Server nicht nach jedem zurückzuschreibenden Objekt abgefragt, sondern es wird eine einzelne Zurückschreibungsanforderung an den Server gesendet.

1. Der Client teilt dem Server mit, dass eine Zurückschreibung ohne Abfrage ausgeführt werden soll, und stellt dem Server die Details zu den Dateibereichen, Verzeichnissen und Dateien zur Verfügung.
2. Der Server verwendet eine separate Tabelle, um die Einträge aufzuzeichnen, die die Zurückschreibung führen.
3. Die zurückzuschreibenden Daten werden an den Client gesendet. Die auf Platte gespeicherten Datei- und Verzeichnisobjekte werden sofort gesendet, da ein Sortieren dieser Daten vor dem Zurückschreiben des Objekts nicht erforderlich ist.
4. Sie können Mehrfachsitzungen verwenden, um die Daten zurückzuschreiben. Befinden sich die Daten auf mehreren Bändern, sind mehrere Mountpunkte auf dem Server verfügbar. Die Kombination der Option **resourceutilization** und **MAXNUMMP** ermöglicht Mehrfachsitzungen.

Wenn Sie eine uneingeschränkte Quellendateispezifikation mit Platzhalterzeichen in den Befehl **restore** eingeben und keine der folgenden Optionen angeben, verwendet der Client eine Methode *Zurückschreibung ohne Abfrage* zum Zurückschreiben von Dateien und Verzeichnissen vom Server: **inactive**, **latest**, **pick**, **fromdate**, **todate**. Diese Methode wird als *Zurückschreiben ohne Abfrage* bezeichnet, weil der Server nicht nach jedem zurückzuschreibenden Objekt abgefragt, sondern eine einzige Zurückschreibungsanforderung an den Server gesendet wird. In diesem Fall gibt der Server die Dateien und Verzeichnisse ohne weitere Aktion durch den Client an den Client zurück. Der Client akzeptiert lediglich die vom Server kommenden Daten und schreibt sie an das im Befehl **restore** angegebene Ziel zurück.

Bei Verwendung des IBM Spectrum Protect-GUI-Clients wäre ein Beispiel für einen unbeschränkten Befehl mit Platzhalterzeichen die Auswahl eines Ordners im Fenster 'Baumstruktur zurückschreiben'. Ein Beispiel für einen eingeschränkten Befehl mit Platzhalterzeichen wäre die Auswahl einzelner Dateien aus einem Ordner.

Im Befehlszeilenclient wäre ein Beispiel für einen unbeschränkten Befehl mit Platzhalterzeichen:

```
"/Users/user1/Documents/2004/*"  
/home/mydocs/2004/*
```

Ein Beispiel für eine eingeschränkte Dateispezifikation mit Platzhalterzeichen wäre:

```
/Users/user1/Documents/2004/sales.*  
/home/mydocs/2004/sales.*
```

Wiederanlauffähiger Zurückschreibungsprozess

Wird der Zurückschreibungsprozess aufgrund eines Stromausfalls oder eines Netzfehlers gestoppt, zeichnet der Server den Punkt auf, an dem dieser Ausfall oder Fehler erfolgte.

Dieser Punkt ist dem Client als *wiederanlauffähige Zurückschreibung* bekannt. Es können mehrere wiederanlauffähige Zurückschreibungssitzungen vorhanden sein. Verwenden Sie den Befehl **query restore** oder wählen Sie **Wiederanlauffähige Zurückschreibungen** im Menü 'Aktionen' aus, um festzustellen, ob Ihr Client über wiederanlauffähige Zurückschreibungssitzungen in der Serverdatenbank verfügt.

Eine wiederanlauffähige Zurückschreibung muss abgeschlossen werden, bevor weitere Sicherungen des Dateisystems versucht werden. Versuchen Sie, die unterbrochene Zurückschreibung zu wiederholen oder den Zieldateibereich zu sichern, schlägt der Versuch fehl, da die ursprüngliche Zurückschreibung nicht abgeschlossen wurde. Sie können die Zurückschreibung an dem Unterbrechungspunkt erneut

starten, indem Sie den Befehl **restart restore** eingeben, oder Sie können die wiederanlauffähige Zurückschreibung löschen, indem Sie den Befehl **cancel restore** verwenden.

Im Dialogfenster **Wiederanlauffähige Zurückschreibungen** in der IBM Spectrum Protect-GUI können Sie die unterbrochene Zurückschreibung auswählen und löschen oder die Zurückschreibung erneut starten. Wenn Sie die unterbrochene Zurückschreibung erneut starten, wird mit der ersten Transaktion begonnen. Diese kann aus einer oder aus mehreren Dateien bestehen, die nicht vollständig zurückgeschrieben war oder waren, als die Unterbrechung auftrat. Aus diesem Grund können Sie einige Aufforderungen zum Ersetzen für Dateien aus der unterbrochenen Transaktion empfangen, die bereits zurückgeschrieben wurden.

Führen Sie folgende Schritte aus, um wiederanlauffähige Zurückschreibungen über die GUI auszuführen:

1. Wählen Sie **Aktionen** -> **Wiederanlauffähige Zurückschreibungen** in der Hauptanzeige aus.
2. Wählen Sie die wiederanlauffähige Zurückschreibungssitzung aus, die ausgeführt werden soll.
3. Klicken Sie auf die Schaltfläche **Erneut starten** unten auf der Anzeige.

Zugehörige Verweise:

„Resourceutilization“ auf Seite 557

„Restore“ auf Seite 771

Solaris Zettabyte-Dateisysteme (ZFS) zurückschreiben

ZFS-Dateisysteme (Zettabyte File System) verwenden Speicherpools zum Verwalten von physischen Speichereinheiten.

Wie Sie ein ZFS-Dateisystem zurückschreiben, ist davon abhängig, wie das Dateisystem gesichert wurde.

- Wenn Sie alle Dateien und Ordner als separate Objekte gesichert haben, können Sie sie mit einer Zurückschreibung auf Dateiebene zurückschreiben. Beispiel:

```
dsmc restore /tank/myZFS/ -subdir=yes -replace=all
```

Sie dürfen eine Zurückschreibung auf Dateiebene nicht für eine Wiederherstellung nach einem Katastrophenfall ausführen. Auch wenn Sie alle Systemdateien und -ordner erfolgreich aus einer Sicherung zurückschreiben, die von einem Client für Sichern/Archivieren erstellt wurde, kann das zurückgeschriebene System instabil sein oder fehlschlagen.

- Wenn Sie eine vollständige ZFS-Momentaufnahme als einzelne Datei gesichert haben, müssen Sie die Momentaufnahme-Datei vom Server in ein temporäres Verzeichnis zurückschreiben. Beispiel:

```
dsmc restore /tmpdir/mySnapshotfile
```

Anschließend können Sie das Dateisystem mithilfe der Oracle Solaris ZFS-Befehle aus der Momentaufnahme-Datei zurückschreiben. Beispiel:

```
zfs receive tank/myZFS@mySnapshot < /tmpdir/mySnapshotFile
```

Der Vorteil des Zurückschreibens eines ZFS aus einer Momentaufnahme-Datei liegt darin, dass im Notfall das gesamte Dateisystem zurückgeschrieben werden kann.

Ausführliche Informationen zum Zurückschreiben von Daten auf ZFS-Dateisystemen finden Sie in der bei Oracle erhältlichen Produktdokumentation. Wenn Sie

einen ZFS-Root-Pool zurückschreiben, lesen Sie die Abschnitte, in denen die Neuerstellung des Root-Pools und die Wiederherstellung von Root-Pool-Momentaufnahmen beschrieben werden.

Zugehörige Tasks:

„Solaris Zettabyte-Dateisysteme (ZFS) sichern“ auf Seite 227

Zusätzliche Zurückschreibungstasks

In diesem Abschnitt werden einige weiterführende Hinweise für das Zurückschreiben von Daten erläutert.

Einen anderen Benutzer zum Zurückschreiben und Abrufen Ihrer Dateien berechtigen

Sie können andere Benutzer an derselben Workstation oder an einer anderen Workstation dazu berechtigen, Sicherungsversionen Ihrer Dateien zurückzuschreiben oder Archivierungskopien Ihrer Dateien abzurufen.

Informationen zu diesem Vorgang

Auf diese Weise können mehrere Benutzer oder Workstations, die mit einem anderen Knotennamen verwendet werden, Dateien gemeinsam benutzen. Soll ein Benutzer an einer anderen Workstation dazu berechtigt werden, Ihre Dateien zurückzuschreiben oder abzurufen, muss auf der anderen Workstation einer der UNIX-Clients aktiv und die Workstation muss bei Ihrem Server registriert sein.

Anmerkung: Mac OS X kann *nur* Mac OS X-Knoten zurückschreiben.

Wie folgt vorgehen, um andere Benutzer zu berechtigen, die eigenen Dateien zurückzuschreiben oder abzurufen:

Vorgehensweise

1. Klicken Sie auf **Dienstprogramme** → **Knotenzugriffsliste** im Hauptfenster. Das Fenster Knotenzugriffsliste wird angezeigt.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**. Das Fenster 'Zugriffsregel hinzufügen' wird angezeigt.
3. Im Fenster 'Zugriffsregel hinzufügen' wählen Sie ein Element im Feld 'Zugriff erlauben für' aus, um den Typ der Daten anzugeben, auf die der andere Benutzer zugreifen kann. Sie können entweder gesicherte oder archivierte Objekte auswählen.
4. Geben Sie in das Feld 'Zugriff erteilen für Knoten' den Knotennamen der Host-Workstation des Benutzers ein, der auf Ihre Daten zugreifen darf.
5. Geben Sie in das Feld 'Benutzer' den Namen des Benutzers auf einem Knoten ein, der auf Ihre Daten zugreifen kann.
6. Wählen Sie im Feld 'Dateibereich und Verzeichnis' den Dateibereich und das Verzeichnis aus, auf den bzw. das der Benutzer zugreifen kann. Sie können jeweils einen Dateibereich und ein Verzeichnis auswählen. Wenn Sie dem Benutzer Zugriff auf einen anderen Dateibereich oder ein anderes Verzeichnis geben wollen, müssen Sie eine andere Zugriffsregel erstellen.
7. Soll der Zugriff des Benutzers auf bestimmte Dateien im Verzeichnis begrenzt werden, geben Sie den Namen oder das Muster für den Namen der Dateien auf dem Server, auf die der andere Benutzer zugreifen darf, im Feld Dateiname an. Im Feld 'Dateiname' kann nur ein Eintrag eingegeben werden. Dabei kann es sich um den Namen einer einzelnen Datei oder um ein Muster han-

deln, das mit einem oder mehreren Dateien übereinstimmt. Es kann ein Platzhalterzeichen als Teil des Musters verwendet werden. Ihr Eintrag muss mit Dateien übereinstimmen, die auf dem Server gespeichert wurden.

8. Für die Java-GUI: Wenn Sie Zugriff auf alle Dateien erteilen wollen, die mit der Dateinamenspezifikation innerhalb des ausgewählten Verzeichnisses einschließlich der Unterverzeichnisse übereinstimmen, klicken Sie auf **Unterverzeichnisse einschließen**.
9. Klicken Sie auf die Schaltfläche **OK**, um die Zugriffsregel zu sichern und das Fenster 'Zugriffsregel hinzufügen' zu schließen.
10. Die von Ihnen erstellte Zugriffsregel wird im Listenfenster des Fensters 'Knotenzugriffsliste' angezeigt. Nach Beendigung der Arbeit im Fenster 'Knotenzugriffsliste' klicken Sie auf die Schaltfläche **OK**. Wenn Sie Ihre Änderungen nicht sichern möchten, klicken Sie auf **Abbrechen** oder schließen Sie das Fenster.

Ergebnisse

In der Befehlszeilenschnittstelle des Clients verwenden Sie den Befehl **set access**, um einen anderen Knoten zu berechtigen, Ihre Dateien zurückzuschreiben oder abzurufen. Sie können auch den Befehl **query access** verwenden, um Ihre aktuelle Liste einzusehen, und den Befehl **delete access**, um Knoten aus der Liste zu löschen.

Zugehörige Verweise:

„Delete Access“ auf Seite 720

„Query Access“ auf Seite 745

„Set Access“ auf Seite 814

Dateien von einem anderen Clientknoten zurückschreiben oder abrufen

Nachdem andere Benutzer Ihnen den Zugriff auf ihre Dateien auf dem Server erteilt haben, können Sie diese Dateien in Ihr lokales System zurückschreiben oder abrufen.

Informationen zu diesem Vorgang

Sie können Dateibereiche für einen anderen Benutzer auf dem Server anzeigen, die Sicherungsversionen für einen anderen Benutzer zurückschreiben oder die Archivierungskopien für einen anderen Benutzer in Ihr lokales Dateisystem abrufen:

Vorgehensweise

1. Klicken Sie auf **Dienstprogramme** im Hauptfenster.
2. Klicken Sie auf **Zugriff auf anderen Knoten**. Das Fenster 'Zugriff auf anderen Knoten' wird angezeigt.
3. Geben Sie den Knotennamen der Host-Workstation des Benutzers in das Feld 'Knotenname' ein. Den Benutzernamen in das Feld 'Benutzername' eingeben.
4. Klicken Sie auf die Schaltfläche **Definieren**.

Ergebnisse

Wird mit Befehlen gearbeitet, können mit den Optionen `fromnode` und `fromowner` der Knotenname und der Name des Benutzers, der Eigner der Dateien ist, angegeben werden.

Sollen beispielsweise Dateien in eines Ihrer eigenen Dateisysteme zurückgeschrieben werden, die auf einer Workstation mit dem Namen Knoten1 gesichert wurden und deren Eigner ein Benutzer mit dem Namen Anne ist, Folgendes eingeben:

```
dsmc restore -fromn=knoten1 -fromo=anne "/home/proj/*" /home/gillis/
```

Verwenden Sie den Befehl **query filespace**, um eine Liste von Dateibereichen abzurufen. Soll beispielsweise eine Liste der Dateibereiche, deren Eigner Anne ist, für Knoten1 angezeigt werden, Folgendes eingeben:

```
dsmc query filespace -fromn=knoten1 -fromo=anne
```

Zugehörige Verweise:

„Fromnode“ auf Seite 461

„Query Filespace“ auf Seite 754

„Restore“ auf Seite 771

„Retrieve“ auf Seite 805

Dateien auf eine andere Workstation zurückschreiben oder abrufen

Von einer anderen Workstation können Dateien zurückgeschrieben oder abgerufen werden, die bereits von Ihrer eigenen Workstation gesichert wurden. Sie müssen das IBM Spectrum Protect-Kennwort kennen, das Ihrem Knoten zugeordnet ist.

Verwenden Sie zum Zurückschreiben oder Abrufen von Dateien auf eine andere Workstation die Option `virtualnodename`, um den Knotennamen der Workstation anzugeben, auf der die Dateien gesichert wurden. Die Option `virtualnodename` kann nicht auf den Hostnamen der Workstation gesetzt werden. Sie können die Option `virtualnodename` verwenden, wenn Sie IBM Spectrum Protect starten, oder Sie können die Option `virtualnodename` zu Ihrer Clientbenutzeroptionsdatei `dsm.opt` hinzufügen. Verwenden Sie die Option `virtualnodename` im Befehl **dsmj**, wenn Sie ausnahmsweise die Workstation eines anderen Benutzers verwenden und die zugehörige Clientbenutzeroptionsdatei nicht aktualisieren wollen.

IBM Spectrum Protect fordert das Kennwort für Ihren ursprünglichen Knoten an. Nach der Eingabe des korrekten Kennworts werden alle Dateisysteme der ursprünglichen Workstation in dem Fenster "Zurückschreiben" oder "Abrufen" angezeigt. Sie können Dateien wie auf Ihrer eigenen Workstation zurückschreiben oder abrufen.

Wichtig: Wird diese Methode verwendet, um auf Dateien zuzugreifen, haben Sie auf alle Dateien Zugriff, die auf Ihrer Workstation gesichert und archiviert wurden. Sie werden als virtueller Root betrachtet.

Die Option `virtualnodename` kann in einem Befehl verwendet werden. Sollen beispielsweise die Dateien in *projx* zurückgeschrieben werden, Folgendes eingeben:

```
dsmc restore -virtualnodename=nodeone „/home/monnett/projx/*“
```

Sollen die Dateien auf der anderen Workstation nicht in dasselbe Verzeichnis zurückgeschrieben oder abgerufen werden, geben Sie ein anderes Ziel ein.

Diese Hinweise gelten sowohl für das Zurückschreiben als auch für das Abrufen von Dateien.

Platte nach Plattenverlust zurückschreiben

Sie können Ihre Dateien nur wiederherstellen, wenn Sie den Client ausführen können. Steht die Platte, die den Client enthält, nicht zur Verfügung (beispielsweise weil sie gestohlen wurde oder aufgrund eines Hardwarefehlers), muss der Client erneut installiert werden, bevor die Dateien wiederhergestellt werden können. Geht auch die Platte verloren, die das Betriebssystem und die DFV-Software enthält, müssen Sie diese wiederherstellen, bevor Sie eine Verbindung zum IBM Spectrum Protect-Server herstellen können.

Informationen zu diesem Vorgang

Der Benutzer kann sich gegen diese Verluste schützen, indem er immer die Installationsdatenträger verfügbar hat, mit denen er einen Status des Systems zurückschreiben kann, der es erlaubt, die Verbindung zum Server herzustellen und mit der Wiederherstellung der Daten zu beginnen. Die Installationsdatenträger sollten Folgendes enthalten:

Vorgehensweise

1. Ein startfähiges Betriebssystem, mit dem Basisfunktionen ausgeführt werden können.
2. Ein korrekt konfiguriertes Kommunikationsprogramm, das eine Datenübertragung mit dem Server ermöglicht.
3. Ein Client mit entsprechend angepassten Optionsdateien. Diese Task kann mithilfe der Befehlszeilenschnittstelle des Clients ausgeführt werden.


Ergebnisse

Das verwendete Kommunikationspaket bestimmt, welche Dateien benötigt werden. Die Handbücher zum Betriebssystem und zur DFV-Software helfen bei der Zusammenstellung der Installationsdatenträger.

Ist auf Ihrer Workstation auch der IBM Spectrum Protect for Space Management installiert, müssen die Installationsdatenträger den HSM-Befehlszeilenclient enthalten.

Anmerkung: Der Administrator kann Operationen zum Zurückschreiben planen, was besonders hilfreich sein kann, wenn eine große Anzahl Dateien zurückgeschrieben werden muss.

Zugehörige Konzepte:

 Sichern und Zurückschreiben auf speicherverwalteten Dateisystemen

Dateibereiche löschen

Erteilt der IBM Spectrum Protect-Administrator einem Benutzer die Berechtigung, kann der Benutzer vollständige Dateibereiche aus dem Server löschen.

Informationen zu diesem Vorgang

Beim Löschen eines Dateibereichs werden alle Dateien und Images, sowohl Sicherungsversionen als auch Archivierungskopien, innerhalb dieses Dateibereichs gelöscht. Wenn Sie beispielsweise den Dateibereich für Ihr Dateisystem `/home/monnet` löschen, löschen Sie damit jede Sicherungskopie für jede Datei in diesem Dateisystem sowie jede Datei, die Sie von diesem Dateisystem archiviert haben. **Das Lö-**

schen eines Dateibereichs muss gründlich überlegt werden. Sie müssen ein berechtigter Benutzer sein, um diese Task auszuführen.

Sie können einzelne Sicherungsversionen löschen, indem Sie den Befehl **delete backup** verwenden.

Sie können Dateibereiche mithilfe der GUI des Clients für Sichern/Archivieren oder der Clientbefehlszeilenschnittstelle löschen. Verwenden Sie zum Löschen von NAS-Dateibereichen den Web-Client oder die Befehlszeilenschnittstelle des Clients.

Soll ein Dateibereich mit der grafischen Benutzerschnittstelle gelöscht werden, führen Sie die folgenden Schritte aus:

Vorgehensweise

1. Wählen Sie **Dienstprogramme** → **Dateibereiche löschen** im Hauptfenster aus.
2. Klicken Sie auf die Auswahlfelder neben den Dateibereichen, die gelöscht werden sollen.
3. Klicken Sie auf die Schaltfläche **Löschen**. Der Client fordert Sie zur Bestätigung auf, bevor der Dateibereich gelöscht wird.

Ergebnisse

Sie können einen Dateibereich auch mit dem Befehl **delete filepace** löschen. Verwenden Sie die Option *class* im Befehl **delete filepace**, um NAS-Dateibereiche zu löschen.

Zugehörige Verweise:

„Class“ auf Seite 374

„Delete Backup“ auf Seite 722

„Delete Filespace“ auf Seite 727

SELinux für das Zurückschreiben von Dateien auf dem Red Hat Enterprise Linux 5-Client aktivieren

Wenn Sie Benutzer ohne Rootberechtigung sind und versuchen, Dateien auf einem Red Hat Enterprise Linux 5-Client zurückzuschreiben, müssen Sie zuerst SELinux aktivieren.

Wenn Sie SELinux nicht aktivieren, werden Sie beim Zurückschreiben von Dateien mit geänderten erweiterten Attributen Probleme bekommen.

Kapitel 6. Daten archivieren und abrufen (UNIX und Linux)

Sie können selten verwendete Dateien auf dem IBM Spectrum Protect-Server archivieren und bei Bedarf abrufen. Das Archivieren und Abrufen von Dateien ist dem Sichern und Zurückschreiben von Dateien ähnlich. Viele Fenster und Konzepte sind ähnlich.

Mit Ausnahme der Prozeduren für den Profileditor gelten alle primären Archivierungs- und Abrufprozeduren in diesem Abschnitt auch für den Web-Client.

Sie können die folgenden primären Archivierungs- und Abruftasks ausführen:

- „Daten über die grafische Benutzerschnittstelle archivieren“
- „Beispiele für das Archivieren von Daten über die Befehlszeile“ auf Seite 280
- „Archivierungsdaten löschen“ auf Seite 284
- „Daten über die grafische Benutzerschnittstelle abrufen“ auf Seite 287
- „Beispiele für das Abrufen von Daten über die Befehlszeile“ auf Seite 287

Zugehörige Konzepte:

Kapitel 4, „Daten sichern“, auf Seite 167

Zugehörige Tasks:

„Web-Client-Sitzung starten“ auf Seite 158

Dateien archivieren

Sollen Dateien archiviert werden, müssen diese explizit zum Archivieren ausgewählt werden. Der Benutzer kann die Dateien auswählen, indem er eine Dateispezifikation verwendet oder indem er die Dateien aus einer Verzeichnisbaumstruktur auswählt.

Der Administrator kann Zeitpläne zur automatischen Archivierung bestimmter Dateien auf der Workstation definieren. In den folgenden Abschnitten ist beschrieben, wie Dateien ohne Zeitpläne archiviert werden.

Zugehörige Tasks:

„Client-Scheduler-Prozess für die Ausführung als Hintergrundtask und den automatischen Start beim Systemstart definieren“ auf Seite 297

Daten über die grafische Benutzerschnittstelle archivieren

Dateien oder Dateigruppen können unter Verwendung von Dateinamen archiviert werden. Sie können Dateien, die bestimmten Suchkriterien entsprechen, mithilfe einer Verzeichnisstruktur auswählen.

Vorgehensweise

Archivieren Sie Dateien mit der folgenden Prozedur.

1. Klicken Sie auf **Archivieren** im Hauptfenster.
2. Erweitern Sie im Fenster **Archivieren** die Verzeichnisbaumstruktur, indem Sie auf das Pluszeichen (+) oder auf das Ordnersymbol neben einem Objekt in der Baumstruktur klicken. Zum Suchen oder Filtern von Dateien klicken Sie auf das Symbol **Suchen** in der Funktionsleiste.
3. Geben Sie die Suchkriterien in das Fenster **Dateien suchen** ein.

4. Klicken Sie auf **Suchen**.
5. Klicken Sie im Fenster **Übereinstimmende Dateien** auf die Auswahlfelder neben den Dateien, die archiviert werden sollen, und schließen Sie das Fenster **Übereinstimmende Dateien**.
6. Geben Sie die Filterkriterien in das Fenster **Dateien suchen** ein.
7. Klicken Sie auf **Filter**. Im Fenster **Archivieren** werden die gefilterten Dateien angezeigt.
8. Klicken Sie auf die Auswahlfelder neben den gefilterten Dateien oder Verzeichnissen, die archiviert werden sollen.
9. Geben Sie im Feld **Beschreibung** eine Beschreibung für das Archivierungspaket an, akzeptieren Sie die Standardbeschreibung oder wählen Sie eine vorhandene Beschreibung aus. Die maximale Länge einer Beschreibung ist 254 Zeichen. Wird eine vorhandene Archivierungsbeschreibung verwendet, werden die ausgewählten Dateien oder Verzeichnisse dem Archivierungspaket hinzugefügt. Alle Archivierungspakete mit derselben Beschreibung werden zum Abrufen, Abfragen und Löschen zusammengefasst.
10. Um bestimmte Archivierungsoptionen zu ändern, klicken Sie auf **Optionen**. Die geänderten Optionen sind nur während der aktuellen Sitzung wirksam.
11. Klicken Sie auf **Archivieren**. Im Fenster **Task-Liste** für die Archivierung wird der Verarbeitungsstatus der Archivierung angezeigt.

Beispiele für das Archivieren von Daten über die Befehlszeile

Archivierungsservices werden angefordert, um Kopien von Dateien für die spätere Verwendung, zu Dokumentationszwecken oder aufgrund gesetzlicher Anforderungen in ihrem aktuellen Status aufzubewahren. Dieser Abschnitt enthält einige Beispiele für das Archivieren von Daten über die Befehlszeile.

Sie können eine einzelne Datei, eine Dateigruppe oder alle Dateien in einem Verzeichnis oder Unterverzeichnis archivieren. Nach dem Archivieren einer Datei können Sie die Originaldatei von Ihrer Workstation löschen.

Die folgende Tabelle enthält Beispiele zur Verwendung des Befehls **archive** zum Archivieren von Objekten.

Tabelle 48. Beispiele für Archivierungsbefehle

Task	Befehl	Hinweise
Alle Dateien im Verzeichnis /home/proj1 mit der Dateierweiterung .txt archivieren.	dsmc archive "/home/proj1/*.txt"	Mithilfe von Platzhalterzeichen können mehrere Dateien gleichzeitig archiviert werden.
Alle Dateien im Verzeichnis /home/jones/proj/ archivieren und die Dateien auf Ihrer Workstation löschen.	dsmc archive /home/jones/proj/ -deletefiles	Werden die archivierten Dateien wieder auf der Workstation benötigt, können sie jederzeit abgerufen werden. Weitere Informationen zu der Option deletefiles finden Sie in „Deletefiles“ auf Seite 396.

Tabelle 48. Beispiele für Archivierungsbefehle (Forts.)

Task	Befehl	Hinweise
Die Dateien /home/jones/h1.doc und /home/jones/test.doc archivieren.	<code>dsmc archive /home/jones/h1.doc /home/jones/test.doc</code>	Geben Sie die Option <code>removeoperandlimit</code> mit dem Befehl archive an, wird die Beschränkung auf 20 Operanden nicht umgesetzt und nur durch die verfügbaren Ressourcen oder andere Begrenzungen des Betriebssystems eingeschränkt. Mit dieser Option können Sie mehr als 20 Dateien in einem einzelnen Befehl angeben. Weitere Informationen zu dieser Option finden Sie in „Removeoperandlimit“ auf Seite 546.
Eine Liste von Dateien in der Datei /home/avi/filelist.txt archivieren.	<code>dsmc archive -filelist=/home/avi/filelist.txt</code>	Verwenden Sie die Option <code>filelist</code> , um eine Liste von Dateien zu verarbeiten. Weitere Informationen finden Sie in „Filelist“ auf Seite 453.
Die Datei /home/jones/ch1.doc archivieren und der Archivierungskopie eine Beschreibung zuordnen.	<code>dsmc archive /home/jones/ch1.doc -description="Kapitel 1, erste Version"</code>	Wenn Sie keine Beschreibung im Befehl archive angeben, lautet der Standardwert Archivierungsdatum:x; hierbei gibt x das aktuelle Systemdatum an. Weitere Informationen zu der Option <code>description</code> finden Sie in „Description“ auf Seite 397.
Alle Dateien im Verzeichnis /home/jones/proj/ und seinen Unterverzeichnissen archivieren.	<code>dsmc archive /home/jones/proj/ -subdir=yes</code>	Weitere Informationen zu der Option <code>subdir</code> finden Sie in „Subdir“ auf Seite 605.
Die Option <code>v2archive</code> im Befehl archive verwenden, um nur Dateien im Verzeichnis /home/relx/dir1 zu archivieren, aber nicht die Verzeichnisse <code>relx</code> oder <code>dir1</code> .	<code>dsmc archive "/home/relx/dir1/" -v2archive</code>	Der Client für Sichern/Archivieren archiviert nur Dateien im Verzeichnis /home/relx/dir1. Verzeichnisse in diesem Pfad werden nicht verarbeitet. Weitere Informationen zu der Option <code>v2archive</code> finden Sie in „V2archive“ auf Seite 627.
Verwenden Sie die Option <code>archmc</code> im Befehl archive , um die verfügbare Verwaltungsklasse für Ihre Maßnahmendomäne anzugeben, an die Sie Ihre archivierten Dateien binden wollen.	<code>dsmc archive -archmc=ret2yrs /home/plan/proj1/budget.jan</code>	Weitere Informationen zu der Option <code>archmc</code> finden Sie in „Archmc“ auf Seite 357. Weitere Informationen zu Verwaltungsklassen siehe Kapitel 9, „Speicherverwaltungsmaßnahmen“, auf Seite 309.
Unter der Annahme, dass Sie eine Momentaufnahme des Dateisystems /usr initiiert und die Momentaufnahme als /snapshot/day1 angehängt haben, archivieren Sie die Verzeichnisbaumstruktur /usr/dir1/sub1 aus der lokalen Momentaufnahme und verwalten Sie sie auf dem IBM Spectrum Protect-Server unter dem Dateibereichsnamen /usr.	<code>dsmc archive /usr/dir1/sub1/ -subdir=yes -snapshotroot=/snapshot/day1</code>	Der Client betrachtet den Wert für <code>snapshotroot</code> als Dateibereichsnamen. Weitere Informationen finden Sie in „Snapshotroot“ auf Seite 593.

Zugehörige Verweise:

„Archive“ auf Seite 692

Lokale Momentaufnahme einem Serverdateibereich zuordnen

Um Daten in der lokalen Momentaufnahme den realen Dateibereichsdaten zuzuordnen, die auf dem IBM Spectrum Protect-Server gespeichert sind, verwenden Sie die Option `snapshotroot`.

Wenn Sie die Option `snapshotroot` im Befehl **archive** für eine Anwendung eines anderen Anbieters verwenden, die eine Momentaufnahme eines logischen Datenträgers erstellt, können Sie die Daten der lokalen Momentaufnahme den realen Dateibereichsdaten zuordnen, die auf dem IBM Spectrum Protect-Server gespeichert sind.

Die Option `snapshotroot` kann nicht zum Erstellen einer Datenträgermomentaufnahme verwendet werden, sondern sie dient zur Verwaltung der Daten, die von einer Datenträgermomentaufnahme erstellt werden.

Zugehörige Verweise:

„Snapshotroot“ auf Seite 593

Daten mit dem Clientknoten-Proxy archivieren

Archivierungen mehrerer Knoten, die Speicher gemeinsam benutzen, können zu einem einheitlichen Zielknotennamen auf dem IBM Spectrum Protect-Server konsolidiert werden.

Vorbereitende Schritte

Alle Agentenknoten in der Mehrfachknotenumgebung sollten denselben Plattformtyp aufweisen. Verwenden Sie Zielknoten nicht als traditionelle Knoten. Verwenden Sie sie nur für Mehrfachknotenverarbeitung.

Beachten Sie die folgenden Features einer Sitzung mit Proxy-Berechtigung:

- Eine Proxy-Operation verwendet die Einstellungen für den Zielknoten (beispielsweise **maxnummp** und **deduplication**) sowie Zeitpläne, die auf dem IBM Spectrum Protect-Server definiert sind. Die Einstellungen und Zeitpläne für den Agentenknoten auf dem IBM Spectrum Protect-Server werden ignoriert.
- Sie können keine Sicherungen oder Zurückschreibungen von Systemstatus oder Systemservices ausführen.
- Sie können nicht auf einen anderen Knoten zugreifen (weder von der GUI-Drop-down-Liste noch mithilfe der Option `fromnode`).
- Sie können keine NAS-Sicherung oder -Zurückschreibung ausführen.

Informationen zu diesem Vorgang

Die Konsolidierung archivierter Dateien zu einem einheitlichen Zielknotennamen auf dem Server ist nützlich, wenn die für die Durchführung der Archivierung verantwortliche Workstation sich mit der Zeit ändern kann, wie es z. B. bei einem Xsan oder Cluster der Fall ist. Mit der Option `asnodename` können Daten außerdem von einem anderen System zurückgeschrieben werden als dem, auf dem die Sicherung ausgeführt wurde. Verwenden Sie die Option `asnodename` mit dem entsprechenden Befehl, um unter dem Zielknotennamen Daten auf dem IBM Spectrum Protect-Server zu sichern, zu archivieren, zurückzuschreiben oder abzurufen. Diese Unterstützung ist nur mit IBM Spectrum Protect Version 5.3 und höher verfügbar.

Tivoli Storage Manager FastBack-Clients werden ebenfalls mit einem Clientknoten-Proxy gesichert.

Die Konfiguration Ihrer Umgebung für Proxy-Operationen besteht aus mehreren Schritten, zu denen das Definieren von Optionen und Befehlen auf dem Client für Sichern/Archivieren und auf dem Server gehören.

Vorgehensweise

Führen Sie die Schritte 1 bis 5 aus, um den Client zu installieren und den Knoten, die Archivierungsprozeduren im Namen eines anderen Knotens ausführen können, Proxy-Berechtigung zu erteilen.

1. Installieren Sie den Client für Sichern/Archivieren auf allen Knoten in einer gemeinsamen Datenumgebung.
2. Registrieren Sie jeden Knoten beim IBM Spectrum Protect-Server, falls er nicht existiert. Registrieren Sie den einheitlichen Zielknotennamen, damit er von allen Agentenknoten in Ihrer gemeinsamen Datenumgebung gemeinsam genutzt werden kann.
3. Registrieren Sie jeden Knoten in der gemeinsamen Datenumgebung beim IBM Spectrum Protect-Server. Dies ist der Agentenknotenname, der für Authentifizierungszwecke verwendet wird. Daten werden nicht unter Verwendung des Knotennamens gespeichert, wenn die Option `asnodename` verwendet wird.
4. Erteilen Sie mithilfe des Befehls `GRANT PROXYNODE` allen Knoten in der gemeinsam genutzten Umgebung Proxy-Berechtigung, damit sie auf den Zielknotennamen auf dem IBM Spectrum Protect-Server zugreifen können (IBM Spectrum Protect-Administrator).
5. Verwenden Sie den Verwaltungsklientbefehl `QUERY PROXYNODE`, um die Clientknoten des berechtigten Benutzers anzuzeigen, denen mit dem Befehl `GRANT PROXYNODE` die Berechtigung erteilt wurde.

Der Schritt 6 stellt sicher, dass archivierte Dateien auf dem Server verschlüsselt werden.

6. Definieren Sie die Option `encryptkey` in der Optionsdatei.

Geben Sie `encryptkey=save` in der Optionsdatei an, um den Verschlüsselungsschlüssel in der IBM Spectrum Protect-Kennwortdatei zu speichern. Sichern Sie mindestens eine Datei mit `asnode=ProxyNodeName`, um auf jedem Agentenknoten in der Mehrfachknotenumgebung einen lokalen Verschlüsselungsschlüssel zu erstellen.

Geben Sie `encryptkey=prompt` in der Optionsdatei an, wenn die Knotenbenutzer den Verschlüsselungsschlüssel verwalten sollen. Stellen Sie sicher, dass die Benutzer der Agentenknoten in der Mehrfachknotenumgebung denselben Verschlüsselungsschlüssel verwenden.

Wiederholen Sie diesen Schritt, wenn Sie den Verschlüsselungsschlüssel ändern. Verwenden Sie in der gemeinsam genutzten Umgebung denselben Verschlüsselungsschlüssel für alle Dateien, die gesichert werden.

Führen Sie die Schritte 7 bis 10 aus, um den Mehrfachknotenbetrieb von der grafischen Benutzerschnittstelle (GUI) aus zu aktivieren.

7. Prüfen Sie, ob der Clientknoten Proxy-Berechtigung für einen Zielknoten hat (oder berechtigt ist, als Zielknoten zu handeln). Verwenden Sie dazu den Verwaltungsklientbefehl `QUERY PROXYNODE`.
8. Wählen Sie **Editieren > Vorgaben** aus, um das Vorgabenfenster zu öffnen.
9. Wählen Sie die Registerkarte **Allgemein** aus und füllen Sie das Feld **Wie Knotenname** mit dem Namen des für den Proxy berechtigten Zielknotens aus.
10. Klicken Sie auf **Anwenden** und anschließend auf **OK**, um das Fenster Vorgaben zu schließen.

Führen Sie Schritt 11 auf Seite 284 aus, um zu bestätigen, dass Ihr Clientknoten jetzt als Zielknoten auf den Server zugreift.

11. Öffnen Sie das Baumstrukturfenster und bestätigen Sie, dass der Zielknotenname, der im Feld **Wie Knotenname** angegeben ist, angezeigt wird. Sie können auch überprüfen, ob der Zielknotenname im Feld **Zugriff als Knoten** im Fenster **Verbindungsinformationen** angezeigt wird.
12. Optional: Um zur Operation mit Einzelknoten zurückzukehren, löschen Sie **Wie Knotenname** im Feld **Zugriff als Knoten** auf der Registerkarte **Allgemein > Vorgaben**.

Zugehörige Verweise:

„Asnodename“ auf Seite 359

„Sitzungseinstellungen und Zeitpläne für eine Proxy-Operation“ auf Seite 360

Archivierungsdaten löschen

Sie können einzelne Archivierungsobjekte aus dem IBM Spectrum Protect-Server löschen, ohne den gesamten Dateibereich löschen zu müssen, zu dem die Objekte gehören.

Vorbereitende Schritte

Der IBM Spectrum Protect-Administrator muss Ihnen die Berechtigung zum Löschen archivierter Objekte erteilen. Um festzustellen, ob Sie über diese Berechtigung verfügen, wählen Sie **Datei > Verbindungsinformationen** in der GUI des Clients für Sichern/Archivieren oder im Hauptmenü des Web-Clients aus. Ihr Berechtigungsstatus zum Löschen von Archivierungen wird im Feld **Archivierungsdateien löschen** angezeigt. Wird in diesem Feld **Nein** angezeigt, können Sie archivierte Objekte nur löschen, wenn Ihnen Ihr Administrator die entsprechende Berechtigung erteilt.

Vorgehensweise

Führen Sie die folgenden Schritte im Web-Client oder in der GUI aus, um ein archiviertes Objekt aus dem Server zu löschen. Als Alternative zum Web-Client bzw. zur GUI können Sie archivierte Objekte auch mit dem Befehl **delete archive** über die Befehlszeile löschen.

1. Wählen Sie **Archivierungsdaten löschen** im Menü **Dienstprogramme** aus.
2. Erweitern Sie im Fenster **Archivierung löschen** die Verzeichnisbaumstruktur, indem Sie auf das Pluszeichen (+) oder auf das Ordnersymbol neben einem Objekt klicken, das eingeblendet werden soll. Objekte in der Baumstruktur sind nach der Beschreibung der Archivierungspakete zusammengefasst.
3. Wählen Sie die archivierten Objekte aus, die gelöscht werden sollen.
4. Klicken Sie auf **Löschen**. Der Client fordert Sie zur Bestätigung auf, bevor die ausgewählten Objekte gelöscht werden. Im Fenster **Task-Liste** für das Löschen von Archivierungen wird der Löschststatus angezeigt.

Zugehörige Verweise:

„Delete Archive“ auf Seite 721

Erweiterte Archivierungstasks

Zugriffsberechtigungen, symbolische Verbindungen und feste Verbindungen sind erweiterte Funktionen, die beim Archivieren von Daten zu berücksichtigen sind.

Zugriffsberechtigungen

Bei der Archivierung einer Datei sichert der Client die der Datei zugeordneten UNIX-Standardzugriffsberechtigungen.

Abhängig vom Betriebssystem werden auch erweiterte Berechtigungen gesichert. Beispielsweise sichert der Client Zugriffssteuerungslisten für Dateien auf einer AIX-Workstation.

Archiviert ein Benutzer eine Datei, für die Lesezugriff besteht, ist der Benutzer der Eigner der archivierten Kopie der Datei. Nur dieser Benutzer kann die archivierte Datei abrufen, es sei denn, einem anderen Benutzer wird der Zugriff auf diese Datei erteilt.

Symbolische Verbindungen archivieren und abrufen

Der Client für Sichern/Archivieren verfährt beim Archivieren und Abrufen symbolischer Verbindungen anders als bei regulären Dateien und Verzeichnissen.

Wie der Client symbolische Verbindungen archiviert und abruft, ist von Optionseinstellungen, von der Verfügbarkeit des Zielverzeichnisses und von der Angabe der Objekte abhängig.

Eine *symbolische Verbindung* ist unter UNIX eine Datei, die einen Zeiger auf eine andere Datei oder ein anderes Verzeichnis enthält. Das Objekt, auf das die symbolische Verbindung zeigt, wird als *Zielobjekt* bezeichnet.

Eine symbolische Verbindung kann entweder als Pfadangabe für das Zielverzeichnis oder als Verzeichnis gesichert werden. Wird die symbolische Verbindung als Verzeichnis gesichert, können auch die Dateien und Ordner im Zielverzeichnis gesichert werden.

Welche Objekte zurückgeschrieben werden, ist von der Art der Sicherung der symbolischen Verbindung, vom Umfang der Zurückschreibung, von der Einstellung der Option `followsymbolic` und von der Verfügbarkeit des Zielverzeichnisses zum Zeitpunkt der Zurückschreibung abhängig.

Weitere Informationen über die Verarbeitung symbolischer Verbindungen bei der Archivierung enthält die Beschreibung der Option `archsymb linkasfile`.

Anmerkung: Die hier beschriebene Verarbeitung symbolischer Verbindungen gilt nicht für Mac OS X. Symbolische Verbindungen werden immer als Dateien archiviert und den Zeigern wird nicht gefolgt.

Die folgende Tabelle zeigt Archivierungs- und Abruffunktionen für symbolische Verbindungen und die jeweiligen Aktionen:

Tabelle 49. Verwaltung symbolischer Verbindungen für Archivieren und Abrufen

Funktion	Aktion
Archivierung einer Dateiverbindung.	Archiviert die Datei, auf die die symbolische Verbindung zeigt.
Archivierung einer Verzeichnisverbindung.	Archiviert das Verzeichnis und seinen Inhalt.
Archivierung einer Datei mit <code>subdir=yes</code> .	Archiviert die Datei, den Verzeichnispfad und alle Dateien gleichen Namens in der Unterverzeichnisstruktur.
Archivierung eines Verzeichnisses mit <code>subdir=yes</code> .	Archiviert das Verzeichnis, seinen Inhalt und den Inhalt der Unterverzeichnisse.
Archivierung einer symbolischen Verbindung, die auf eine Datei oder ein Verzeichnis zeigt, die bzw. das nicht vorhanden ist.	Archiviert die symbolische Verbindung.

Tabelle 49. Verwaltung symbolischer Verbindungen für Archivieren und Abrufen (Forts.)

Funktion	Aktion
Abrufen einer symbolischen Verbindung, die auf eine Datei zeigt; Datei und Verbindung sind vorhanden.	Die Datei wird ersetzt, wenn replace=y definiert wird.
Abrufen einer symbolischen Verbindung, die auf eine Datei zeigt; die symbolische Verbindung ist nicht mehr vorhanden.	Ruft die Datei in das Verzeichnis ab, in dem sich die symbolische Verbindung befindet, wobei der Dateiname durch den Namen der symbolischen Verbindung ersetzt wird.
Abrufen einer symbolischen Verbindung, die auf ein Verzeichnis zeigt; die symbolische Verbindung und das Verzeichnis sind nicht mehr vorhanden.	In dem Verzeichnis, in dem sich die symbolische Verbindung befindet, wird ein Verzeichnis erstellt, und alle Dateien und Unterverzeichnisse werden in dieses Verzeichnis zurückgeschrieben. Der Name der symbolischen Verbindung wird als Name des neuen Verzeichnisses verwendet.
Abrufen einer symbolischen Verbindung, die auf ein Verzeichnis zeigt; die symbolische Verbindung und das Verzeichnis sind vorhanden.	Das Verzeichnis wird nicht abgerufen, solange die symbolische Verbindung vorhanden ist.

Zugehörige Verweise:

„Archsymlinkasfile“ auf Seite 358

Feste Verbindungen

Wenn Sie Dateien archivieren, die fest verbunden sind, archiviert der Client für Sichern/Archivieren jede Instanz der verbundenen Datei.

Wenn Sie beispielsweise zwei Dateien, die fest verbunden sind, archivieren, archiviert der Client die Dateidaten zweimal.

Wenn Sie fest verbundene Dateien abrufen, stellt der Client die Verbindungen wieder her. Hatten Sie beispielsweise ein Dateipaar mit fester Verbindung und ist nur eine der fest verbundenen Dateien auf Ihrer Workstation, werden beide Dateien beim Abrufen fest verbunden. Bei diesem Verfahren gibt es eine einzige Ausnahme, und zwar, wenn Sie zwei fest verbundene Dateien archivieren und dann die Verbindung zwischen diesen Dateien auf Ihrer Workstation unterbrechen. Wenn Sie die beiden Dateien vom Server abrufen, respektiert der Client das aktuelle Dateisystem und ruft die feste Verbindung nicht ab.

Tipp: Werden nicht alle fest verbundenen Dateien gleichzeitig archiviert oder abgerufen, können Probleme auftreten. Um sicherzustellen, dass fest verbundene Dateien synchronisiert bleiben, führen Sie die Archivierung und den Abruf fest verbundener Dateien immer gleichzeitig durch.

Archivierungen abrufen

Eine Datei wird abgerufen, wenn eine Archivierungskopie aus dem Server auf Ihre Workstation zurückgestellt werden soll.

Viele der weiterführenden Überlegungen zum Abrufen von Dateien sind mit den Überlegungen zum Zurückschreiben von Dateien identisch.

Wichtig: Wenn Sie eine Datei ohne Spezifikationen abrufen und mehrere Versionen der Archivierungskopie auf dem Server vorhanden sind, ruft der Client alle Kopien

ab. Nachdem die erste Kopie abgerufen ist, wird die zweite Kopie abgerufen. Wenn es auf Ihrer Client-Workstation eine bestehende Kopie gibt, werden Sie zum Ersetzen, Überspringen oder Abbrechen aufgefordert.

Zugehörige Konzepte:

„Dateien auf eine andere Workstation zurückschreiben oder abrufen“ auf Seite 276

Zugehörige Tasks:

„Einen anderen Benutzer zum Zurückschreiben und Abrufen Ihrer Dateien berechtigen“ auf Seite 274

„Dateien von einem anderen Clientknoten zurückschreiben oder abrufen“ auf Seite 275

Daten über die grafische Benutzerschnittstelle abrufen

Sie können eine archivierte Datei über die grafische Benutzerschnittstelle (GUI) abrufen.

Vorgehensweise

1. Klicken Sie auf **Abrufen** im Hauptfenster der Client-Java-GUI. Das Fenster **Abrufen** wird angezeigt.
2. Erweitern Sie die Verzeichnisbaumstruktur, indem Sie auf das Pluszeichen (+) oder auf das Ordnersymbol neben dem Objekt, das eingeblendet werden soll, klicken. Zum Suchen oder Filtern von Dateien klicken Sie auf das Symbol **Suchen** in der Funktionsleiste.
3. Geben Sie die Suchkriterien in das Fenster **Dateien suchen** ein.
4. Klicken Sie auf **Suchen**. Das Fenster **Übereinstimmende Dateien** wird angezeigt.
5. Klicken Sie auf die Auswahlfelder neben den Dateien, die abgerufen werden sollen, und schließen Sie das Fenster **Übereinstimmende Dateien**.
6. Geben Sie die Filterkriterien in das Fenster **Dateien suchen** ein.
7. Klicken Sie auf **Filter**. Im Fenster **Abrufen** werden die gefilterten Dateien angezeigt.
8. Klicken Sie auf die Auswahlfelder der gefilterten Dateien oder Verzeichnissen, die abgerufen werden sollen.
9. Um bestimmte Abrufoptionen zu ändern, klicken Sie auf **Optionen**. Die geänderten Optionen sind nur während der aktuellen Sitzung wirksam.
10. Klicken Sie auf **Abrufen**. Das Fenster **Abrufziel** wird angezeigt. Geben Sie die entsprechenden Informationen in das Fenster **Abrufziel** ein.
11. Klicken Sie auf **Abrufen**. Im Fenster **Task-Liste** wird der Verarbeitungstatus des Abrufs angezeigt.

Beispiele für das Abrufen von Daten über die Befehlszeile

Sie können eine einzelne Datei, eine Dateigruppe oder alle Dateien in einem Verzeichnis oder Unterverzeichnis abrufen.

Wenn Sie eine Datei abrufen, sendet der IBM Spectrum Protect-Server eine Kopie dieser Datei. Die archivierte Datei verbleibt im Speicher.

Verwenden Sie den Befehl **retrieve**, um Dateien aus dem Speicher abzurufen und auf Ihrer Workstation zu speichern. Die folgende Tabelle enthält Beispiele zur Verwendung des Befehls **retrieve**.

Tabelle 50. Beispiele für Befehle zum Abrufen archivierter Dateien

Task	Befehl	Hinweise
Die Datei /home/jones/h1.doc in ihr Ursprungsverzeichnis abrufen.	<code>dsmc retrieve /home/jones/h1.doc</code>	Wird kein Ziel angegeben, werden die Dateien an ihre ursprüngliche Position abgerufen.
Die Datei /home/jones/h1.doc mit einem neuen Namen und in ein anderes Verzeichnis abrufen.	<code>dsmc retrieve /home/jones/h1.doc /home/smith/h2.doc</code>	Keine.
Alle Dateien im Verzeichnis /home/jones, die mit den Zeichen .bak enden, in das Verzeichnis /home/smith abrufen.	<code>dsmc retrieve "/home/jones/*.bak" /home/smith/</code>	Keine.
Die Datei /home/jones/ch1.doc abrufen und eine Beschreibung zuordnen.	<code>dsmc retrieve /home/jones/ch1.doc -description="Kapitel 1, erste Version"</code>	Wenn Sie keine Beschreibung im Befehl retrieve angeben, lautet der Standardwert Abrufdatum:x; hierbei gibt x das aktuelle Systemdatum an.
Die Option <code>pick</code> verwenden, um eine Liste von Archivierungskopien anzuzeigen, aus denen Sie Dateien zum Abrufen auswählen können.	<code>dsmc retrieve "/home/jones/*" -pick</code>	Keine.
Eine Liste von Dateien, die in der Datei <code>retrievelist.txt</code> angegeben ist, in ihr Ursprungsverzeichnis abrufen.	<code>dsmc retrieve -filelist=/home/dir2/retrievelist.txt</code>	Keine.

Zugehörige Verweise:

„Retrieve“ auf Seite 805

„Description“ auf Seite 397

„Filelist“ auf Seite 453

„Pick“ auf Seite 528

Verwaltungsklassen für die Archivierung

Der Client für Sichern/Archivieren überprüft die Optionen `include` in Ihrer Liste der Einschluss-/Ausschlussoptionen um zu bestimmen, welche Verwaltungsklasse Ihren archivierten Dateien zugeordnet werden soll.

Wenn Sie einer Datei nicht mit der Option `include` eine Verwaltungsklasse zuordnen, ordnet der Client der Datei die Standardverwaltungsklasse zu. Der Client kann eine Datei nur dann archivieren, wenn die ausgewählte Verwaltungsklasse eine Archivierungskopiengruppe enthält.

Sie können die Standardverwaltungsklasse mithilfe der Option **archmc** überschreiben oder indem Sie in der grafischen Benutzerschnittstelle auf **Optionen** im Fenster **Archivieren** und dann auf **Einschluss-/Ausschlussliste überschreiben** klicken und die Verwaltungsklasse auswählen.

Sie können Einschluss-/Ausschlussanweisungen auch in der Verzeichnisstruktur der Java-GUI des Clients für Sichern/Archivieren oder des Web-Clients hinzufügen. Anschließend können Sie mithilfe der Funktion **Dienstprogramme - Voranzeige für Einschluss/Ausschluss** die Voranzeige der Einschluss-/Ausschlussliste aufrufen, bevor Sie Daten an den Server senden.

Zugehörige Konzepte:

„Dateien eine Verwaltungsklasse zuordnen“ auf Seite 316

„Informationen zu Verwaltungsklassen und Kopiengruppen anzeigen“ auf Seite 311

Zugehörige Verweise:

„**Preview Archive**“ auf Seite 742

„**Preview Backup**“ auf Seite 744

Kapitel 7. Übersicht über den IBM Spectrum Protect-Scheduler

Der zentrale IBM Spectrum Protect-Scheduler ermöglicht, dass Clientoperationen zu angegebenen Zeiten automatisch stattfinden.

Zum besseren Verständnis der Zeitplanung mit IBM Spectrum Protect müssen mehrere Begriffe definiert werden:

Zeitplandefinition

Eine Zeitplandefinition auf dem IBM Spectrum Protect-Server gibt kritische Merkmale einer automatisierten Aktivität an. Hierzu gehören die Art und der Zeitpunkt der Aktion sowie die Häufigkeit, mit der die Aktion stattfinden soll. Für einen Zeitplan können zahlreiche weitere Eigenschaften definiert werden. Informationen zum Befehl **DEFINE SCHEDULE** finden Sie in der Dokumentation zum IBM Spectrum Protect-Server.

Zeitplanzuordnung

Eine Zeitplanzuordnung ist eine Zuordnung zu einer bestimmten Zeitplandefinition für einen Clientknoten. Mehrfachzeitplanzuordnungen ermöglichen, dass einzelne Zeitplandefinitionen von vielen Clientknoten verwendet werden können. Da Zeitplandefinitionen in bestimmten Maßnahmendomänen eingeschlossen sind, können nur Knoten, die für eine bestimmte Maßnahmendomäne definiert sind, Zeitplänen zugeordnet werden, die in dieser Domäne definiert sind.

Geplantes Ereignis

Ein geplantes Ereignis ist ein bestimmtes Vorkommen, wann ein Zeitplan für einen Knoten ausgeführt wird. Die folgenden Bedingungen müssen erfüllt sein, damit automatisch geplante Ereignisse für einen Client stattfinden:

- Eine Zeitplandefinition muss für eine bestimmte Maßnahmendomäne vorhanden sein.
- Eine Zeitplanzuordnung muss für den erforderlichen Knoten, der zu dieser Maßnahmendomäne gehört, vorhanden sein.
- Der Client-Schedulerprozess muss auf dem Clientsystem aktiv sein.

Beim Erstellen einer Zeitplandefinition auf dem IBM Spectrum Protect-Server können Sie die folgenden Zeitplanaktionen verwenden: incremental, selective, archive, restore, retrieve, Imagesicherung (gilt nicht für Mac OS X), Imagezurückschreibung (gilt nicht für Mac OS X), command und macro. Die am häufigsten verwendete Aktion ist 'incremental', wobei der Parameter **objects** nicht definiert wird. Bei dieser Einstellung führt der Client für Sichern/Archivieren eine Domänenteilsicherung aller Dateisysteme aus, die durch die Clientdomänenoption definiert sind. Eine Zeitplandefinition mit der Aktion **command** bewirkt, dass ein Betriebssystembefehl oder ein Shell-Script ausgeführt werden kann. Wenn Sie Tasks für IBM Spectrum Protect for Data Protection-Clients automatisieren, müssen Sie Zeitplandefinitionen mit der Aktion **command** verwenden, die die Befehlszeilendienstprogramme für diese Anwendungen aufrufen.

Der Zeitplan *Startfenster* zeigt den verfügbaren Zeitraum für den Start eines geplanten Ereignisses an. Das Startfenster wird durch die folgenden Zeitplandefinitionsparameter definiert: **startdate**, **starttime**, **durunits** und **duration**. Die Optionen **startdate** und **starttime** definieren den Beginn des Startfensters für das

allererste geplante Ereignis. Der Beginn des Startfensters für nachfolgende geplante Ereignisse variiert je nach den Zeitplandefinitionswerten für **period** und **perunit**. Die Parameter **duration** und **durunits** definieren die Länge des Startfensters. Die Zeitplanaktion muss innerhalb des Startfensters starten. Dies illustrieren die Ergebnisse der folgenden Zeitplandefinition:

```
define schedule standard test1 action=incremental starttime=12:00:00 period=1
perunits=hour dur=30 duru=minutes
```

Ereignis	Fensterstart	Fensterende	Tatsächlicher Start (nur als Beispiel, die Zeiten variieren)
1	12:00:00	12:30:00	12:05:33
2	13:00:00	13:30:00	13:15:02
3	14:00:00	14:30:00	14:02:00
usw.			

Die Variation der tatsächlichen Startzeiten ist ein Ergebnis der vom zentralen IBM Spectrum Protect-Scheduler zur Verfügung gestellten Zufallsgenerierungsfunktion, die hilft, die Last der geplanten Sitzungen auf dem IBM Spectrum Protect-Server zu verteilen.

Beispiele: Leerzeichen in Dateinamen in Zeitplandefinitionen

Wenn Sie den Zeitplanparameter **objects** oder den Zeitplanparameter **options** mit Dateispezifikationen definieren oder aktualisieren, die Leerzeichen enthalten, müssen Sie alle Dateispezifikationen mit Leerzeichen in Anführungszeichen (") und dann die gesamte Spezifikation in Hochkommas (') einschließen.

Die folgenden Beispiele zeigen, wie Zeitplanparameter **object** begrenzt werden, wenn Dateispezifikationen Leerzeichen enthalten:

```
objects="/home/proj1/Some file.doc"
objects="/home/proj1/Some file.doc" "/home/Another file.txt" /home/noblanks.txt'
objects="/home/My Directory With Blank Spaces/"
objects="/Users/user1/Documents/Some file.doc"
objects="/Users/user1/Documents/Some file.doc"
"/Users/user5/Documents/Another file.txt" /Users/user3/Documents/noblanks.txt'
objects="/Users/user1/My Directory With Blank Spaces/'"
```

Diese Syntax stellt sicher, dass eine Dateispezifikation mit Leerzeichen (z. B. /home/proj1/Some file.doc) als Name einer einzigen Datei und nicht als Namen von zwei separaten Dateien (/home/proj1/Some und file.doc) behandelt wird.

Die folgenden Beispiele zeigen, wie Zeitplanparameter **options** begrenzt werden, wenn Dateispezifikationen Leerzeichen enthalten:

```
options='-preschedulecmd="/home/me/my files/bin/myscript"
-postschedulecmd="/home/me/my files/bin/mypostscript" -quiet'
options='-presched="/home/me/my files/bin/precmd" -postsched=finish'
```

Weitere Informationen finden Sie auch in der Beschreibung der Parameter **objects** und **options** unter den Befehlen **DEFINE SCHEDULE** und **UPDATE SCHEDULE**. Die Beschreibungen dieser Befehle und Parameter finden Sie in der Dokumentation zum IBM Spectrum Protect-Server.

Zugehörige Konzepte:

„Eingabezeichenfolgen angeben, die Leerzeichen oder Hochkommas oder Anführungszeichen enthalten“ auf Seite 156

Bevorzugte Startzeiten für bestimmte Knoten

Gelegentlich wollen Sie vielleicht sicherstellen, dass ein bestimmter Knoten seine geplante Aktivität so nah wie möglich an der definierten Startzeit des Zeitplans beginnt. Diese Notwendigkeit ergibt sich normalerweise, wenn Zeitplanung im Modus mit Bedienerführung verwendet wird.

Abhängig von der Anzahl Clientknoten, die dem Zeitplan zugeordnet sind, und von der Position des Knotens in der Bedienerführungsreihenfolge, kann es dazu kommen, dass der Knoten erheblich später angefordert wird als die Startzeit für den Zeitplan beträgt.

In diesem Fall können Sie die folgenden Schritte ausführen:

1. Kopieren Sie den Zeitplan mit einem anderen Namen in einen neuen Zeitplan (oder definieren Sie einen neuen Zeitplan mit den bevorzugten Attributen).
2. Definieren Sie das Prioritätsattribut des neuen Zeitplans so, dass er eine höhere Priorität als der ursprüngliche Zeitplan hat.
3. Löschen Sie die Zuordnung des Knotens zum ursprünglichen Zeitplan und ordnen Sie anschließend den Knoten dem neuen Zeitplan zu.

Nun verarbeitet der IBM Spectrum Protect-Server den neuen Zeitplan zuerst.

Schedulerverarbeitungsoptionen

Schedulerverarbeitungsoptionen legen fest, welche Operationen beim Starten eines Scheduler-Jobs ausgeführt werden.

Sie können die meisten dieser Schedulerverarbeitungsoptionen in der Clientoptionsdatei definieren. Einige dieser Optionen können jedoch auf dem IBM Spectrum Protect-Server für alle Clients definiert werden.

Die folgende Tabelle zeigt, welche Optionen jeweils vom Client und vom Server definiert und welche Option vom Server überschrieben werden. Ein X in einer Spalte zeigt an, wo die Option angegeben werden kann.

Option	Clientdefiniert	Serverdefiniert	Globale Überschreibung durch Server
managedservices	X		
maxcmdretries	X		Befehl SET MAXCMDRETRIES
maxschedsessions		X	
postschedulecmd, postnschedulecmd	X		
preschedulecmd, prenschedulecmd	X		
querschedperiod	X		Befehl SET QUERSCHEDPERIOD
randomize		X	
retryperiod	X		Befehl SET RETRYPERIOD
schedcmddisabled	X		
schedlogname	X		
schedlogretention	X		

Option	Clientdefiniert	Serverdefiniert	Globale Überschreibung durch Server
schedmode	X		Befehl SET SCHEDMODES
sessioninitiation	X	X	Befehl UPDATE NODE
tcpclientaddress	X	X (auch auf dem Server definiert, wenn sessioninit=serveronly als Teil der Knotendefinition definiert ist)	
tcpclientport	X	X (auch auf dem Server definiert, wenn sessioninit=serveronly als Teil der Knotendefinition definiert ist)	

Clientdefinierte Optionen sind je nach Option und Plattform in der Datei `dsm.sys` oder `dsm.opt` definiert. Der IBM Spectrum Protect-Server kann auch einige Optionen in einer Clientoptionsgruppe oder als Teil der Optionsparameter der Zeitplandefinition definieren. Der IBM Spectrum Protect-Server kann auch einige Optionen global für alle Clients definieren. Standardmäßig wird die Clienteinstellung für diese Optionen berücksichtigt. Wenn auf dem IBM Spectrum Protect-Server die globale Überschreibung gesetzt ist, wird die Clienteinstellung für die Option ignoriert. Das Definieren von Clientoptionen als Teil der Zeitplandefinition ist nützlich, wenn Sie spezifische Optionen für eine geplante Aktion verwenden wollen, die sich von den normalerweise vom Clientknoten verwendeten Optionseinstellungen unterscheiden oder für jeden Zeitplan, den der Knoten ausführt, verschieden sind.

Die Option `schedmode` steuert die Kommunikationsinteraktion zwischen dem IBM Spectrum Protect-Client und -Server. Es gibt zwei Varianten im Planungsmodus: *client polling* (Clientsendeaufruf) und *server prompted* (Serversystemanfrage). Diese Varianten werden in der Dokumentation zum IBM Spectrum Protect-Server erläutert.

Rückkehrcodes für Zeitpläne in Zeitplanscripts auswerten

Sie können Umgebungsvariablen verwenden, um den aktuellen IBM Spectrum Protect-Rückkehrcode zu bestimmen, bevor Sie ein Script mithilfe der Clientoption `preschedulecmd` oder `postschedulecmd` ausführen.

IBM Spectrum Protect stellt den aktuellen Wert des Rückkehrcodes in der Umgebungsvariablen mit dem Namen `TSM_PRE_CMD_RC` bereit. Die Variable `TSM_PRE_CMD_RC` ist der aktuelle Wert des IBM Spectrum Protect-Rückkehrcodes, bevor Sie ein Zeitplanscript ausführen. Der Wert der Variablen `TSM_PRE_CMD_RC` ist nicht notwendigerweise mit dem Rückkehrcode identisch, den IBM Spectrum Protect nach der Ausführung des Zeitplanscripts ausgibt. Mit der Variablen `TSM_PRE_CMD_RC` kann in Zeitplanscripts der aktuelle Status des Zeitplans bestimmt werden.

Die Variable `TSM_PRE_CMD_RC` wird mit jeder der folgenden Planungsoptionen definiert: `preschedule`, `prenschedule`, `postschedule` und `postnschedule`. `TSM_PRE_CMD_RC` hat Einfluss auf die Zeitpläne, in denen die Option `ACTION=COMMAND` angegeben ist.

Ein Verwendungsbeispiel für die Variable `TSM_PRE_CMD_RC`:

```

if [[ -n ${TSM_PRE_CMD_RC} ]] ; then

    if [[ ${TSM_PRE_CMD_RC} == 0 ]] ; then
        echo "The TSM_PRE_CMD_RC is 0"

    elif [[ ${TSM_PRE_CMD_RC} == 4 ]] ; then
        echo "The TSM_PRE_CMD_RC is 4"

    elif [[ ${TSM_PRE_CMD_RC} == 8 ]] ; then
        echo "The TSM_PRE_CMD_RC is 8"

    elif [[ ${TSM_PRE_CMD_RC} == 12 ]] ; then
        echo "The TSM_PRE_CMD_RC is 12"
    else
        echo "The TSM_PRE_CMD_RC is an unexpected value: ${TSM_PRE_CMD_RC}"
    fi

else
    echo "The TSM_PRE_CMD_RC is not set"
fi

```

Rückkehrcodes von preschedulecmd- und postschedulecmd-Scripts

In diesem Abschnitt werden die Rückkehrcodes beschrieben, die möglicherweise angezeigt werden, wenn Sie die Optionen preschedulecmd und postschedulecmd verwenden.

- Wenn der durch die Option preschedulecmd angegebene Befehl mit einem Rückkehrcode ungleich null endet, nimmt IBM Spectrum Protect an, dass der Befehl fehlgeschlagen ist. In diesem Fall kann weder das geplante Ereignis noch ein postschedulecmd- oder postnschedulecmd-Befehl ausgeführt werden. Der Verwaltungsbefehl **query event** mit der Option format=detailed zeigt an, dass das Ereignis mit dem Rückkehrcode 12 fehlgeschlagen ist.
- Wenn der durch die Option postschedulecmd angegebene Befehl mit einem Rückkehrcode ungleich null endet, betrachtet IBM Spectrum Protect den Befehl als fehlgeschlagen. Der Verwaltungsbefehl **query event** mit der Option format=detailed zeigt an, dass das Ereignis mit dem Rückkehrcode 8 beendet wurde; es sei denn, die geplante Operation wurde mit einem höheren Rückkehrcode beendet. In diesem Fall hat der höhere Rückkehrcode Vorrang. Wenn die geplante Operation mit dem Rückkehrcode 0 oder 4 endet und der Befehl postschedulecmd fehlschlägt, zeigt der Verwaltungsbefehl **query event** daher an, dass das Ereignis mit dem Rückkehrcode 8 beendet wurde. Wenn die geplante Operation mit dem Rückkehrcode 12 endet, hat dieser Rückkehrcode Vorrang und **query event** zeigt an, dass das Ereignis mit dem Rückkehrcode 12 fehlgeschlagen ist.

Beim Interpretieren des Rückkehrcodes von einem Befehl betrachtet IBM Spectrum Protect 0 als Erfolg und alles Andere als Fehler. Obwohl dieses Verhalten in der Branche überall akzeptiert wird, kann es nicht zu 100% garantiert werden. Beispiel: Der Befehl widget wurde vielleicht so entwickelt, dass er den Rückkehrcode 3 ausgibt, wenn er erfolgreich ausgeführt wurde. Deshalb ist es möglich, dass der Befehl preschedulecmd oder postschedulecmd unter Umständen mit einem Rückkehrcode ungleich null endet und dennoch erfolgreich ist. Um zu verhindern, dass IBM Spectrum Protect solche Befehle als fehlgeschlagen behandelt, können Sie diese Befehle in ein Script einbetten und das Script so codieren, dass es die Befehlsrückkehrcodes korrekt interpretiert. Das Script wird mit Rückkehrcode 0 beendet, wenn

der Befehl erfolgreich war; andernfalls wird es mit einem Rückkehrcode ungleich null beendet. Die Logik für ein Script, das widget ausführt, sieht möglicherweise wie in diesem Beispiel aus:

```
run 'widget'
  if lastcc == 3
    exit 0
  else
    exit 1
```

Zugehörige Verweise:

„Postschedulecmd/Postnschedulecmd“ auf Seite 531

„Preschedulecmd/Prenschedulecmd“ auf Seite 534

Clientakzeptor-Scheduler-Services gegenüber traditionellen Scheduler-Services

Sie können den IBM Spectrum Protect-Client so konfigurieren, dass der Schedulerprozess mit dem IBM Spectrum Protect-Clientakzeptordämon verwaltet wird.

Der Clientakzeptordämon stellt einen einfachen Zeitgeber zur Verfügung, der den Schedulerprozess nach Bedarf automatisch startet und stoppt. Alternativ dazu hält die traditionelle Methode den IBM Spectrum Protect-Schedulerprozess fortlaufend aktiv. Im allgemeinen ist die Verwendung des Clientakzeptordämons zum Verwalten des Schedulers die bevorzugte Methode.

Der folgende Abschnitt enthält einen Vergleich zwischen den vom Clientakzeptordämon (CAD) verwalteten Services und den Methoden der traditionellen Scheduler-Services.

Vom Clientakzeptordämon verwaltete Services

- Werden mithilfe der Option `managedservices schedule` definiert und mit den Clientakzeptordämonservices (`dsmcad`) gestartet.
- Der Clientakzeptordämon startet und stoppt den Schedulerprozess für jede geplante Aktion nach Bedarf.
- Erfordern weniger Systemressourcen bei Inaktivität.
- Die IBM Spectrum Protect-Clientoptionen und die Überschreibungsoptionen auf dem IBM Spectrum Protect-Server werden jedes Mal aktualisiert, wenn die Clientakzeptordämonservices eine geplante Sicherung starten.
- Können nicht bei Sicherungen mit `SESSIONINITiation=SERVEROnly` verwendet werden.

Traditionelle IBM Spectrum Protect-Scheduler-Services

- Werden mit dem Befehl `dsmc sched` gestartet.
- Bleiben aktiv, selbst wenn die geplante Sicherung beendet ist.
- Erfordern einen höheren Verbrauch an Systemressourcen bei Inaktivität.
- Die IBM Spectrum Protect-Clientoptionen und die Überschreibungsoptionen auf dem IBM Spectrum Protect-Server werden nur einmal verarbeitet, wenn `dsmc sched` gestartet wird. Wenn Sie eine Option aus einer Clientoptionsgruppe löschen, müssen Sie den Scheduler erneut starten, damit der Scheduler die Löschung registriert.

Tipp: Starten Sie den traditionellen Scheduler regelmäßig, um Systemressourcen freizugeben, die zuvor von Systemaufrufen verwendet wurden.

Client-Scheduler-Prozess für die Ausführung als Hintergrundtask und den automatischen Start beim Systemstart definieren

Sie können den IBM Spectrum Protect-Client-Scheduler so konfigurieren, dass er als Systemtask im Hintergrund ausgeführt und automatisch gestartet wird, wenn Ihr System gestartet wird.

Informationen zu diesem Vorgang

Sie können diese Task unabhängig davon ausführen, ob Sie den Scheduler mit dem Clientakzeptor verwalten oder ob Sie zum Starten des Client-Schedulers die traditionelle Methode verwenden.

Wenn Sie einen vom Clientakzeptor verwalteten Zeitplan ausführen, definieren Sie den Clientakzeptorprozess (nicht den Schedulerprozess) für den automatischen Start zur Startzeit. Wenn Sie die traditionelle Methode verwenden, definieren Sie den Schedulerprozess für den automatischen Start zur Startzeit.

Sie können den Clientakzeptor so konfigurieren, dass er als Systemtask im Hintergrund ausgeführt wird und automatisch gestartet wird, wenn Ihr System gestartet wird. Um den Clientakzeptor für die Verwaltung geplanter Sicherungen zu konfigurieren, geben Sie mit der Option `managedservices` an, ob der Clientakzeptor nur den Scheduler, nur den Web-Client oder sowohl den Scheduler als auch den Web-Client verwaltet. Die Methode zum Definieren des Clientakzeptors als Systemtask ist je nach Plattform unterschiedlich.

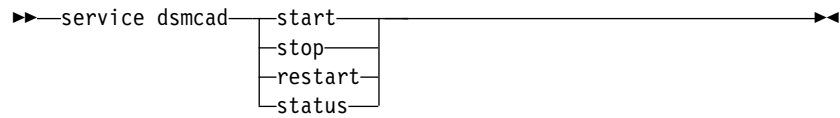
Damit der Scheduler automatisch gestartet werden kann, müssen Sie dem Client die Speicherung seines Kennworts ermöglichen, indem Sie die Option `passwordaccess` auf **generate** setzen und das Kennwort speichern, indem Sie einen einfachen Clientbefehl wie `dsmc query session` ausführen. Zu Testzwecken können Sie den Scheduler immer im Vordergrund starten, indem Sie `dsmc sched` über eine Eingabeaufforderung ausführen (ohne eine Zeilengruppe `managedservices` zu definieren).

Um den Scheduler zur Startzeit automatisch zu starten, verwenden Sie entweder die Methode zur Verwaltung durch den Clientakzeptor oder die traditionelle Methode.

Methode zur Verwaltung durch den Clientakzeptor

1. Setzen Sie in Ihrer Datei `dsm.sys` die Option `managedservices` auf **schedule** oder **schedule webclient**.
2. Starten Sie den Clientakzeptor.
 - a. Fügen Sie auf AIX- und Solaris-Clients den folgenden Eintrag zur Systemstartdatei (bei den meisten Plattformen `/etc/inittab`) hinzu:

```
tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # TSM Client  
Acceptor Daemon
```
 - b. Auf Linux-Clients erstellt das Installationsprogramm ein Startscript für den Clientakzeptor (`dsmcad`) an der Position `/etc/init.d`. Der Clientakzeptor (`dsmcad`) muss gestartet werden, damit er Scheduler-Tasks oder den Web-Client verwalten kann. Führen Sie die folgenden Befehle als Rootbenutzer aus, um den Clientakzeptor zu starten, zu stoppen, erneut zu starten oder seinen Status zu überprüfen:



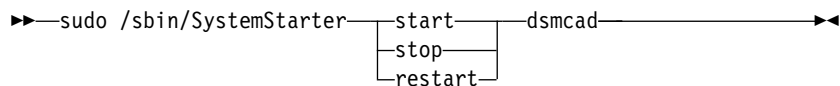
Damit der Clientakzeptor nach einem Systemwiederanlauf automatisch gestartet werden kann, fügen Sie den Service wie folgt über eine Shelleingabeaufforderung hinzu:

```
# chkconfig --add dsmcad
```

Wenn das Betriebssystem Linux den Initialisierungsservice `systemd` ausführt, führen Sie die folgenden Schritte aus, um `dsmcad` zu starten und zur Systemstartzeit auszuführen:

- 1) Kopieren Sie die bereitgestellte `systemd`-Einheitendatei `/opt/tivoli/tsm/client/ba/bin/dsmcad.service` in das Verzeichnis `/etc/systemd/system/`.
- 2) Führen Sie den folgenden Befehl aus, um die `systemd`-Einheitenliste zu aktualisieren:
`systemctl daemon-reload`
- 3) Führen Sie den folgenden Befehl aus, um den Clientakzeptor zur Systemstartzeit zu starten:
`systemctl enable dsmcad.service`
- 4) Führen Sie den folgenden Befehl aus, um den Clientakzeptor zu starten:
`systemctl start dsmcad.service`

- c. Unter Mac OS X muss der Clientakzeptordämon als Starteintrag installiert sein. Ein Systemadministrator muss die IBM Spectrum Protect-Tools für Administratoren verwenden, um den Clientakzeptor zu installieren und zu starten. Um den Clientakzeptor zu starten, zu stoppen oder erneut zu starten, verwenden Sie den folgenden Befehl:



3. Setzen Sie in der Datei `dsm.sys` die Option `passwordaccess` auf **generale**.
4. Führen Sie einen Befehl wie `dsmc query sess` aus, um das Kennwort für den Knoten zu speichern.

Traditionelle Methode:

1. Legen Sie die Option `managedservices` fest.
 - Auf AIX-, Linux- und Solaris-Clients müssen Sie die Option entweder vollständig entfernen (standardmäßig wird **webclient** angenommen) oder auf **webclient** setzen.
 - Setzen Sie auf Mac OS X-Clients die Option `managedservices` entweder auf **webclient** oder auf **none**. Setzen Sie die Option nicht auf die Einstellung **schedule**.
2. Fügen Sie unter AIX, Linux und Solaris den folgenden Eintrag zur Systemstartdatei (z. B. `/etc/inittab`) hinzu, sofern dies unterstützt wird:
`tsmsched::once:/usr/bin/dsmc sched > /dev/null 2>&1 # TSM scheduler`

3. Setzen Sie in der Datei `dsm.sys` die Option `passwordaccess` auf **genera-**
te.
4. Führen Sie einen Befehl wie `dsmc query sess aus`, um das Kennwort
für den Knoten zu speichern.
5. Um den Client-Scheduler auf Ihrem Clientknoten zu starten und eine
Verbindung zum Serverzeitplan herzustellen, müssen Sie den folgenden
Befehl eingeben:

```
dsmc schedule
```

Falls sich das aktuelle Verzeichnis nicht in Ihrer Umgebungsvariablen
`PATH` befindet, geben Sie den folgenden Befehl ein:

```
./dsmc schedule
```

Wenn Sie den Client-Scheduler starten, ist dieser kontinuierlich aktiv,
bis Sie das Fenster schließen, den Prozess beenden oder sich vom Sys-
tem abmelden.

Geben Sie folgenden Befehl ein, damit der Befehl **schedule** im Hinter-
grund ausgeführt wird und der Client-Scheduler auch nach einer Ab-
meldung vom System aktiv bleibt:

```
nohup dsmc schedule 2> /dev/null &
```

Zugehörige Verweise:

„Cadlistenonport“ auf Seite 372

Beispiele: Informationen zu geplanter Arbeit anzeigen

Zeitpläne können klassisch oder erweitert sein, je nachdem, wie das Intervall bis
zur nächsten Ausführung definiert wird.

Bei klassischen Zeitplänen kann der Zeitraum so klein wie eine Stunde sein. Bei er-
weiterten Plänen können Aktionen an bestimmten Tagen ausgeführt werden.

Um die für Ihren Clientknoten definierten Zeitpläne anzuzeigen, geben Sie Folgen-
des ein:

```
dsmc query schedule
```

Der Client für Sichern/Archivieren zeigt detaillierte Informationen zur gesamten
für Ihren Clientknoten geplanten Arbeit an. In Tabelle 51 auf Seite 300 wird die Bei-
spielausgabe des Befehls **query schedule** für klassische Zeitpläne angezeigt.

Tabelle 51. Beispielausgabe des Befehls 'query schedule' für klassische Zeitpläne

Zeitplanname: DAILY_INC
Beschreibung: Tägliche Systemsicherung
Zeitplanstil: Klassisch
Aktion: Teilsicherung
Optionen: QUIET
Objekte:
Priorität: 1
Nächste Ausführung: 30 Minuten
Dauer: 4 Stunden
Periode: 1 Tag
Wochentag: Jeden Tag
Monat:
Tag im Monat:
Woche im Monat:
Verfällt: Nie
 Zeitplan: WEEKLY_INC
Beschreibung: Wöchentliche Sicherung für Projektdateien
Zeitplanstil: Klassisch
Aktion: Teilsicherung
Optionen: QUIET
Objekte: /proj
Priorität: 1
Nächste Ausführung: 60 Minuten
Dauer: 8 Stunden
Periode: 7 Tage
Wochentag: Freitag
Monat:
Tag im Monat:
Woche im Monat:
Verfällt: Nie

Der Zeitplan mit dem Namen **WEEKLY_INC** startet eine wöchentliche Teilsicherung im Dateisystem /proj.

Der Zeitplan mit dem Namen **DAILY_INC** startet eine tägliche Teilsicherung. Die nächste Teilsicherung beginnt in 30 Minuten. Da keine Objekte aufgelistet sind, führt der Client die Teilsicherung in Ihrer Standarddomäne aus. Der Zeitplan hat kein Verfallsdatum.

Damit der Status geplanter Ereignisse genauer bestimmt werden kann, enthält die Ausgabe von **query schedule** für einen erweiterten Zeitplan auf Clients von IBM Spectrum Protect Version 5.3 und höher neue Felder. Diese Felder werden immer angezeigt, selbst wenn es sich um einen klassischen Zeitplan oder eine Clientsitzung der Version 5.3 mit einem Server vor Version 5.3 handelt; die neuen Felder sind dann aber leer. Beachten Sie, dass bei einem Client einer älteren Version (vor Version 5.3) der Server den Zeitraum als unendlich und den Wochentag als unzulässigen Tag zurückmeldet. In Tabelle 52 auf Seite 301 wird die Beispielausgabe des Befehls **query schedule** für erweiterte Zeitpläne angezeigt.

Tabelle 52. Beispielausgabe des Befehls 'query schedule' für erweiterte Zeitpläne

```

Zeitplanname: QUARTERLY_FULL
Beschreibung: Vierteljährliche Gesamtsicherung
Zeitplanstil: Erweitert
Aktion: Selektive Sicherung
Optionen: subdir=yes
Objekte: /* /Volumes/fs2/*
Priorität: 5
Nächste Ausführung: 1744 Stunden und 26 Minuten
Dauer: 1 Tag
Periode:
Wochentag: Freitag
Monat: März, Juni, September, Dezember
Tag im Monat: Jeden Tag
Woche im Monat: Letzte
Verfällt: Nie
    
```

Informationen zu beendeter Arbeit anzeigen

Wenn Sie den Befehl **schedule** im Vordergrund ausführen, wird die Ausgabe geplanter Befehle auf Ihrem Bildschirm angezeigt.

Die Ausgabe wird außerdem in die Datei dsmsched.log im Installationsverzeichnis gestellt, wenn Sie den Verzeichnis- und Dateinamen nicht mit der Option schedlogname ändern.

Wenn der Befehl **schedule** im Hintergrund ausgeführt wird, wird die Ausgabe geplanter Befehle in die Datei dsmsched.log im aktuellen Verzeichnis oder in den vom Benutzer angegebenen Pfad und Dateinamen übertragen. Die Datei dsm-sched.log kann keine symbolische Verbindung sein.

Anmerkung: Unter Mac OS X befindet sich das Protokoll standardmäßig an einer der folgenden Positionen:

```
~/Library/Logs/tivoli/tsm
/Library/Logs/tivoli/tsm
```

Wenn die geplante Arbeit beendet ist, im Planungsprotokoll überprüfen, ob die Arbeit erfolgreich ausgeführt wurde.

Wenn ein geplanter Befehl verarbeitet wird, enthält das Planungsprotokoll folgenden Eintrag:

```
Geplantes Ereignis Ereignisname erfolgreich ausgeführt
```

Falls das geplante Ereignis nicht erfolgreich ausgeführt wird, erhalten Sie eine Nachricht wie die Folgende:

```
ANS1512E Geplantes Ereignis Ereignisname fehlgeschlagen. Rückkehrcode = Code.
```

Der Client gibt an, ob IBM Spectrum Protect den geplanten Befehl, der zu dem *Ereignisnamen* gehört, erfolgreich ausgegeben hat (action=command). Erfolg oder Misserfolg des Befehls wird nicht überprüft. Der Status des Befehls kann durch Auswertung des Rückkehrcodes vom geplanten Befehl im Planungsprotokoll bestimmt werden. Vor dem Eintrag für den Rückkehrcode des Befehls im Planungsprotokoll steht folgender Text:

```
Befehl beendet. Der Rückkehrcode lautet:
```

Das Planungsprotokoll kann unendlich groß werden, wenn Sie es nicht mit der Option `schedlogretention` bereinigen oder mit der Option `schedlogmax` eine Maximalgröße angeben.

Zugehörige Konzepte:

„Planungsoptionen angeben“

Planungsoptionen angeben

Sie können Planungsoptionen in der Clientoptionsdatei oder in der grafischen Benutzerschnittstelle (GUI) ändern.

Gibt der Administrator jedoch einen Wert für diese Optionen an, überschreibt dieser Wert die Angabe des Benutzers in der Clientdatei.

Zugehörige Konzepte:

„Planungsoptionen“ auf Seite 340

Zeitplanungsoptionen für Befehle

Der Scheduler führt Befehle unter der Benutzer-ID 0 (Root) aus. Einige Befehle müssen möglicherweise jedoch unter einer anderen Benutzer-ID als 0 ausgeführt werden.

In diesem Fall kann Ihr IBM Spectrum Protect-Administrator mit der Serveroption `schedcmduser` Zeitpläne für Befehle definieren, die unter einer anderen Benutzer-ID als der Benutzer-ID des Schedulers ausgeführt werden.

Die Option `schedcmduser` gibt den Namen eines gültigen Benutzers auf dem System an, auf dem ein geplanter Befehl ausgeführt wird. Diese Option kann nur vom IBM Spectrum Protect-Serveradministrator definiert werden. Wenn diese Option angegeben wird, wird der Befehl mit der Berechtigung des angegebenen Benutzers ausgeführt. Andernfalls wird der Befehl mit der Berechtigung des Schedulers ausgeführt.

►►—SCHEDCMDUser—*Benutzername*—◄◄

Benutzername

Gibt den Namen eines gültigen Benutzers auf dem System an, auf dem ein geplanter Befehl ausgeführt wird.

Anmerkung: Die Option `schedcmduser` beeinflusst *nicht* die Benutzer-ID, die für Befehle vor und nach dem Zeitplan verwendet wird. Befehle vor und nach dem Zeitplan werden immer als Root (Benutzer-ID 0) ausgeführt.

Geplante Befehle aktivieren oder inaktivieren

Sie können die Option `schedcmddisabled` verwenden, um die Planung von Befehlen durch den Server zu inaktivieren.

Befehle werden mithilfe der Option `action=command` im Serverbefehl `DEFINE SCHEDULE` geplant.

Durch die Option `schedcmddisabled` werden die Befehle `preschedulecmd` und `postschedulecmd` nicht inaktiviert. Sie können jedoch `preschedulecmd` oder

postschedulecmd mit einem Leerzeichen oder einer Nullzeichenfolge angeben, um die Zeitplanung dieser Befehle zu inaktivieren.

Mithilfe der Option schedrestretrdisabled können Sie verhindern, dass der IBM Spectrum Protect-Serveradministrator Planungsoperationen für Zurückschreibung oder Abruf ausführt.

Mithilfe der Option srvprepostscheddisabled können Sie verhindern, dass der IBM Spectrum Protect-Serveradministrator bei der Ausführung geplanter Operationen Befehle ausführt, die vor bzw. nach der Ausführung des Zeitplans ausgeführt werden.

Mithilfe der Option srvprepostsnapdisabled können Sie verhindern, dass der IBM Spectrum Protect-Serveradministrator bei der Ausführung geplanter Operationen für Image-Momentaufnahmesicherungen Befehle vor und nach der Momentaufnahme ausführt.

Zugehörige Verweise:

„Schedcmddisabled“ auf Seite 562

„Schedrestretrdisabled“ auf Seite 572

„Srvprepostscheddisabled“ auf Seite 596

„Srvprepostsnapdisabled“ auf Seite 597

Mehrere Zeitplananforderungen auf einem System verwalten

In bestimmten Situationen ist es zu bevorzugen, für jedes Clientsystem mehrere geplante Aktivitäten zu haben.

Informationen zu diesem Vorgang

Normalerweise können Sie dies erreichen, indem Sie einem Knoten mehrere Zeitplandefinitionen zuordnen. Dies ist die Standardmethode für die Ausführung mehrerer Zeitpläne auf einem System.

Sie müssen sicherstellen, dass sich die Zeitplanfenster für die einzelnen Zeitpläne nicht überlappen. Ein einzelner Client-Schedulerprozess ist nicht in der Lage, mehrere geplante Aktionen gleichzeitig auszuführen, d. h., bei einer Überlappung wird der zweite zu startende Zeitplan ausgelassen, wenn der erste Zeitplan nicht bis zum Ende des Startfensters des zweiten Zeitplans beendet ist.

Angenommen, die meisten Dateisysteme auf Ihrem Clientsystem müssen täglich und ein Dateisystem mit kritischen Daten muss stündlich gesichert werden. In diesem Fall müssten Sie für die Handhabung dieser Anforderung zwei Zeitpläne definieren. Um einen Konflikt zwischen dem stündlichen und dem täglichen Datensicherungszeitplan zu vermeiden muss die *Startzeit* der beiden Zeitpläne variiert werden.

In bestimmten Fällen ist es notwendig, mehrere Schedulerprozesse auf einem System auszuführen. Mehrfachprozesse erfordern eine separate Optionsdatei für jeden Prozess und müssen folgende Informationen aufweisen:

- Definieren Sie für jeden Prozess einen eindeutigen Knotennamen.
- Geben Sie für jeden Prozess eindeutige Zeitplan- und Fehlerprotokolle an.
- Im Modus mit Bedienerführung müssen Sie die Option tcpclientport verwenden, um für jeden Prozess einen eindeutigen Anschluss anzugeben.

Die Vorteile bei der Verwendung mehrerer Zeitplanprozesse:

- Sie können mehrere geplante Sicherungen gleichzeitig ausführen.
- Mithilfe der Clientoptionsdatei oder der Überschreibungsoptionen auf dem IBM Spectrum Protect-Server können Sie für jeden gestarteten Zeitplan unterschiedliche Sicherungskriterien angeben.

Die Nachteile bei der Verwendung mehrerer Zeitplanprozesse:

- Für jeden Knotennamen auf dem IBM Spectrum Protect-Server wird ein eindeutiger Dateibereich erstellt.
- Beim Zurückschreiben der Daten müssen Sie denselben Knotennamen verwenden, der der Sicherung zugeordnet ist.

Auf UNIX- und Linux-Plattformen können entweder mit der vom Clientakzeptordämon verwalteten Methode oder mit der traditionellen Methode der Ausführung des Schedulers mehrere Zeitplanprozesse ausgeführt werden. In beiden Fällen gibt es bestimmte Konfigurationsvoraussetzungen:

- Jeder Prozess muss mit einem anderen Knotennamen ausgeführt werden.
- Für jeden Schedulerprozess müssen Sie mehrere Zeilengruppen in der Datei `dsm.sys` erstellen. In jeder Zeilengruppe müssen Sie einen eindeutigen Knotennamen definieren und eindeutige Werte für die Optionen `errorlogname` und `schedlogname` angeben. Sie können für jede Zeilengruppe aber auch angepasste `domain-`, `include-` und `exclude-`Anweisungen definieren.
- Setzen Sie in Ihrer Datei `dsm.sys` die Option `passwordaccess` in jeder Zeilengruppe auf `'generate'`. Das Kennwort muss für jeden Knotennamen, der einen Schedulerprozess ausführt, generiert werden, indem ein Befehl wie z. B. `dsmc query sess` ausgeführt wird.
- Ist bei der Ausführung die Option `schedmode` auf `prompt` gesetzt, sollten Sie einen eindeutigen `tcpclientport`-Wert für jede Zeilengruppe definieren.

Sie müssen jeden Befehl bzw. jede Instanz `dsmc sched` mit der Option `-servername` starten, um in `dsm.sys` auf den eindeutigen Zeilengruppennamen zu verweisen. Bei `dsmcad` ist es erforderlich, für jede Instanz von `dsmcad` die Umgebungsvariable `DSM_CONFIG` zu definieren, um auf die eindeutige Optionsdatei zu verweisen.

Das folgende Beispiel zeigt die Konfiguration zweier Zeitplanprozesse, die vom Clientakzeptordämon verwaltet werden, in der Datei `dsm.sys`. Bitte beachten Sie, dass Sie vollständige Pfadangaben für die Namen der Protokolldateien verwenden müssen, um zu vermeiden, dass die Dateien in das Stammverzeichnis geschrieben werden:

```

servername tsm1_sched1
nodename      aixsvt01_sched1
tcpserve      firebat
tcpclientport 1507
passwordaccess generate
domain        /svt1
schedmode     prompted
schedlogname  /tsm/dsmsched1.log
errorlogname  /tsm/dsmerror1.log
managedservices schedule

servername tsm1_sched2
nodename      aixsvt01_sched2
tcpserve      firebat
tcpclientport 1508
passwordaccess generate
domain        /svt1
schedmode     prompted
schedlogname  /tsm/dsmsched2.log
errorlogname  /tsm/dsmerror2.log
managedservices schedule

```

Inhalt von /test/dsm.opt1:

```
servername tsm1_sched1
```

Inhalt von /test/dsm.opt2:

```
servername tsm1_sched2
```

Öffnen Sie zwei Shellbefehlsfenster:

- In Shellbefehlsfenster 1 geben Sie Folgendes ein:

```
export DSM_CONFIG=/test/dsm.opt1
sudo dsmcad
```

- In Shellbefehlsfenster 2 geben Sie Folgendes ein:

```
export DSM_CONFIG=/test/dsm.opt2
sudo dsmcad
```

Anmerkung: Sie sollten diese Befehle in ein Shell-Skript eingeben, falls Sie beabsichtigen, die dsmcad-Prozesse direkt von /etc/inittab zu starten, damit die korrekte Variable DSM_CONFIG definiert werden kann, bevor dsmcad gestartet wird.

Kapitel 8. Clientrückkehrcodes

Die Befehlszeilenschnittstelle für Sichern/Archivieren und der Scheduler werden mit einem Rückkehrcode verlassen, der den Erfolg oder das Fehlschlagen der Clientoperation genau wiedergibt.

Scripts, Stapeldateien und andere Automatisierungsfunktionen können den Rückkehrcode von der Befehlszeilenschnittstelle aus verwenden. Bei Operationen, bei denen der IBM Spectrum Protect-Scheduler verwendet wird, werden die Rückkehrcodes in der Ausgabe des Verwaltungsbefehls **QUERY EVENT** angezeigt.

Im Allgemeinen bezieht sich der Rückkehrcode auf die Nachricht mit der höchsten Wertigkeit während der Clientoperation.

- Ist die Nachricht mit der höchsten Wertigkeit eine Informationsnachricht (ANSnnnnI), lautet der Rückkehrcode 0.
- Ist die Nachricht mit der höchsten Wertigkeit eine Warnung (ANSnnnnW), lautet der Rückkehrcode 8.
- Ist die Nachricht mit der höchsten Wertigkeit eine Fehlermeldung (ANSnnnnE oder ANSnnnnS), lautet der Rückkehrcode 12.

Eine Ausnahme von den genannten Regeln tritt auf, wenn Warnungen oder Fehlermeldungen anzeigen, dass einzelne Dateien nicht verarbeitet werden konnten. Der Rückkehrcode für Dateien, die nicht verarbeitet werden können, ist 4. Überprüfen Sie die Datei `dsmerror.log`, um die Ursache der Fehler festzustellen, die während der Clientoperationen auftreten. Fehler, die während geplanter Ereignisse auftreten, werden in der Datei `dsmsched.log` aufgezeichnet.

Tabelle 53 enthält eine Beschreibung der Rückkehrcodes und ihrer Bedeutung.

Tabelle 53. Clientrückkehrcodes und ihre Bedeutung

Code	Erläuterung
0	Alle Operationen wurden erfolgreich abgeschlossen.
4	Die Operation wurde erfolgreich abgeschlossen, einige Dateien wurden jedoch nicht verarbeitet. Es sind keine anderen Fehler oder Warnungen aufgetreten. Dieser Rückkehrcode kommt häufig vor. Dateien werden aus verschiedenen Gründen nicht verarbeitet; die folgende Liste enthält die häufigsten Gründe. <ul style="list-style-type: none">• Die Datei entspricht einem Eintrag in einer Ausschlussliste. Ausgeschlossene Dateien generieren Protokolleinträge nur während selektiver Sicherungen.• Die Datei wurde von einer anderen Anwendung verwendet, und der Client konnte nicht auf die Datei zugreifen.• An der Datei wurden während der Operation so viele Änderungen vorgenommen, die aufgrund des Attributs für die Kopiennummerierung nicht zulässig sind. Siehe „Attribut 'Kopiennummerierung'“ auf Seite 313.
8	Die Operation wurde mit mindestens einer Warnung abgeschlossen. Bei geplanten Ereignissen lautet der Status Beendet. Überprüfen Sie die Datei <code>dsmerror.log</code> (und für geplante Ereignisse die Datei <code>dsmsched.log</code>) auf ausgegebene Warnungen, um ihre Auswirkungen auf die Operation zu bestimmen.

Tabelle 53. Clientrückkehrcodes und ihre Bedeutung (Forts.)

Code	Erläuterung
12	Die Operation wurde mit mindestens einer Fehlnachricht (außer Fehlnachrichten für übersprungene Dateien) abgeschlossen. Bei geplanten Ereignissen lautet der Status Fehlgeschlagen. Überprüfen Sie die Datei <code>dsmerror.log</code> (und für geplante Ereignisse die Datei <code>dsmsched.log</code>) auf ausgegebene Fehlnachrichten, um ihre Auswirkungen auf die Operation zu bestimmen. Im Allgemeinen bedeutet dieser Rückkehrcode, dass der Fehler schwerwiegend genug war, um die erfolgreiche Beendigung der Operation zu verhindern. Beispielsweise gibt ein Fehler, der die Verarbeitung eines vollständigen Dateisystems verhindert, den Rückkehrcode 12 aus.
<i>Sonstige</i>	<p>Bei geplanten Operationen, bei denen ein Befehl ausgeführt wird, wird der Rückkehrcode des ausgeführten Befehls zurückgegeben. Ist der Rückkehrcode 0, lautet der Status der geplanten Operation Beendet. Hat der Rückkehrcode einen anderen Wert als 0, lautet der Status Fehlgeschlagen.</p> <p>Einige Befehle geben möglicherweise einen anderen Rückkehrcode als Null zurück, wenn die Operation erfolgreich ausgeführt wurde. Für diese Befehle können Sie den Status Fehlgeschlagen vermeiden, wenn Sie den Befehl in ein Script <i>verpacken</i>, das den Befehl startet, das Ergebnis interpretiert und beendet wird. Das Script sollte den Rückkehrcode 0 ausgeben, wenn der Befehl erfolgreich war, oder einen Rückkehrcode ungleich null, wenn der Befehl fehlgeschlagen ist. Bitten Sie dann Ihren IBM Spectrum Protect-Serveradministrator, die Zeitplandefinition so zu ändern, dass Ihr Script anstelle des Befehls ausgeführt wird.</p>

Der Rückkehrcode für ein Clientmakro ist der höchste der Rückkehrcodes, die für die einzelnen Befehle ausgegeben werden, aus denen das Makro besteht. Ein Makro besteht beispielsweise aus den folgenden Befehlen:

```
selective "/home/devel/*" -subdir=yes
incremental "/home/devel/TestDriver/*" -subdir=yes
archive "/home/plan/proj1/*" -subdir=yes
```

Wenn der erste Befehl mit dem Rückkehrcode 0, der zweite Befehl mit dem Rückkehrcode 8 und der dritte Befehl mit dem Rückkehrcode 4 beendet wird, ist der Rückkehrcode für das Makro 8.

Weitere Informationen zum Befehl **QUERY EVENT** finden Sie in der Dokumentation zum IBM Spectrum Protect-Server.

Zugehörige Konzepte:

„Zeitplanungsoptionen für Befehle“ auf Seite 302

Kapitel 9. Speicherverwaltungsmaßnahmen

Speicherverwaltungsmaßnahmen sind vom Administrator definierte Regeln für die Verwaltung der Sicherungen und Archivierungen auf dem Server.

Ihre Daten werden diesen Maßnahmen zugeordnet (oder an sie gebunden); wenn die Daten dann gesichert oder archiviert werden, werden sie gemäß den Maßnahmenbedingungen verwaltet. Zu den Maßnahmekriterien gehören eine Maßnahmen-domäne, eine Maßnahmengruppe, eine Verwaltungsklasse und eine Kopiengruppe.

Maßnahmen legen Folgendes fest:

- Ob eine Datei für Sicherungs- oder Archivierungsservices ausgewählt werden kann.
- Wie viele Sicherungsversionen aufbewahrt werden.
- Wie lange inaktive Sicherungsversionen und Archivierungskopien aufbewahrt werden.
- Wo die Kopien im Speicher aufbewahrt werden.
- Für Teilsicherungen legen Maßnahmen außerdem Folgendes fest:
 - Wie oft eine Datei gesichert werden kann.
 - Ob eine Datei geändert werden muss, bevor sie erneut gesichert wird.

Wenn der IBM Spectrum Protect for Space Management-Client installiert ist, definiert Ihr Administrator auch Regeln, die festlegen, ob Dateien für die Umlagerung aus Ihren lokalen Dateisystemen in den Speicher auswählbar sind.

In diesem Abschnitt wird Folgendes erläutert:

- Maßnahmekriterien (Maßnahmendomänen, Maßnahmengruppen, Kopiengruppen und Verwaltungsklassen)
- Wie Maßnahmen angezeigt werden
- Wie Ihre Daten Maßnahmen zugeordnet werden

Maßnahmendomänen und Maßnahmengruppen

Eine *Maßnahmendomäne* ist eine Gruppe von Clients mit ähnlichen Sicherungs- und Archivierungsanforderungen.

Maßnahmendomänen enthalten eine oder mehrere Maßnahmengruppen. Ein Administrator verwendet Maßnahmendomänen für die logische Verwaltung einer Gruppe von Clientknoten.

Eine Maßnahmendomäne kann beispielsweise Folgendes enthalten:

- Eine Abteilung, z. B. Buchhaltung.
- Einen physischen Standort, wie z. B. ein bestimmtes Gebäude oder Stockwerk.
- Ein lokales Netz, wie z. B. alle Clients, die einem bestimmten Dateiserver zugeordnet sind.

IBM Spectrum Protect enthält eine Standardmaßnahmendomäne mit dem Namen *Standard*. Der Clientknoten ist am Anfang eventuell der Standardmaßnahmendomäne zugeordnet. Der Administrator kann jedoch zusätzliche Maßnahmendomänen definieren, wenn weitere Benutzergruppen mit eindeutigen Sicherungs- und Archivierungsanforderungen vorhanden sind.

Eine *Maßnahmengruppe* besteht aus mindestens einer Verwaltungsklasse. Eine Maßnahmendomäne kann viele Maßnahmengruppen enthalten. Der Administrator verwendet eine Maßnahmengruppe, um verschiedene Verwaltungsklassen auf der Basis von Geschäfts- und Benutzeranforderungen zu implementieren. Es kann nur jeweils eine Maßnahmengruppe aktiv sein. Sie wird als *aktive Maßnahmengruppe* bezeichnet. Jede Maßnahmengruppe enthält eine *Standardverwaltungsklasse* und eine beliebige Anzahl zusätzlicher Verwaltungsklassen.

Verwaltungsklassen und Kopiengruppen

Eine *Verwaltungsklasse* ist eine Gruppe von Sicherungs- und Archivierungskopiengruppen, die bestimmte Speicherverwaltungsanforderungen zum Sichern und Archivieren von Daten enthält.

Ein Administrator kann separate Verwaltungsklassen für die Sicherungs- und Archivierungsanforderungen unterschiedlicher Daten definieren, wie z. B.:

- Geschäftskritische Systemdaten
- Anwendungsdaten, die sich häufig ändern
- Berichtsdaten, die monatlich über die Verwaltung überprüft werden
- Rechtliche Hinweise, die ohne zeitliche Begrenzung aufbewahrt werden müssen und viel Plattenspeicherplatz erfordern

Anmerkung: Wenn IBM Spectrum Protect for Space Management installiert ist, können auch spezifische Anforderungen für die Umlagerung von Dateien in Speicher enthalten sein.

Die meisten Änderungen von Speicherverwaltungsmaßnahmen betreffen Verwaltungsklassen. Alle Dateien und Verzeichnisse, die Sie sichern, und alle Dateien, die Sie archivieren, sind wie folgt einer Verwaltungsklasse zugeordnet (oder an sie *gebunden*):

- Sind Ihre Daten keiner Verwaltungsklasse zugeordnet, verwendet IBM Spectrum Protect die Standardverwaltungsklasse in der aktiven Maßnahmengruppe.
- Beim Sichern von Verzeichnissen können Sie eine Verwaltungsklasse mit einer Anweisung *include* oder mit der Option *dirmc* angeben. Wird keine Verwaltungsklasse angegeben, verwendet IBM Spectrum Protect diejenige Verwaltungsklasse in der aktiven Maßnahmengruppe, die die längste Aufbewahrungsdauer für einzige Version angibt. Erfüllen mehrere Verwaltungsklassen dieses Kriterium, verwendet IBM Spectrum Protect die letzte gefundene Verwaltungsklasse in alphabetischer Reihenfolge.
- Für das Archivieren von Verzeichnissen können Sie eine Verwaltungsklasse mit der Anweisung *include.archive* oder mit der Option *archmc* angeben. Wird keine Verwaltungsklasse angegeben, ordnet der Server dem Archivierungsverzeichnis die Standardverwaltungsklasse zu. Hat die Standardverwaltungsklasse keine Archivierungskopiengruppe, ordnet der Server die Verwaltungsklasse zu, die derzeit über die Archivierungskopiengruppe mit dem kürzesten Aufbewahrungszeitraum verfügt.

Sie können *include*-Anweisungen in Ihrer Einschluss-/Ausschlussliste verwenden, um Dateien Verwaltungsklassen zuzuordnen. In Ihrer Clientoptionsdatei können Sie mit der Option *dirmc* Verzeichnisse einer Verwaltungsklasse zuordnen.

Innerhalb einer Verwaltungsklasse befinden sich die spezifischen Sicherungs- und Archivierungsanforderungen in den *Kopiengruppen*. Kopiengruppen definieren die spezifischen Speicherverwaltungsattribute, die beschreiben, wie der Server gesicherte oder archivierte Daten verwaltet. Zu den Kopiengruppen gehören *Siche-*

rungskopiengruppen und *Archivierungskopiengruppen*. Eine Verwaltungsklasse kann eine Sicherungskopiengruppe und/oder eine Archivierungskopiengruppe oder keine Kopiengruppe enthalten.

Eine *Sicherungskopiengruppe* enthält Attribute, mit denen während der Sicherung Folgendes bestimmt wird:

- Wie viele Tage vergehen müssen, bis eine Datei wieder gesichert wird.
- Wie eine Datei während einer Sicherung verarbeitet wird, wenn sie im Gebrauch ist.

Sie enthält außerdem Attribute, mit denen die Sicherungsversionen der Dateien auf dem Server verwaltet werden. Diese Attribute steuern Folgendes:

- Auf welchem Datenträgertyp der Server Sicherungsversionen Ihrer Dateien und Verzeichnisse speichert.
- Wie viele Sicherungsversionen Ihrer Dateien und Verzeichnisse der Server aufbewahrt.
- Wie lange der Server Sicherungsversionen Ihrer Dateien und Verzeichnisse aufbewahrt.
- Wie lange der Server inaktive Sicherungsversionen aufbewahrt.
- Wie lange die letzte verbliebene inaktive Version einer Datei aufbewahrt wird.

Eine *Archivierungskopiengruppe* enthält Attribute, die Folgendes steuern:

- Ob eine Datei archiviert wird, die im Gebrauch ist.
- Auf welchem Datenträgertyp der Server Archivierungskopien Ihrer Dateien speichert.
- Wie lange der Server Archivierungskopien der Dateien aufbewahrt.

Zugehörige Konzepte:

„Verwaltungsklasse für Dateien auswählen“ auf Seite 315

„Aufbewahrungszeitraum“ auf Seite 319

Informationen zu Verwaltungsklassen und Kopiengruppen anzeigen

Sie können Maßnahmeninformationen mit der Befehlszeilenschnittstelle oder mit einer grafischen Benutzerschnittstelle anzeigen.

Klicken Sie in einer grafischen Benutzerschnittstelle auf **Maßnahmeninformationen anzeigen** im Menü 'Dienstprogramme'. Im Fenster **Maßnahmeninformationen** werden die verfügbaren Verwaltungsklassen angezeigt. In einer Befehlszeile verwenden Sie den Befehl **query mgmtclass**, um die verfügbaren Verwaltungsklassen anzuzeigen. Mit der Option **detail** erhalten Sie weitere Informationen.

Tabelle 54 zeigt die Standardwerte für die Sicherungs- und Archivierungskopiengruppen in der Standardverwaltungsklasse.

Tabelle 54. Standardattributwerte in der Standardverwaltungsklasse

Attribut	Standardwert für Sicherung	Standardwert für Archivierung
Name der Kopiengruppe	Standard	Standard
Kopienart	Sichern	Archivieren
Kopienhäufigkeit	0 Tage	CMD (Befehl)
Versionen bestehender Daten	2 Versionen	Nicht zutreffend
Versionen gelöschter Daten	1 Version	Nicht zutreffend

Tabelle 54. Standardattributwerte in der Standardverwaltungsklasse (Forts.)

Attribut	Standardwert für Sicherung	Standardwert für Archivierung
Extraversionen aufbewahren	30 Tage	Nicht zutreffend
Einzige Version aufbewahren	60 Tage	Nicht zutreffend
Kopiennummerierung	Gemeinsam statisch	Gemeinsam statisch
Kopienmodus	Geändert	Absolut
Kopienziel	Backuppool	Archivepool
Version aufbewahren	Nicht zutreffend	365 Tage
LAN-unabhängig	Ziel	No
Deduplizierung aktiviert	No	No

Attribut 'Kopiengruppenname'

Das Attribut *Kopiengruppenname* ist der Name der Kopiengruppe. Der Standardwert für die Sicherung und Archivierung ist *Standard*.

Attribut 'Kopienart'

Das Attribut *Kopienart* ist die Art der Kopiengruppe. Der Wert für Sicherungen lautet immer *Sichern*, der Wert für Archivierungen immer *Archivieren*.

Attribut 'Kopienhäufigkeit'

Das Attribut *Kopienhäufigkeit* ist die Mindestanzahl Tage, die zwischen aufeinanderfolgenden Teilsicherungen vergehen muss. Verwenden Sie dieses Attribut während einer vollständigen Teilsicherung.

Die Kopienhäufigkeit arbeitet mit dem Parameter **mode** zusammen. Gelten beispielsweise frequency=0 und mode=modified, wird eine Datei oder ein Verzeichnis nur gesichert, wenn sie bzw. es sich seit der letzten Teilsicherung geändert hat. Gelten frequency=0 und mode=absolute, wird ein Objekt bei jeder Teilsicherung gesichert. Gelten frequency=0 und mode=absolute, haben Änderungen und die Anzahl Tage seit der letzten Sicherung keinen Einfluss auf die aktuelle Sicherungsoperation. Das Attribut für die Häufigkeit (frequency) wird bei selektiven Sicherungen nicht überprüft.

Bei Archivierungskopiengruppen lautet die Einstellung für die Kopienhäufigkeit immer CMD (Befehl). Beim Archivieren eines Objekts gibt es keine Einschränkungen bezüglich der Häufigkeit.

Bei einer journalbasierten Sicherung wird die Kopienhäufigkeit ignoriert.

Attribut 'Versionen bestehender Daten'

Das Attribut *Versionen bestehender Daten* gibt die maximale Anzahl verschiedener Sicherungsversionen an, die für Dateien und Verzeichnisse aufbewahrt werden.

Wird eine Verwaltungsklasse ausgewählt, die mehrere Sicherungsversionen zulässt, wird die aktuellste Version als *aktive* Version bezeichnet. Alle anderen Versionen werden als *inaktive* Versionen bezeichnet. Beträgt die maximal zulässige Anzahl der Versionen 5 und wird bei einer Sicherung eine sechste Version erstellt, wird die älteste Version aus dem Serverspeicher gelöscht.

Attribut 'Versionen gelöschter Daten'

Das Attribut *Versionen gelöschter Daten* gibt die maximale Anzahl verschiedener Sicherungsversionen an, die für gelöschte Dateien und Verzeichnisse aufbewahrt werden.

Dieser Parameter wird ignoriert, bis Sie die Datei oder das Verzeichnis löschen.

Wenn Sie die Datei oder das Verzeichnis löschen, wird die aktive Sicherungsversion bei der nächsten Teilsicherung zu einer inaktiven Version. Der IBM Spectrum Protect-Server löscht die ältesten Versionen, die die durch diesen Parameter angegebene Anzahl überschreiten.

Das Verfallsdatum für die übrigen Versionen richtet sich nach den Parametern *Extraversionen aufbewahren* und *Einzige Version aufbewahren*.

Attribut 'Extraversionen aufbewahren'

Das Attribut *Extraversionen aufbewahren* gibt an, wie viele Tage alle Sicherungsversionen außer der aktuellsten Sicherungsversion aufbewahrt werden.

Die aktuellste Version ist die aktive Version, die nie gelöscht wird. Wird *Keine Begrenzung* angegeben, werden Extraversionen aufbewahrt, bis die Anzahl der Sicherungsversionen den Wert des Parameters *Versionen bestehender Daten* oder *Versionen gelöschter Daten* überschreitet. In diesem Fall wird die älteste Extraversion sofort gelöscht.

Attribut 'Einzige Version aufbewahren'

Das Attribut *Einzige Version aufbewahren* gibt die Anzahl Tage an, während der die letzte inaktive Version einer Datei oder eines Verzeichnisses aufbewahrt wird.

Wird *Keine Begrenzung* angegeben, wird die letzte Version unbegrenzt aufbewahrt.

Nach dem Löschen einer Datei aus dem Clientsystem wird dieser Parameter bei der nächsten Teilsicherung wirksam. Alle nachfolgenden Aktualisierungen dieses Parameters wirken sich nicht auf Dateien aus, die bereits inaktiv sind. Beispiel: Ist dieser Parameter auf 10 Tage gesetzt, wenn eine Datei während einer Teilsicherung inaktiviert wird, wird die Datei nach 10 Tagen vom Server gelöscht.

Attribut 'Kopiennummerierung'

Das Attribut *Kopiennummerierung* legt fest, ob eine Datei während einer Sicherung oder Archivierung im Gebrauch sein kann und welche Maßnahmen zu ergreifen sind, wenn dies der Fall ist.

Dieses Attribut kann einen der folgenden Werte aufweisen:

- **Statisch.** Eine Datei oder ein Verzeichnis darf während einer Sicherung oder Archivierung nicht geändert werden. Wird das Objekt während eines Sicherungs- oder Archivierungsversuchs geändert, wird es nicht gesichert oder archiviert.
- **Gemeinsam statisch.** Eine Datei oder ein Verzeichnis darf während der Sicherung oder Archivierung nicht geändert werden. Der Client wiederholt einen Sicherungs- oder Archivierungsversuch abhängig von dem für die Option *changingretries* in Ihrer Optionsdatei angegebenen Wert maximal vier Mal. Wird das Objekt bei jedem Sicherungs- oder Archivierungsversuch geändert, wird es nicht gesichert oder archiviert.

- **Dynamisch.** Eine Datei oder ein Verzeichnis wird beim ersten Versuch gesichert oder archiviert, auch wenn sie bzw. es sich während der Sicherung oder Archivierung ändert.
- **Gemeinsam dynamisch.** Eine Datei oder ein Verzeichnis wird gesichert oder archiviert, auch wenn sie bzw. es sich während der Sicherung oder Archivierung ändert. Der Client wiederholt einen Sicherungs- oder Archivierungsversuch maximal vier mal. Die Anzahl der Versuche ist von dem Wert abhängig, der für die Option `changingretries` in Ihrer Optionsdatei angegeben ist. Die Datei wird beim letzten Versuch gesichert oder archiviert, auch wenn sie sich ändert.

Bei einer Verwaltungsklasse, die die Sicherung oder Archivierung einer im Gebrauch befindlichen Datei gestattet, wird die Sicherungsversion oder Archivierungskopie im Serverspeicher möglicherweise als Kopie mit grober Übereinstimmung gespeichert. Eine *Kopie mit grober Übereinstimmung* ist eine Sicherungsversion oder Archivierungskopie, die den aktuellen Inhalt einer Datei nicht korrekt wiedergibt. Sie kann einige, jedoch nicht alle Änderungen enthalten. Ist dies nicht akzeptabel, muss eine Verwaltungsklasse ausgewählt werden, die eine Sicherungsversion oder Archivierungskopie nur dann erstellt, wenn sich die Datei während der Sicherung oder Archivierung nicht ändert. Wenn Sie die statische Durchnummerierung verwenden, können Anwendungen eine Datei nicht mit Schreibzugriff öffnen, während die Datei gesichert wird.

Wird eine Dateikopie mit grober Übereinstimmung zurückgeschrieben oder abgerufen, ist die Datei möglicherweise unbrauchbar. Sie sollten die Durchnummerierung "Dynamisch" oder "Gemeinsam dynamisch" beim Sichern von Dateien nur verwenden, wenn Sie sicher sind, dass die Zurückschreibung der Kopie mit grober Übereinstimmung verwendbar ist.

Wichtig: Bei der Auswahl einer Verwaltungsklasse, die eine Kopiengruppe mit der Durchnummerierung "Gemeinsam dynamisch" oder "Dynamisch" enthält, muss mit besonderer Vorsicht vorgegangen werden.

Zugehörige Verweise:

„Snapshotproviderimage“ auf Seite 592

Parameter für den Kopienmodus

Der Parameter für den **Kopienmodus** legt fest, ob eine Datei oder ein Verzeichnis für die Teilsicherung unabhängig davon berücksichtigt wird, ob sie bzw. es sich seit der letzten Sicherung geändert hat.

Bei der Ausführung selektiver Sicherungen überprüft der Client den Parameter für den Modus nicht.

Der Wert für diesen Parameter kann eine der folgenden Einstellungen sein:

geändert

Das Objekt wird bei der Teilsicherung nur dann berücksichtigt, wenn es sich seit der letzten Sicherung geändert hat. Ein Objekt wird als geändert betrachtet, wenn eine der folgenden Bedingungen zutrifft:

- Abweichung des Datums oder der Uhrzeit der letzten Änderung.
- Größenabweichung.
- Wenn sich nur die Metadaten (wie beispielsweise Zugriffsberechtigungen) ändern, sichert der Client unter Umständen nur die Metadaten.
- Eigenerabweichung.

absolut

Das Objekt wird bei der Teilsicherung berücksichtigt, unabhängig davon, ob es sich seit der letzten Sicherung geändert hat. Bei Archivierungskopien-

gruppen lautet der Modus immer **Absolut**, d. h., ein Objekt wird unabhängig davon archiviert, ob es sich seit der letzten Archivierungsanforderung geändert hat.

Zugehörige Verweise:

„Absolute“ auf Seite 355

Attribut 'Kopienziel'

Das Attribut *Kopienziel* gibt das Ziel an, an dem Sicherungen oder Archivierungen gespeichert werden.

Das Ziel kann ein Speicherpool mit Platteneinheiten oder ein Speicherpool mit Einheiten, die austauschbare Datenträger (z. B. Band) unterstützen, sein.

Attribut 'Version aufbewahren'

Das Attribut *Version aufbewahren* gibt die Anzahl Tage an, die eine archivierte Datei im Speicher aufbewahrt wird.

Nach Ablauf der angegebenen Anzahl an Tagen für die archivierte Kopie einer Datei wird sie aus dem Serverspeicher gelöscht.

Attribut 'Daten deduplizieren'

Das Attribut *Daten deduplizieren* gibt an, ob während der Sicherungs- und Archivierungsverarbeitung redundante Daten an den IBM Spectrum Protect-Server übertragen werden.

Zugehörige Konzepte:

„Clientseitige Datendeduplizierung“ auf Seite 90

Zugehörige Verweise:

„Deduplication“ auf Seite 394

„Enablededupcache“ auf Seite 426

„Exclude-Optionen“ auf Seite 438

Verwaltungsklasse für Dateien auswählen

Entspricht die Standardverwaltungsklasse den Sicherungs- und Archivierungsanforderungen für alle Dateien auf der Workstation des Benutzers, muss der Benutzer die Dateien dieser Verwaltungsklasse nicht zuordnen. Die Zuordnung erfolgt automatisch beim Sichern oder Archivieren der Dateien.

Wenn für Dateien eine andere Verwaltungsklasse ausgewählt wird, müssen folgende Fragen beachtet werden:

- Enthält die Verwaltungsklasse eine Sicherungskopiengruppe?
Wird versucht, eine Datei zu sichern, die einer Verwaltungsklasse ohne Sicherungskopiengruppe zugeordnet ist, wird die Datei nicht gesichert.
- Enthält die Verwaltungsklasse eine Archivierungskopiengruppe?
Es ist nicht möglich, eine Datei zu archivieren, die einer Verwaltungsklasse ohne Archivierungskopiengruppe zugeordnet ist.
- Enthält die Sicherungskopiengruppe Attribute, die eine ausreichend häufige Sicherung der Dateien gewährleisten?
Kopienmodus und -häufigkeit legen gemeinsam fest, wie oft eine Datei bei Teilsicherungen gesichert wird. Diese Attribute werden bei einer selektiven Sicherung nicht überprüft.

- Welche Nummerierungsmethode wird von der Kopiengruppe verwendet?
Die Nummerierungsmethode bestimmt das Verhalten von IBM Spectrum Protect, wenn sich eine Datei während ihrer Sicherung ändert.
- Sind in der Sicherungskopiengruppe eine angemessene Anzahl Sicherungsversionen angegeben?
- Ist in der Archivierungskopiengruppe ein angemessener Aufbewahrungszeitraum für Archivierungskopien angegeben?

Zugehörige Konzepte:

„Attribut 'Kopiennummerierung'“ auf Seite 313

Dateien eine Verwaltungsklasse zuordnen

Eine Verwaltungsklasse definiert, wann Dateien bei einer Sicherung berücksichtigt werden, wie lange sie auf dem Server aufbewahrt werden und wie viele Versionen einer Datei der Server aufbewahren soll.

Der Serveradministrator wählt eine Standardverwaltungsklasse aus. Der Benutzer kann eine eigene Verwaltungsklasse angeben, um die Standardverwaltungsklasse außer Kraft zu setzen.

Soll Verzeichnissen eine andere Verwaltungsklasse als die Standardverwaltungsklasse zugeordnet werden, verwenden Sie die Option `dirmc` in Ihrer Optionsdatei.

Sie können eine Verwaltungsklasse für eine Datei oder Dateigruppe zuordnen, indem Sie eine Anweisung `include` in Ihrer Optionsdatei verwenden. Sie können auch eine Verwaltungsklasse zuordnen, indem Sie eine Anweisung `include` in der Einschluss-/Ausschlussdatei verwenden, die durch die Option `incl excl` angegeben ist. Bei dem Namen der Verwaltungsklasse muss die Groß-/Kleinschreibung nicht berücksichtigt werden.

Soll mithilfe des Befehlszeilenclients allen Dateien im Verzeichnis `costs` die Verwaltungsklasse `budget` zugeordnet werden, geben Sie Folgendes ein:

```
include /home/proj2/costs/* budget
```

Soll eine Verwaltungsklasse mit dem Namen `managall` angegeben werden, die für alle Dateien verwendet werden soll, denen Sie nicht explizit eine Verwaltungsklasse zuordnen, geben Sie Folgendes ein:

```
include /* managall
```

Die folgenden Beispiele zeigen, wie Dateien eine Verwaltungsklasse zugeordnet wird:

```
exclude /*.sno
include /home/winter/*.* ice mcweekly
include /home/winter/december/*.* ice mcdaily
include /home/winter/january/*.* ice mcmmonthly
include /home/winter/february/white.sno
```

Folgende Verarbeitungsschritte werden durchgeführt:

1. Die Datei `white.sno` im Verzeichnis `february` im Verzeichnis `winter` wird gemäß den folgenden Regeln für die Verarbeitung von unten nach oben gesichert. Da Sie in dieser Anweisung keine Verwaltungsklasse angegeben haben, wird der Datei die Standardverwaltungsklasse zugeordnet.
2. Allen Dateien mit der Erweiterung `ice` im Verzeichnis `january` wird die Verwaltungsklasse `mcmmonthly` zugeordnet.

3. Allen Dateien mit der Erweiterung `ice` im Verzeichnis `december` wird die Verwaltungsklasse `mcdaily` zugeordnet.
4. Allen übrigen Dateien mit der Erweiterung `ice` in einem beliebigen Verzeichnis unter dem Verzeichnis `winter` wird die Verwaltungsklasse `mcweekly` zugeordnet.
5. Alle Dateien mit der Erweiterung `sno` in allen Verzeichnissen werden von der Sicherung ausgeschlossen. Die Ausnahme zu dieser Regel ist `white.sno` im Verzeichnis `february`, das sich im Verzeichnis `winter` befindet.

Soll eine eigene Standardverwaltungsklasse `Verwaltungsklassenname` für Dateien angegeben werden, die nicht explizit eingeschlossen werden, stellen Sie die folgende Anweisung an den Anfang Ihrer Einschlussliste:

```
include /*.../* Verwaltungsklassenname
```

Wenn eine Datei mithilfe der grafischen Benutzerschnittstelle archiviert wird, kann eine andere Verwaltungsklasse ausgewählt werden, um die der Datei zugeordnete Verwaltungsklasse außer Kraft zu setzen.

Zugehörige Verweise:

„Dirmc“ auf Seite 402

„Include-Optionen“ auf Seite 473

Verwaltungsklasse für archivierte Dateien überschreiben

Wenn Sie eine Datei archivieren, können Sie die zugeordnete Verwaltungsklasse mit der grafischen Benutzerschnittstelle (GUI) überschreiben oder indem Sie die Option `archmc` im Befehl **archive** verwenden.

Die Überschreibung der Verwaltungsklasse mit der GUI ist äquivalent zu der Verwendung der Option `archmc` im Befehl **archive**. In der grafischen Benutzerschnittstelle müssen Sie die Schaltfläche **Optionen** in der Archivierungsbaumstruktur drücken, um die Verwaltungsklasse zu überschreiben und eine andere Verwaltungsklasse auszuwählen.

Geben Sie in der Befehlszeile den folgenden Befehl ein, um der Datei `budget.jan` die Verwaltungsklasse **ret2yrs** zuzuordnen:

```
dsmc archive -archmc=ret2yrs /home/jones/budget.jan
```

Verwaltungsklasse für Verzeichnisse auswählen

Entspricht die Verwaltungsklasse in Ihrer aktiven Maßnahmengruppe mit der längsten Einstellung für "Einzigste Version aufbewahren" (RETONLY) Ihren Sicherungsanforderungen für Verzeichnisse, ist es möglicherweise nicht notwendig, dieser Verwaltungsklasse Verzeichnisse zuzuordnen. Die Zuordnung der Verwaltungsklasse erfolgt automatisch bei der Sicherung Ihrer Verzeichnisse.

Wenn mehrere Verwaltungsklassen mit der längsten Einstellung für RETONLY vorhanden sind, wählt der IBM Spectrum Protect-Client die Verwaltungsklasse aus, deren Name in alphabetischer Reihenfolge an letzter Stelle steht.

Entspricht die Standardverwaltungsklasse nicht Ihren Anforderungen, müssen Sie eine Verwaltungsklasse mit einem angemessenen Aufbewahrungszeitraum auswählen, der durch den Parameter `Einzigste Version aufbewahren` angegeben wird. Beispiel: Wenn die Verwaltungsklasse Daten direkt auf Band sichert, Sie aber Ihre Verzeichnissicherungen auf Platte haben möchten, müssen Sie eine andere

Verwaltungsklasse auswählen. Verzeichnisse sollten Sie mindestens so lange aufbewahren wie die Dateien, die diesen Verzeichnissen zugeordnet sind.

Verwenden Sie für Sicherungsverzeichnisse die Option `dirmc`, um die Verwaltungsklasse anzugeben, an die die Verzeichnisse gebunden werden.

Verwenden Sie für Archivierungsverzeichnisse die Option `archmc` im Befehl **archive**.

Sie können die folgenden Methoden verwenden, um die verfügbaren Verwaltungsklassen und deren Attribute anzuzeigen:

- GUI- oder Web-Client: Wählen Sie **Maßnahmeninformationen anzeigen** im Menü **Dienstprogramme** aus.
- Befehlszeilenclient: Führen Sie den Befehl `dsmc query mgmtclass -detail` aus.

Anmerkung: Wenn während der Verfallsverarbeitung auf dem IBM Spectrum Protect-Server ein archiviertes Verzeichnis für den Verfall auswählbar ist, prüft der Server, ob es für vorhandene archivierte Dateien erforderlich ist, dass das archivierte Verzeichnis bestehen bleibt. Ist dies der Fall, verfällt das archivierte Verzeichnis nicht und der Client für Sichern/Archivieren aktualisiert das Einfügedatum im archivierten Verzeichnis, um sicherzustellen, dass das Verzeichnis nicht verfällt, bevor die Dateien in ihm verfallen.

Verwaltungsklassen an Dateien binden

Durch das *Binden* wird eine Datei einer Verwaltungsklasse zugeordnet.

Wenn eine Datei zum ersten Mal gesichert wird, bindet sie IBM Spectrum Protect entweder an die Standardverwaltungsklasse oder an die in der Einschluss-/Ausschlussliste angegebene Verwaltungsklasse.

Wenn die Sicherungskopiengruppe der Verwaltungsklasse die Aufbewahrung mehrerer Sicherungsversionen der Datei angibt und wenn mehrere Sicherungen angefordert werden, verfügt der Server immer über eine aktive Sicherungsversion (die aktuelle Version) und mindestens eine inaktive Sicherungsversion der Datei. Alle Sicherungsversionen einer Datei werden an dieselbe Verwaltungsklasse gebunden und gemäß den Attributen in der Sicherungskopiengruppe verwaltet.

Wenn eine Datei zum ersten Mal archiviert wird, bindet sie IBM Spectrum Protect an die Standardverwaltungsklasse, an die in der Einschluss-/Ausschlussliste angegebene Verwaltungsklasse oder an eine Verwaltungsklasse, die angegeben wird, wenn die Archivierungsoptionen während einer Archivierung geändert werden.

Archivierte Dateien werden nicht erneut an eine andere Verwaltungsklasse gebunden. Wenn Sie die Verwaltungsklasse für eine Datei mit einer Anweisung `include .archive`, mit der Option `archmc` oder über die GUI des Clients für Sichern/Archivieren ändern, bleiben zuvor archivierte Kopien der Datei an die Verwaltungsklasse gebunden, die bei ihrer Archivierung angegeben wurde.

Wird eine Datei auf dem Clientsystem gelöscht, werden die inaktiven Objekte dieser Datei nicht erneut gebunden.

Informationen zur Zuordnung von Dateien und Verzeichnissen zu Verwaltungsklassen finden Sie in der Dokumentation zum IBM Spectrum Protect-Server.

Sicherungsversionen von Dateien erneut binden

Beim *erneuten Binden* wird eine Datei oder das Image eines logischen Datenträgers einer neuen Verwaltungsklasse zugeordnet.

Sicherungsversionen von Dateien werden unter folgenden Bedingungen erneut an eine andere Verwaltungsklasse gebunden. In jedem Fall werden die Dateien (aktive und inaktive) erst bei der nächsten Sicherung erneut gebunden.

- Um die Verwaltungsklasse einer Datei zu ändern, wird eine andere Verwaltungsklasse in einer Include-Anweisung angegeben. Die Sicherungen werden gemäß der alten Verwaltungsklasse verwaltet, bis eine neue Sicherung durchgeführt wird.
- Der Administrator löscht die Verwaltungsklasse aus der aktiven Maßnahmengruppe des Benutzers. Die Standardverwaltungsklasse wird zum Verwalten der Sicherungsversionen verwendet, wenn die Datei erneut gesichert wird.
- Der Administrator ordnet den Clientknoten einer anderen Maßnahmendomäne zu, deren aktive Maßnahmengruppe keine Verwaltungsklasse mit demselben Namen enthält. Die Standardverwaltungsklasse für die neue Maßnahmendomäne wird zum Verwalten der Sicherungsversionen verwendet.

Informationen zur Zuordnung von Dateien und Verzeichnissen zu Verwaltungsklassen finden Sie in der Dokumentation zum IBM Spectrum Protect-Server.

Aufbewahrungszeitraum

IBM Spectrum Protect stellt einen *Aufbewahrungszeitraum für Sicherung* und einen *Aufbewahrungszeitraum für Archivierung* zur Verfügung, die die Sicherungs- und Archivierungsdaten schützen sollen, wenn es eine Datei nicht erneut an eine geeignete Verwaltungsklasse binden kann.

Der Aufbewahrungszeitraum für Sicherung wird in folgenden Fällen verwendet:

- Der Benutzer ändert die Verwaltungsklasse einer Datei, aber weder die Standardverwaltungsklasse noch die neue Verwaltungsklasse enthält eine Sicherungskopiengruppe.
- Die Verwaltungsklasse, an die eine Datei gebunden ist, ist nicht mehr vorhanden, und die Standardverwaltungsklasse enthält keine Sicherungskopiengruppe.

Der in der Maßnahmendomäne definierte Aufbewahrungszeitraum für Sicherung startet, wenn eine Teilsicherung ausgeführt wird. Der Standardwert ist 30 Tage. Der Administrator kann diesen Zeitraum jedoch verlängern oder verkürzen.

Wenn der IBM Spectrum Protect-Server eine Datei mithilfe des Aufbewahrungszeitraums für Sicherung verwaltet, werden keine neuen Sicherungsversionen der Datei erstellt. Alle vorhandenen Sicherungsversionen der Datei verfallen 30 Tage (bzw. die in der Maßnahmendomäne angegebene Anzahl Tage) nach dem Tag, an dem sie als inaktiv markiert wurden.

Archivierungskopien werden niemals erneut gebunden, da jede Archivierungsoperation eine andere Archivierungskopie erstellt. Archivierungskopien bleiben an den Verwaltungsklassennamen gebunden, der angegeben wurde, als sie vom Benutzer archiviert wurden. Ist die Verwaltungsklasse, an die eine Archivierungskopie gebunden ist, nicht mehr vorhanden, oder enthält sie keine Archivierungskopiengruppe mehr, verwendet der Server die Standardverwaltungsklasse. Wenn Sie später die Standardverwaltungsklasse ändern oder ersetzen, verwendet der Server die aktualisierte Standardverwaltungsklasse, um die Archivierungskopie zu verwalten.

Enthält die Standardverwaltungsklasse keine Archivierungskopiengruppe, verwendet der Server den für die Maßnahmendomäne angegebenen Aufbewahrungszeitraum für Archivierung.

Ereignisgesteuerte Maßnahme für Aufbewahrungsschutz

Alle Verwaltungsklassen mit einer Archivierungskopiengruppe müssen einen Aufbewahrungszeitraum angeben, z. B. die Anzahl Tage, die ein archiviertes Objekt auf dem Server gespeichert wird, bevor es gelöscht wird.

Eine ereignisgesteuerte Maßnahme bietet die Option, dass der Aufbewahrungszeitraum entweder zu dem Zeitpunkt beginnt, an dem das Objekt archiviert wird, oder zu einem späteren Zeitpunkt, wenn ein Aktivierungsereignis für dieses Objekt an den Server gesendet wird.

Mit dem Kopiengruppenwert `RETINIT=CREATE` wird der Aufbewahrungszeitraum für Daten gestartet, wenn die Datei archiviert wird. Mit dem Kopiengruppenwert `RETINIT=EVENT` wird der Aufbewahrungszeitraum für Daten gestartet, wenn der Server benachrichtigt wird, dass das Ereignis eingetreten ist.

Das folgende Beispiel veranschaulicht dieses Konzept:

Der Benutzer verfügt über zwei Dateien, `create.file` und `event.file`. Dem Benutzer stehen zwei Verwaltungsklassen zur Verfügung: `CREATE` mit `RETINIT=CREATE` und `EVENT` mit `RETINIT=EVENT`. Beide Verwaltungsklassen haben einen Aufbewahrungszeitraum von 60 Tagen. Der Benutzer archiviert beide Dateien am selben Tag:

```
dsmc archive create.file -archmc=CREATE
dsmc archive event.file -archmc=EVENT
```

Zehn Tage später gibt der Benutzer den Befehl `set event -type=hold` für die Datei `create.file` aus, damit die Datei nicht gelöscht werden kann. Am selben Tag gibt der Benutzer `set event -type=activate` für die Datei `event.file` aus. Zu diesem Zeitpunkt sind für `create.file` 50 Tage Aufbewahrungszeitraum übrig, und für `event.file` 60 Tage. Wird keine andere Aktion ausgeführt, bleibt `create.file` für immer auf dem Server und `event.file` verfällt 70 Tage nach dem Erstellen (60 Tage nach Eintreten des Ereignisses). Der Benutzer gibt jedoch 20 Tage nach der ursprünglichen Archivierung den Befehl `set event -type=release` für die Datei `create.file` aus. Dreißig Tage ihres Aufbewahrungszeitraums sind vergangen, so dass die Datei in 30 Tagen verfällt (durch die Sperre wird der Aufbewahrungszeitraum nicht erweitert).

Informationen zum Kopiengruppenwert `RETINIT` finden Sie in der Dokumentation zum IBM Spectrum Protect-Server.

Zugehörige Verweise:

„Set Event“ auf Seite 817

Dateien auf einem Datenaufbewahrungsserver archivieren

Bis zu diesem Punkt gibt es keinen Unterschied zwischen der Archivierung auf einem normalen Server und einem Datenaufbewahrungsserver.

Das folgende Beispiel veranschaulicht die Unterschiede zwischen den beiden Servern und was an Tag 5 unternommen werden kann:

Wenn die Dateien nicht auf einem Datenaufbewahrungsserver archiviert wurden, kann der Benutzer den Befehl `delete archive create.file event.file` ausgeben und beide

Dateien werden gelöscht. Wurden die Dateien auf einem Datenaufbewahrungsserver archiviert, schlägt derselbe Befehl bei beiden Dateien fehl. Der Datenaufbewahrungsserver zwingt den Benutzer, die Archivierungen aufzubewahren, bis die vorgegebenen Aufbewahrungskriterien erfüllt sind.

Der Unterschied an Tag 15 (nach der Sperre) sieht wie folgt aus:

Der Befehl **delete archive** *create.file event.file* auf dem Server, der kein Datenaufbewahrungsserver ist, löscht jetzt *event.file*, gibt aber einen Fehler *Löschen nicht möglich* für *create.file* zurück, da die Datei im Haltestatus ist. Bei demselben Befehl auf einem Datenaufbewahrungsserver wird das Löschen beider Dateien immer noch zurückgewiesen.

Kapitel 10. Verarbeitungsoptionen

Sie können Standardwerte für die Verarbeitung von Clientoptionen verwenden oder die Verarbeitungsoptionen so anpassen, dass sie Ihren spezifischen Erfordernissen entsprechen. Dieser Abschnitt enthält eine Übersicht über Verarbeitungsoptionen und einen Optionsreferenzabschnitt, der detaillierte Informationen zu jeder Option bereitstellt.

Zugehörige Konzepte:

„Optionen in Befehlen verwenden“ auf Seite 346

Zugehörige Verweise:

„Syntaxdiagramme lesen“ auf Seite xiv

Übersicht über die Verarbeitungsoptionen

IBM Spectrum Protect verwendet *Verarbeitungsoptionen*, um die Übertragung, die Sicherungs- und Archivierungsverarbeitung und andere Verarbeitungstypen zu steuern.

Sie können Verarbeitungsoptionen in der Clientsystemoptionsdatei (`dsm.sys`), in der Clientbenutzeroptionsdatei (`dsm.opt`) oder in der Befehlszeile angeben.

Sie können folgende Optionstypen definieren:

- Optionen für die Datenübertragung
- Server- und Knotenoptionen
- Verarbeitungsoptionen für Sichern und Archivieren
- Verarbeitungsoptionen für Zurückschreiben und Abrufen
- Planungsoptionen
- Formatoptionen
- Befehlsverarbeitungsoptionen
- Berechtigungsoptionen
- Fehlerverarbeitungsoptionen
- Transaktionsverarbeitungsoptionen
- Web-Client-Optionen
- Diagnoseoptionen

Der Client für Sichern/Archivieren umfasst außerdem eine Gruppe von Clientbefehlsoptionen, die Sie nur in der Befehlszeile mit bestimmten Befehlen eingeben können. Sie können einige der Optionen in Ihrer Optionsdatei überschreiben, indem Sie sie mit den entsprechenden Befehlen für Sichern/Archivieren eingeben.

Zugehörige Konzepte:

„Optionen mit einem Befehl eingeben“ auf Seite 347

Zugehörige Tasks:

„Clientsystemoptionsdatei erstellen und ändern“ auf Seite 58

Übertragungsoptionen

Mithilfe von Übertragungsoptionen können Sie angeben, wie Ihr Clientknoten mit dem IBM Spectrum Protect-Server kommuniziert. Dieser Abschnitt enthält Informationen über die Typen von Übertragungsoptionen, die verwendet werden können.

Für UNIX und Linux verwenden Sie eines der folgenden Übertragungsprotokolle:

- TCP/IP
- Shared Memory (AIX, Linux)

Geben Sie das Übertragungsprotokoll mit der Option `commmethod` an.

Bitten Sie Ihren IBM Spectrum Protect-Administrator um Hilfe bei der Festlegung Ihrer Übertragungsoptionen.

Zugehörige Verweise:

„`Commmethod`“ auf Seite 376

TCP/IP-Optionen

Zur Verwendung des TCP/IP-Übertragungsprotokolls müssen Sie die Option `tcpserveraddress` in Ihre Clientoptionsdatei einschließen.

Die anderen TCP/IP-Optionen haben Standardwerte, die Sie ggf. ändern können. Dieser Abschnitt enthält Informationen über die Typen von Übertragungsoptionen, die verwendet werden können.

Tabelle 55. TCP/IP-Optionen

Option	Beschreibung
<code>httpport</code> „ <code>Httpport</code> “ auf Seite 465	Gibt eine TCP/IP-Anschlussadresse für den Web-Client an.
<code>lanfreetcpport</code> „ <code>Lanfreetcpport</code> “ auf Seite 497	Gibt die Nummer des TCP/IP-Anschlusses an, an dem der IBM Spectrum Protect-Speicheragent empfangsbereit ist.
<code>lanfreetcpsrveraddress</code> „ <code>Lanfreetcpsrveraddress</code> “ auf Seite 499	Gibt die TCP/IP-Adresse für den IBM Spectrum Protect-Speicheragenten an.
<code>tcpbuffsize</code> „ <code>Tcpbuffsize</code> “ auf Seite 609	Gibt die Größe des internen TCP/IP-Kommunikationspuffers in Kilobyte an.
<code>tcpnodelay</code> „ <code>Tcpnodelay</code> “ auf Seite 613	Gibt an, ob der Server oder Client die Verzögerung beim Senden aufeinanderfolgender kleiner Pakete im Netz inaktiviert. Diese Option ist für alle UNIX-Clients gültig.
<code>tcpadminport</code> „ <code>Tcpadminport</code> “ auf Seite 609	Gibt eine separate TCP/IP-Anschlussnummer an, an der der Server Anforderungen für Verwaltungsclientsitzungen erwartet. Dies ermöglicht sichere Verwaltungssitzungen innerhalb eines privaten Netzes.
<code>tcpcadaddress</code> „ <code>Tpcadaddress</code> “ auf Seite 610	Gibt eine TCP/IP-Adresse für <code>dsmcad</code> an.
<code>tcpport</code> „ <code>Tcpport</code> “ auf Seite 614	Gibt die TCP/IP-Anschlussadresse für einen IBM Spectrum Protect-Server an.
<code>tcpserveraddress</code> „ <code>Tcpserveraddress</code> “ auf Seite 614	Gibt die TCP/IP-Adresse für einen IBM Spectrum Protect-Server an.
<code>tcpwindowsize</code> „ <code>Tcpwindowsize</code> “ auf Seite 615	Gibt die Größe (in Kilobyte) des TCP/IP-Schiebefensters für Ihren Clientknoten an.

Tabelle 55. TCP/IP-Optionen (Forts.)

Option	Beschreibung
webports „Webports“ auf Seite 680	Aktiviert die Verwendung des Web-Clients außerhalb einer Firewall, indem die TCP/IP-Anschlussnummer angegeben wird, die vom Clientakzeptordämon und dem Web-Client-Agentenservice (Web-Client-Agentenservice gilt nicht für Mac OS X) für die Kommunikation mit der Web-GUI verwendet wird.

Zugehörige Verweise:

„Nfstimeout“ auf Seite 516

Optionen für Shared Memory

Dieser Abschnitt enthält Informationen über die Shared Memory-Optionen, die Sie verwenden können.

Tabelle 56. Übertragungsoptionen für Shared Memory

Option	Beschreibung
lanfreeshmport „Lanfreeshmport“ auf Seite 496	Gibt die eindeutige Zahl an, die vom Client und vom Speicheragenten verwendet wird, um den für die Datenübertragung verwendeten gemeinsam benutzten Speicherbereich (Shared Memory) zu identifizieren.
lanfreeshmport „Shmport“ auf Seite 579	Gibt die eindeutige Zahl an, die vom Client und vom Server verwendet wird, um den für die Datenübertragung verwendeten gemeinsam benutzten Speicherbereich (Shared Memory) zu identifizieren.

Serveroptionen

Mit der Option `servername` in der Datei `dsm.sys` können Sie eine Gruppe von Optionen (Zeilengruppen) beginnen, mit denen die Verbindung zum IBM Spectrum Protect-Server hergestellt wird.

Sie können mehrere Zeilengruppen in der Datei `dsm.sys` definieren, um eine Verbindung zu verschiedenen Servern herstellen zu können. Unter jeder `servername`-Zeilengruppe müssen alle Clientoptionszeilengruppen aufgelistet sein, die erforderlich sind, um die Kommunikation mit einem Server herzustellen. Die Zeilengruppenliste kann auch andere Optionen für Sicherungs- und Archivierungsoperationen enthalten.

Wenn Ihre Clientsystemoptionsdatei nur eine Zeilengruppe enthält, richtet Ihr Clientknoten alle Serviceanforderungen an den in dieser Zeilengruppe angegebenen Server.

Wenn Ihre Clientsystemoptionsdatei mehrere Zeilengruppen enthält, können Sie mit der Option `defaultserver` einen Standardserver angeben. Wenn Sie keinen Standardserver angeben, stellt IBM Spectrum Protect eine Verbindung zu dem Server her, den Sie in der ersten Zeilengruppe Ihrer Datei `dsm.sys` angeben.

Fügen Sie die Option `defaultserver` am Anfang der Datei `dsm.sys` vor allen Serverzeilengruppen ein. Weitere Informationen enthält „Defaultserver“ auf Seite 396.

Geben Sie mit der Option `servername` in der Clientbenutzeroptionsdatei (`dsm.opt`) oder in der Befehlszeile einen Server an, an den Sicherungs- und Archivierungsser-

viceanforderungen gerichtet werden sollen. Damit wird der in der Datei dsm.sys angegebene Standardserver überschrieben.

Anmerkung: Den in der Clientsystemoptionsdatei angegebenen Umlagerungsserver können Sie nicht überschreiben.

Tabelle 57 zeigt eine dsm.sys-Beispieldatei.

Tabelle 57. Beispiel einer Clientsystemoptionsdatei

Beispieldatei dsm.sys	
DEFAULTServer	server2
SErvername	server1
NODename	node1
COMMMethod	TCPip
TCPPort	1500
TCPServeraddress	node.domain.company.com
PASSWORDAccess	generate
GGroups	system adsm
USERS	ashton stewart kaitlin
INCLExcl	/adm/adsm/backup1.excl
SErvername	server2
COMMMethod	SHAREdmem
shmport	1520
PASSWORDAccess	prompt
GGroups	system adsm
USERS	danielle derek brant
INCLExcl	/adm/adsm/backup2.excl

Verarbeitungsoptionen für Sichern und Archivieren

Sie können Clientoptionen zur Steuerung einiger Aspekte der Sicherungs- und Archivierungsverarbeitung angeben.

Tabelle 58. Verarbeitungsoptionen für Sichern und Archivieren

Option	Beschreibung
afmskipuncachedfiles „Afmskipuncachedfiles“ auf Seite 356	Verwenden Sie die Option afmskipuncachedfiles, um anzugeben, ob bei General Parallel File System (GPFS™) nicht zwischengespeicherte und genutzte Dateien in Active File Management-Dateigruppen bei Sicherungs-, Archivierungs- und Umlagerungsoperationen verarbeitet werden.
archmc „Archmc“ auf Seite 357	Verwenden Sie die Option archmc im Befehl archive , um die verfügbare Verwaltungsklasse für Ihre Maßnahmendomäne anzugeben, an die Sie Ihre archivierten Dateien binden wollen.
archsymb linkasfile „Archsymb linkasfile“ auf Seite 358	Gibt an, ob der Client einer symbolischen Verbindung folgen und die Datei oder das Verzeichnis, auf die bzw. das sie verweist, archivieren soll, oder ob nur die symbolische Verbindung archiviert werden soll.

Tabelle 58. Verarbeitungsoptionen für Sichern und Archivieren (Forts.)

Option	Beschreibung
asnodename „Asnodename“ auf Seite 359	Mit der Option asnodename können Agentenknoten Daten im Namen eines anderen Knotens (des Zielknotens) sichern oder zurückschreiben. Diese Option ermöglicht gleichzeitig ablaufende Operationen von mehreren Knoten, um Daten auf demselben Zielknoten und in demselben Dateibereich parallel zu speichern.
automount „Automount“ auf Seite 368	Verwenden Sie diese Option zusammen mit der Option domain, um alle Auto-Mount-Dateisysteme anzugeben, die der Client zu folgenden Zeitpunkten anzuhängen versucht: <ul style="list-style-type: none"> • Wenn der Client für Sichern/Archivieren gestartet wird • Wenn die Sicherung gestartet wird • Wenn der Client für Sichern/Archivieren während der Sicherung ein Auto-Mount-Dateisystem erreicht
autofsrename „Autofsrename“ auf Seite 366	Gibt an, ob ein vorhandener Dateibereich auf einem Unicode-aktivierten Server umbenannt werden soll, damit für die aktuelle Operation ein Unicode-aktivierter Dateibereich erstellt werden kann.
changingretries „Changingretries“ auf Seite 373	Gibt an, wie oft der Client einen Sicherungs- oder Archivierungsversuch wiederholt, wenn die Datei im Gebrauch ist.
compressalways „Compressalways“ auf Seite 379	Die Option compressalways gibt an, ob die Komprimierung eines Objekts fortgesetzt wird, wenn es während der Komprimierung größer wird. Diese Option ist mit der Option compression zu verwenden.
compression „Compression“ auf Seite 380	Die Option compression komprimiert Dateien, bevor sie an den Server gesendet werden. Die Komprimierung der Dateien reduziert den erforderlichen Datenspeicherplatz für Sicherungsversionen und Archivierungskopien der Dateien.
createnewbase „Createnewbase“ auf Seite 383	Die Option createnewbase erstellt eine Basismomentaufnahme und verwendet sie als Quelle für die Ausführung einer vollständigen Teilsicherung. Mit dieser Option wird die Sicherung aller Dateien sichergestellt, die möglicherweise während der Teilsicherung unter Verwendung der Momentaufnahmedifferenz übersprungen wurden.

Tabelle 58. Verarbeitungsoptionen für Sichern und Archivieren (Forts.)

Option	Beschreibung
deduplication „Deduplication“ auf Seite 394	Gibt an, ob redundante Daten auf der Clientseite entfernt werden sollen, wenn der Client während der Sicherungs- oder Archivierungsverarbeitung Daten an den IBM Spectrum Protect-Server überträgt.
dedupcachepath „Dedupcachepath“ auf Seite 393	Gibt die Position an, an der die Cachedatenbank für die clientseitige Datendeduplizierung erstellt wird, wenn die Option enablededupcache=yes bei der Sicherungs- oder Archivierungsverarbeitung definiert ist.
dedupcachesize „Dedupcachesize“ auf Seite 394	Legt die maximale Größe der Cachedatei für die Datendeduplizierung fest.
enablededupcache „Enablededupcache“ auf Seite 426	Gibt an, ob der Cache für die clientseitige Datendeduplizierung aktiviert werden soll, sodass der Client für Sichern/Archivieren die geänderten Daten aus dem Cache erhält.
deletefiles „Deletefiles“ auf Seite 396	Verwenden Sie die Option deletefiles im Befehl archive , um Dateien von Ihrer Workstation zu löschen, nachdem Sie sie archiviert haben. Diese Option kann auch im Befehl restore image und mit der Option incremental verwendet werden, um Dateien aus dem zurückgeschriebenen Image zu löschen, falls sie nach der Erstellung des Image gelöscht wurden.
Beschreibung „Description“ auf Seite 397	Die Option description ordnet Dateien eine Beschreibung zu oder gibt eine Beschreibung für diese Dateien an, wenn der Client Operationen zum Archivieren, Löschen, Abrufen, Abfragen der Archivierung oder Abfragen des Sicherungssatzes ausführt.
detail „Detail“ auf Seite 398	Mit der Option detail können Sie, abhängig vom Befehl, mit dem sie verwendet wird, Informationen zu Verwaltungsklassen, Dateibereichen, Sicherungen und Archivierungen auflisten.
diffsnapshot „Diffsnapshot“ auf Seite 400	Verwenden Sie die Option diffsnapshot, um zu bestimmen, ob der Client eine Differenzmomentaufnahme erstellt.

Tabelle 58. Verarbeitungsoptionen für Sichern und Archivieren (Forts.)

Option	Beschreibung
dirmc „Dirmc“ auf Seite 402	Gibt die Verwaltungsklasse an, die für Verzeichnisse verwendet werden soll. Wenn Sie diese Option nicht angeben, verwendet der Client die Verwaltungsklasse in der aktiven Maßnahmengruppe Ihrer Maßnahmendomäne mit dem längsten Aufbewahrungszeitraum.
dirsonly „Dirsonly“ auf Seite 403	Nur Verzeichnisse sichern, zurückschreiben, archivieren, abrufen oder abfragen.
diskcachelocation „Diskcachelocation“ auf Seite 405	Gibt die Position an, an der die Plattencachedatenbank erstellt wird, wenn die Option <code>memoryefficient=diskcachemethod</code> bei einer Teilsicherung definiert ist.
domain „Domain“ auf Seite 407	Gibt die Dateisysteme an, die für eine Teilsicherung in Ihre Standardclientdomäne aufgenommen werden sollen.
domain.image „Domain.image“ auf Seite 412	Gibt die angehängten Dateisysteme und unformatierten logischen Datenträger an, die Sie für eine Imagesicherung in Ihre Clientdomäne einbeziehen wollen. Diese Option gilt nur für AIX, Linux x86_64, Linux on POWER und Solaris.
domain.nas „Domain.nas“ auf Seite 413	Gibt die Datenträger an, die für NAS-Imagesicherungen in Ihre Standarddomäne einbezogen werden sollen.
domain.vmfull „Domain.vmfull“ auf Seite 414	Gibt die virtuellen Maschinen an, die bei vollständigen Imagesicherungen für virtuelle VMware-Maschinen berücksichtigt werden sollen.
efsdecrypt „Efsdecrypt“ auf Seite 424	Gibt an, ob Dateien, die von einem AIX Encrypted File System (EFS) verschlüsselt werden, in verschlüsseltem oder entschlüsseltem Format gelesen werden.
enablearchiveretentionprotection „Enablearchiveretentionprotection“ auf Seite 425	ermöglicht den Client auf einen Server zu einem Datenaufbewahrungsserver herzustellen.
enablelanfree „Enablelanfree“ auf Seite 429	Gibt an, ob ein verfügbarer LAN-unabhängiger Pfad zu einer an ein Speicherbereichsnetz (SAN) angeschlossenen Speichereinheit aktiviert werden soll.
„Exclude-Optionen“ auf Seite 438 exclude exclude.backup exclude.file exclude.file.backup	Mit diesen Optionen können Sie eine Datei oder Dateigruppe von den Sicherungsservices und von den Speicherverwaltungsservices (wenn der HSM-Client installiert ist) ausschließen. Die Option <code>exclude.backup</code> schließt Dateien nur von der normalen Sicherung aus, nicht von HSM.

Tabelle 58. Verarbeitungsoptionen für Sichern und Archivieren (Forts.)

Option	Beschreibung
encryptiontype „Encryptiontype“ auf Seite 431	Wählen Sie die 256-Bit-AES- oder 128-Bit-AES-Datenverschlüsselung aus. Die 256-Bit-AES-Datenverschlüsselung bietet die stärkste Datenverschlüsselung.
encryptkey „Encryptkey“ auf Seite 431	Gibt an, ob das Kennwort für den Verschlüsselungsschlüssel lokal gesichert werden soll, wenn der Client eine Operation Sichern/Archivieren ausführt, oder ob der Benutzer zur Eingabe des Kennworts für den Verschlüsselungsschlüssel aufgefordert werden soll.
exclude.archive „Exclude-Optionen“ auf Seite 438	Schließt eine dem Muster entsprechende Datei oder Dateigruppe nur von den Archivierungsservices aus.
exclude.attribute.symlink „Exclude-Optionen“ auf Seite 438	Schließt eine Datei oder Dateigruppe, bei denen es sich um symbolische Verbindungen oder Aliasnamen handelt (Aliasnamen gelten für Mac OS X), nur von der Sicherungsverarbeitung aus.
exclude.compression „Exclude-Optionen“ auf Seite 438	Schließt Dateien von der Komprimierungsverarbeitung aus, wenn die Option <code>compression</code> auf <i>yes</i> gesetzt ist. Diese Option gilt für Sicherungen und Archivierungen.
exclude.dir „Exclude-Optionen“ auf Seite 438	Schließt ein Verzeichnis, seine Dateien sowie alle zugehörigen Unterverzeichnisse und ihre Dateien von der Sicherungsverarbeitung aus.
exclude.encrypt „Exclude-Optionen“ auf Seite 438	Schließt die angegebenen Dateien von der Verschlüsselungsverarbeitung aus.
exclude.fs „Exclude-Optionen“ auf Seite 438	Schließt Dateibereiche aus, die mit einem Muster übereinstimmen. Diese Option ist für alle UNIX-Clients gültig.
exclude.fs.nas „Exclude-Optionen“ auf Seite 438	Bei Verwendung im Befehl backup nas werden Dateisysteme auf dem NAS-Dateiserver von der Imagesicherung ausgeschlossen. Diese Option ist nur für AIX- und Solaris-Clients gültig.
exclude.image „Exclude-Optionen“ auf Seite 438	Schließt angehängte Dateisysteme und unformatierte logische Datenträger, die dem angegebenen Muster entsprechen, von den Imagegesamtsicherungsoperationen aus. Diese Option ist nur für AIX-, Solaris- und alle Linux-Clients gültig.
fbbranch „Fbbranch“ auf Seite 446	Gibt die Filialen-ID des fernen FastBack-Servers an, der gesichert oder archiviert werden soll.
fbclientname „Fbclientname“ auf Seite 447	Gibt den Namen eines oder mehrerer FastBack-Clients an, die vom Sicherungsproxy gesichert werden sollen.

Tabelle 58. Verarbeitungsoptionen für Sichern und Archivieren (Forts.)

Option	Beschreibung
fbpolicyname „Fbpolicyname“ auf Seite 448	Gibt den Namen einer oder mehrerer Tivoli Storage Manager FastBack-Maßnahmen an, die vom Sicherungsproxy gesichert werden sollen.
fbreposlocation „Fbreposlocation“ auf Seite 449	Gibt die Position des Tivoli Storage Manager FastBack-Repositorys an, zu dem der IBM Spectrum Protect-Client-Proxy die Verbindung herstellt, um die Befehle MOUNT DUMP , MOUNT ADD und MOUNT DEL auszugeben.
fbserver „Fbserver“ auf Seite 451	Gibt den Hostnamen der FastBack-Server-Workstation oder der FastBack Disaster Recovery Hub-Workstation an, die Eigner des durch die Option fbreposlocation angegebenen Repositorys ist.
fbvolumename „Fbvolumename“ auf Seite 452	Gibt den Namen eines oder mehrerer Tivoli Storage Manager FastBack-Datenträger an, die vom Sicherungs-Proxy gesichert werden sollen.
filelist „Filelist“ auf Seite 453	Gibt eine Liste von Dateien an, die für den Befehl verarbeitet werden sollen. Der Client öffnet die angegebene Dateiliste und verarbeitet die darin aufgelisteten Dateien gemäß dem Befehl.
filesonly „Filesonly“ auf Seite 457	Nur Dateien sichern, zurückschreiben, abrufen oder abfragen.
groupname „Groupname“ auf Seite 464	Verwenden Sie diese Option im Befehl backup group , um den vollständig qualifizierten Namen des Hauptmembers einer Gruppe anzugeben.
ieobjtype „Ieobjtype“ auf Seite 467	Gibt einen Objekttyp für eine Operation für clientseitige Datendeduplizierung an. Diese Option wird mit den Optionen include.dedup und exclude.dedup verwendet.
imagegapsize „Imagegapsize“ auf Seite 469	Gibt die Mindestgröße der leeren Bereiche auf einem Datenträger an, die Sie während der Sicherung überspringen wollen. Diese Option ist für AIX JFS2-Clients gültig.
incl excl „Incl excl“ auf Seite 471	Gibt den Pfad und den Dateinamen einer Einschluss-/Ausschlussoptionsdatei an.
„Include-Optionen“ auf Seite 473 include include.backup include.file include.archive „Include-Optionen“ auf Seite 473	Mit diesen Optionen können Sie Dateien einschließen oder Verwaltungsklassen für die Sicherungsverarbeitung zuordnen. Schließt Dateien für die Archivierungsverarbeitung ein oder ordnet Verwaltungsklassen zu.

Tabelle 58. Verarbeitungsoptionen für Sichern und Archivieren (Forts.)

Option	Beschreibung
<code>include.attribute.symlink</code> „Include-Optionen“ auf Seite 473	Schließt eine Datei oder Dateigruppe, bei denen es sich um symbolische Verbindungen oder Aliasnamen handelt (Aliasnamen gelten für Mac OS X), innerhalb einer größeren Gruppe von ausgeschlossenen Dateien nur bei der Sicherungsverarbeitung ein.
<code>include.compression</code> „Include-Optionen“ auf Seite 473	Schließt Dateien für die Komprimierungsverarbeitung ein, wenn Sie die Option <code>compression</code> auf <i>yes</i> setzen. Diese Option gilt für Sicherungen und Archivierungen.
<code>include.encrypt</code> „Include-Optionen“ auf Seite 473	Schließt die angegebenen Dateien in die Verschlüsselungsverarbeitung ein. Standardmäßig führt der Client keine Verschlüsselungsverarbeitung durch.
<code>include.fs</code> „Include-Optionen“ auf Seite 473	Mit der Option <code>include.fs</code> können Sie steuern, wie der Client Ihren Dateibereich für die Teilsicherung verarbeitet.
<code>include.fs.nas</code> „Include-Optionen“ auf Seite 473	Verwenden Sie die Option <code>include.fs.nas</code> , um eine Verwaltungsklasse an NAS-Dateisysteme zu binden. Sie können auch angeben, ob der Client während einer Imagesicherung des NAS-Dateisystems Inhaltsverzeichnisinformationen (TOC-Informationen) speichert. Verwenden Sie dazu die Option <code>toc</code> mit der Option <code>include.fs.nas</code> in Ihrer Datei <code>dsm.sys</code> . Weitere Informationen finden Sie in „Toc“ auf Seite 619. Diese Option ist nur für AIX- und Solaris-Clients gültig.
<code>include.image</code> „Include-Optionen“ auf Seite 473	Gibt ein Dateisystem oder einen logischen Datenträger an, das/der für die Verarbeitung der Imagesicherung eingeschlossen werden soll. Diese Option stellt außerdem einen Weg zur Verfügung, um eine explizite Verwaltungsklassenzuordnung für ein angegebenes Dateisystem oder einen logischen Datenträger anzugeben. Der Befehl <code>'backup image'</code> ignoriert alle anderen Einschlussoptionen. Diese Option ist für AIX-, Solaris- und alle Linux-Clients gültig.
<code>incrbydate</code> „Incrbydate“ auf Seite 490	Verwenden Sie diese Option im Befehl incremental , um eine Teilsicherung nach Datum anzufordern.

Tabelle 58. Verarbeitungsoptionen für Sichern und Archivieren (Forts.)

Option	Beschreibung
incremental „Incremental“ auf Seite 492	Verwenden Sie diese Option im Befehl restore image , um sicherzustellen, dass Änderungen des Basisimage auch auf das zurückgeschriebene Image angewendet werden. Diese Option ist für AIX-, Solaris- und alle Linux-Clients gültig.
memoryefficientbackup „Memoryefficientbackup“ auf Seite 507	Ein Speicher sparenden Sicherungsalgorithmus für Teilsicherungen an, wenn diese Option im Befehl incremental verwendet wird.
mode „Mode“ auf Seite 509	<p>Die Option mode ist in den folgenden Befehlen wie folgt zu verwenden:</p> <p>backup image Angaben, ob eine selektive Imagesicherung oder eine Imageteilsicherung von Clientdateisystemen ausgeführt werden soll.</p> <p>backup nas Angaben, ob eine vollständige oder eine differenzielle Imagesicherung von NAS-Dateisystemen ausgeführt werden soll.</p> <p>backup group Angaben, ob eine vollständige oder differenzielle Gruppensicherung einer Liste von Dateien ausgeführt werden soll, die sich in einem oder mehreren Dateibereichen befinden.</p> <p>backup vm Angaben, ob eine selektive Sicherung oder eine Teilsicherung von VMware-Systemen ausgeführt werden soll.</p>
monitor „Monitor“ auf Seite 512	Gibt an, ob Sie eine Imagesicherung von Dateisystemen, die zu einem NAS-Dateiserver gehören, überwachen wollen.
noprompt „Noprompt“ auf Seite 519	Unterdrückt die Bestätigungsaufforderung, die von den Befehlen delete group , delete archive , expire und set event angezeigt wird.
noprompt „Noprompt“ auf Seite 519	Unterdrückt die Bestätigungsaufforderung, die von den Befehlen delete group , delete archive , expire , restore image und set event angezeigt wird.

Tabelle 58. Verarbeitungsoptionen für Sichern und Archivieren (Forts.)

Option	Beschreibung
nojournal „Nojournal“ auf Seite 519	Verwenden Sie diese Option im Befehl incremental , um anzugeben, dass statt der standardmäßigen urnalgestützten Sicherung die traditionelle vollständige Teilsicherung ausgeführt werden soll.
optfile „Optfile“ auf Seite 523	Gibt die Clientbenutzeroptionsdatei an, die Sie verwenden wollen, wenn Sie eine Sitzung des Clients für Sichern/ Archivieren starten.
postsnapshotcmd „Postsnapshotcmd“ auf Seite 533	Während einer momentaufnahmebasierten Sicherung können Sie mit dieser Option eine Anwendung manuell öffnen, nachdem die Momentaufnahme erstellt wurde. Diese Option ist nur für momentaufnahmebasierte AIX-JFS2- oder Linux-LVM-Operationen gültig.
preservelastaccessdate „Preservelastaccessdate“ auf Seite 536	Verwenden Sie diese Option während einer Sicherungs- oder Archivierungsoperation, um anzugeben, ob das Datum des letzten Zugriffs auf angegebene Dateien nach einer Sicherungs- oder Archivierungsoperation auf seinen ursprünglichen Wert zurückgesetzt werden soll. Standardmäßig setzt der Client das Datum des letzten Zugriffs auf gesicherte oder archivierte Dateien nicht auf den ursprünglichen Wert vor der Sicherungs- oder Archivierungsoperation zurück.
presnapshotcmd „Presnapshotcmd“ auf Seite 540	Während einer momentaufnahmebasierten Sicherung können Sie mit dieser Option eine Anwendung manuell in den Wartemodus versetzen, bevor die Momentaufnahme erstellt wird. Diese Option ist nur für momentaufnahmebasierte AIX-JFS2- oder Linux-LVM-Operationen gültig.
removeoperandlimit „Removeoperandlimit“ auf Seite 544	Gibt an, dass der Client die Beschränkung auf 20 Operanden entfernt. Wenn Sie die Option removeoperandlimit mit dem Befehl incremental , selective , archive oder backup image angeben, wird die Beschränkung auf 20 Operanden nicht umgesetzt und nur durch die verfügbaren Ressourcen oder andere Begrenzungen des Betriebssystems eingeschränkt.
skipacl „Skipacl“ auf Seite 580	Gibt an, ob die ACL-Verarbeitung vollständig übersprungen werden soll.

Tabelle 58. Verarbeitungsoptionen für Sichern und Archivieren (Forts.)

Option	Beschreibung
skipaclupdatecheck „Skipaclupdatecheck“ auf Seite 581	Gibt an, ob Kontrollsummen- und Größenvergleiche vor und nach einer Sicherung und während einer Teilsicherung ausgeführt werden sollen.
snapdiff „Snapdiff“ auf Seite 581	Gibt eine Teilsicherung der Dateien an, die von NetApp als geändert aufgelistet wurden, anstatt den Datenträger auf Dateien zu untersuchen, die sich geändert haben. Verwenden Sie diese Option bei der Teilsicherung von vollständigen NAS-Datenträgern.
snapshotcachesize „Snapshotcachesize“ auf Seite 590	Nur für Linux und AIX: Verwenden Sie diese Option, um eine entsprechende Momentaufnahmengröße anzugeben, damit alle ursprünglichen Datenblöcke während der Dateiänderung und -löschung gespeichert werden können. Eine Momentaufnahmengröße von 100 Prozent gewährleistet eine gültige Momentaufnahme. Der Standardwert ist 100 Prozent.
snapshotproviderfs „Snapshotproviderfs“ auf Seite 591	Verwenden Sie die Option snapshotproviderfs, um momentaufnahmebasierte Dateisicherungs- und Dateiarchivierungsoperationen zu aktivieren und einen Momentaufnahmeprovider anzugeben. Sie müssen Root sein, um eine momentaufnahmebasierte Dateisicherungs- oder Dateiarchivierungsoperation auszuführen. Wenn Sie kein Rootbenutzer sind, schlägt die Operation mit einer Fehlermeldung fehl.
snapshotproviderimage „Snapshotproviderimage“ auf Seite 592	Verwenden Sie die Option snapshotproviderimage, um momentaufnahmebasierte Imagesicherung zu aktivieren und einen Momentaufnahmeprovider anzugeben. Sie müssen Root sein, um eine momentaufnahmebasierte Imagesicherungsoperation auszuführen. Wenn Sie kein Rootbenutzer sind, schlägt die Operation mit einer Fehlermeldung fehl.

Tabelle 58. Verarbeitungsoptionen für Sichern und Archivieren (Forts.)

Option	Beschreibung
snapshotroot „Snapshotroot“ auf Seite 593	Verwenden Sie die Option snapshotroot im Befehl incremental , selective oder archive mit einer Anwendung eines unabhängigen Softwareanbieters, die eine Momentaufnahme eines logischen Datenträgers bereitstellt, um die Daten der lokalen Momentaufnahme den realen Dateibereichsdaten zuzuordnen, die auf dem IBM Spectrum Protect-Server gespeichert sind. Diese Option ist für alle UNIX- und Linux-Clients gültig.
subdir „Subdir“ auf Seite 605	Gibt an, ob Unterverzeichnisse eines benannten Verzeichnisses eingeschlossen werden sollen.
tapeprompt „Tapeprompt“ auf Seite 607	Gibt an, ob der Client auf einen Bandladevorgang, der für einen Sicherungs-, Archivierungs-, Zurückschreibungs- oder Abrufprozess erforderlich ist, warten soll, oder ob eine Bedienerführung für die Auswahl angezeigt werden soll.
toc „Toc“ auf Seite 619	Verwenden Sie die Option toc mit dem Befehl backup nas oder der Option <code>include.fs.nas</code> , um anzugeben, ob der Client für jede Dateisystemsicherung Inhaltsverzeichnisinformationen (TOC-Informationen) speichert. Wenn Sie TOC-Informationen speichern, können Sie den Serverbefehl QUERY TOC verwenden, um den Inhalt einer Dateisystemsicherung zu bestimmen, sowie den Serverbefehl RESTORE NODE, um einzelne Dateien oder Verzeichnisstrukturen zurückzuschreiben. Sie können auch den Web-Client verwenden, um die gesamte Baumstruktur des Dateisystems zu untersuchen und zurückzuschreibende Dateien und Verzeichnisse auszuwählen.
type „Type“ auf Seite 624	Verwenden Sie die Option type im Befehl query node , um den Typ des abzufragenden Knotens anzugeben.
v2archive „V2archive“ auf Seite 627	Verwenden Sie die Option v2archive im Befehl archive , um anzugeben, dass nur Dateien auf dem Server archiviert werden sollen. Der Client verarbeitet keine Verzeichnisse, die in dem Pfad der Quelldateispezifikation vorhanden sind.
virtualfsname „Virtualfsname“ auf Seite 630 (gilt nicht für Mac OS X)	Verwenden Sie diese Option im Befehl backup group , um den Namen des Containers für die Gruppe anzugeben, mit der die Operation ausgeführt werden soll.

Tabelle 58. Verarbeitungsoptionen für Sichern und Archivieren (Forts.)

Option	Beschreibung
virtualmountpoint „Virtualmountpoint“ auf Seite 636	Definiert einen virtuellen Mountpunkt für ein Dateisystem, wenn Dateien für die Sicherung berücksichtigt werden sollen, die mit einem bestimmten Verzeichnis innerhalb dieses Dateisystems beginnen.
vmchost „Vmchost“ auf Seite 637	Wird mit den Befehlen backup VM , restore VM und query VM verwendet, um den Hostnamen des VMware VirtualCenter oder des ESX-Servers anzugeben, an das/den die Befehle gerichtet sind.
vmcpw „Vmcpw“ auf Seite 638	Wird mit den Befehlen backup VM , restore VM und query VM verwendet, um das Kennwort des VirtualCenter- oder ESX-Benutzers anzugeben, das mit der Option vmcuser angegeben ist.
vmcuser „Vmcuser“ auf Seite 640	Wird mit den Befehlen backup VM , restore VM und query VM verwendet, um den Benutzernamen des VMware VirtualCenter oder des ESX-Servers anzugeben, an das/den die Befehle gerichtet sind.
vmmxvirtualdisks „Vmmxvirtualdisks“ auf Seite 658	Wird mit dem Befehl backup VM verwendet, um die maximale Größe von Platten virtueller VMware-Maschinen (VMDKs) anzugeben, die in eine Sicherungsoperation eingeschlossen werden sollen.
vmskipmaxvirtualdisks „Vmskipmaxvirtualdisks“ auf Seite 666	Wird mit dem Befehl backup VM verwendet, um anzugeben, wie die Sicherungsoperation Platten virtueller VMware-Maschinen (VMDKs) verarbeitet, die die maximale Plattengröße überschreiten. In Version 7.1.3 und früheren Versionen hatte die Option vmskipmaxvirtualdisks den Namen vmskipmaxvmdks.

Verarbeitungsoptionen für Zurückschreiben und Abrufen

Sie können Clientoptionen zur Steuerung einiger Aspekte der Zurückschreibungs- und Abrufverarbeitung verwenden.

In Tabelle 59 sind die verfügbaren Verarbeitungsoptionen für Zurückschreiben und Abrufen aufgelistet.

Tabelle 59. Verarbeitungsoptionen für Zurückschreiben und Abrufen

Option	Beschreibung
dirsonly „Dirsonly“ auf Seite 403	Qualifiziert die Operation (Sichern, Archivieren, Zurückschreiben, Abrufen), sodass nur Verzeichnisse verarbeitet werden.

Tabelle 59. Verarbeitungsoptionen für Zurückschreiben und Abrufen (Forts.)

Option	Beschreibung
disablenqr „Disablenqr“ auf Seite 404	Gibt an, ob der Client für Sichern/Archivieren die Methode zur Zurückschreibung ohne Abfrage verwenden kann, um Dateien und Verzeichnisse vom Server zurückzuschreiben.
filelist „Filelist“ auf Seite 453	Gibt eine Datei an, die eine Liste der Dateien enthält, die von dem angegebenen Befehl verarbeitet werden sollen.
filesonly „Filesonly“ auf Seite 457	Qualifiziert die Operation (Sichern, Archivieren, Zurückschreiben, Abrufen), sodass nur Dateien verarbeitet werden.
followsymbolic „Followsymbolic“ auf Seite 458	Gibt an, ob Dateien in symbolische Verbindungen zurückgeschrieben werden sollen oder ob eine symbolische Verbindung als virtueller Mountpunkt verwendet werden soll.
fromdate „Fromdate“ auf Seite 461	Mit der Option fromdate können Sie in Verbindung mit der Option fromtime ein Datum mit Uhrzeit angeben, ab dem Sie während einer Zurückschreibungs-, Abruf- oder Abfrageoperation nach Sicherungen oder Archivierungen suchen wollen.
fromnode „Fromnode“ auf Seite 461	Ermöglicht, dass ein Knoten Befehle für einen anderen Knoten ausführen kann. Ein Benutzer auf einem anderen Knoten muss Ihnen mit dem Befehl set access die Berechtigung zum Abfragen, Zurückschreiben oder Abrufen von Dateien oder Images für diesen anderen Knoten erteilen.
fromowner „Fromowner“ auf Seite 462	Dateibereiche für einen alternativen Eigner anzeigen. Außerdem einen alternativen Eigner angeben, von dem Dateien zurückgeschrieben oder abgerufen werden sollen.
fromtime „Fromtime“ auf Seite 463	Mit der Option fromtime können Sie in Verbindung mit der Option fromdate eine Anfangszeit angeben, ab der Sie während einer Zurückschreibungs-, Abruf- oder Abfrageoperation nach Sicherungen oder Archivierungen suchen wollen.
ifnewer „Ifnewer“ auf Seite 468	Ersetzt eine vorhandene Datei nur dann durch die neueste Sicherungsversion, wenn die Sicherungsversion aktueller als die vorhandene Datei ist.
imagetofile „Imagetofile“ auf Seite 470	Verwenden Sie die Option imagetofile im Befehl restore image , um anzugeben, dass Sie das Quellenimage in eine Datei zurückschreiben wollen. Es kann erforderlich sein, das Image in eine Datei zurückzuschreiben, wenn der Zieldatenträger defekte Sektoren enthält oder die Imagedaten bearbeitet werden sollen. Diese Option ist für AIX-, Linux- und Solaris-Clients gültig.
inactive „Inactive“ auf Seite 471	Zeigt bei Verwendung mit der Option pick eine Liste aktiver und inaktiver Dateien an.
latest „Latest“ auf Seite 499	Die letzte Sicherungsversion einer Datei zurückschreiben, unabhängig davon, ob sie aktiv oder inaktiv ist.

Tabelle 59. Verarbeitungsoptionen für Zurückschreiben und Abrufen (Forts.)

Option	Beschreibung
localbackupset „Localbackupset“ auf Seite 500	Gibt an, ob die GUI des Clients für Sichern/Archivieren die anfängliche Anmeldung am Server umgeht, um einen lokalen Sicherungssatz auf einer eigenständigen Workstation zurückzuschreiben.
makesparsefile „Makesparsefile“ auf Seite 501 (gilt nicht für Mac OS X)	Verwenden Sie die Option makesparsefile im Befehl restore oder retrieve , um anzugeben, wie Dateien mit freien Bereichen erneut erstellt werden.
monitor „Monitor“ auf Seite 512	Gibt an, ob Sie eine Imagezurückschreibung eines oder mehrerer zu einem NAS-Dateiserver gehörenden Dateisysteme überwachen wollen.
noprompt „Noprompt“ auf Seite 519	Unterdrückt die Bestätigungsaufforderung, die von den Befehlen delete group , delete archive , expire und set event angezeigt wird.
noprompt „Noprompt“ auf Seite 519	Unterdrückt die Bestätigungsaufforderung, die von den Befehlen delete group , delete archive , expire , restore image und set event angezeigt wird.
optfile „Optfile“ auf Seite 523	Gibt die Clientbenutzeroptionsdatei an, die Sie verwenden wollen, wenn Sie eine Sitzung des Clients für Sichern/Archivieren starten.
pick „Pick“ auf Seite 528	Erstellt eine Liste der Sicherungsversionen, Images oder Archivierungskopien, die der eingegebenen Dateispezifikation entsprechen. Aus der Liste können die zu verarbeitenden Versionen ausgewählt werden. Fügen Sie die Option inactive ein, um sowohl aktive als auch inaktive Objekte anzuzeigen.
pitdate „Pitdate“ auf Seite 529	Sie können mit der Option pitdate in Verbindung mit der Option pittime einen Zeitpunkt definieren, für den die aktuellsten Sicherungsversionen angezeigt oder zurückgeschrieben werden sollen.
pittime „Pittime“ auf Seite 530	Sie können mit der Option pittime in Verbindung mit der Option pitdate einen Zeitpunkt definieren, für den die aktuellsten Sicherungsversionen angezeigt oder zurückgeschrieben werden sollen.
preservepath „Preservepath“ auf Seite 537	Gibt an, wie viel vom Quellenpfad als Teil des Zielverzeichnispfades wiederherzustellen ist, wenn Dateien an eine neue Position zurückgeschrieben oder abgerufen werden.
replace „Replace“ auf Seite 547	Gibt an, ob eine vorhandene Datei überschrieben werden soll oder ob Sie zur Eingabe Ihrer Auswahl aufgefordert werden sollen, wenn Sie Dateien zurückschreiben oder abrufen.
showmembers „Showmembers“ auf Seite 579 (gilt nicht für Mac OS X)	Zeigt alle Member einer Gruppe an.
subdir „Subdir“ auf Seite 605	Gibt an, ob Sie Unterverzeichnisse eines benannten Verzeichnisses einschließen wollen.
tapeprompt „Tapeprompt“ auf Seite 607	Gibt an, ob der Client für Sichern/Archivieren auf das Laden eines für eine Zurückschreibung oder einen Abruf erforderlichen Bands warten soll oder ob Sie zur Eingabe Ihrer Auswahl aufgefordert werden sollen.

Tabelle 59. Verarbeitungsoptionen für Zurückschreiben und Abrufen (Forts.)

Option	Beschreibung
todate „Todate“ auf Seite 621	Mit der Option todate können Sie in Verbindung mit der Option totime ein Enddatum mit einer Endzeit angeben, bis zu dem Sie während einer Zurückschreibungs-, Abruf- oder Abfrageoperation nach Sicherungen oder Archivierungen suchen wollen.
totime „Totime“ auf Seite 622	Mit der Option totime können Sie in Verbindung mit der Option todate ein Enddatum und eine Endzeit angeben, bis zu der Sie während einer Zurückschreibungs-, Abruf- oder Abfrageoperation nach Sicherungen oder Archivierungen suchen wollen.
type „Type“ auf Seite 624	Verwenden Sie die Option type im Befehl query node , um den Typ des abzufragenden Knotens anzugeben.
verifyimage „Verifyimage“ auf Seite 629	Verwenden Sie die Option verifyimage im Befehl restore image , um anzugeben, dass die Feststellung von defekten Sektoren auf dem Zieldatenträger aktiviert werden soll. Werden defekte Sektoren auf dem Zieldatenträger festgestellt, gibt der Client eine Warnung auf der Konsole und im Fehlerprotokoll aus.

Die folgenden Optionen sind Optionen des Clients für Sichern/Archivieren, die für umgelagerte Dateien von IBM Spectrum Protect HSM for Windows gelten. Weitere Informationen zu diesen Optionen finden Sie in den Abschnitten des IBM Knowledge Center unter http://www.ibm.com/support/knowledgecenter/SSERFH_8.1.6/hsmwin/welcome.html.

- Checkreparsecontent
- Restorecheckstubaccess
- Restoremigstate
- Skipmigrated

Die folgenden Optionen sind Optionen des Clients für Sichern/Archivieren, die für umgelagerte Dateien von IBM Spectrum Protect for Space Management gelten. Weitere Informationen zu diesen Optionen finden Sie in den Abschnitten des IBM Knowledge Center unter http://www.ibm.com/support/knowledgecenter/SSERBH_8.1.6/hsmul/welcome.html.

- Restoremigstate
- Skipmigrated

Planungsoptionen

In diesem Abschnitt sind die Optionen beschrieben, die Sie zum Steuern der zentralen Zeitplanung verwenden können. Der Client für Sichern/Archivieren verwendet Planungsoptionen nur, wenn der Scheduler aktiv ist.

In Tabelle 60 auf Seite 341 sind die verfügbaren Planungsoptionen aufgelistet.

Tabelle 60. Planungsoptionen

Option	Beschreibung
cadlistenonport „Cadlistenonport“ auf Seite 372	Gibt an, ob Empfangsport für den Clientakzeptor geöffnet werden sollen, wenn der Clientakzeptor zum Verwalten von Zeitplänen im Abfragemodus verwendet wird.
managedservices „Managedservices“ auf Seite 502	Gibt an, ob der Clientakzeptor den Web-Client und/oder den Scheduler verwaltet.
maxcmdretries „Maxcmdretries“ auf Seite 504	Gibt an, wie oft der Client-Scheduler einen geplanten Befehl, der bei der Ausführung fehlgeschlagen ist, maximal zu wiederholen versucht.
postschedulecmd/postnschedulecmd „Postschedulecmd/Postnschedulecmd“ auf Seite 531	Gibt einen Befehl an, der nach Ausführung eines Zeitplans verarbeitet werden soll.
preschedulecmd/preschedulecmd „Preschedulecmd/Preschedulecmd“ auf Seite 534	Gibt einen Befehl an, der vor Ausführung eines Zeitplans verarbeitet werden soll.
querschedperiod „Querschedperiod“ auf Seite 541	Gibt die Anzahl Stunden an, die der Client-Scheduler zwischen den Versuchen, geplante Arbeit auf dem Server abzufragen, wartet.
retryperiod „Retryperiod“ auf Seite 560	Gibt die Anzahl Minuten an, die der Client-Scheduler zwischen den Versuchen, einen geplanten Befehl, der fehlgeschlagen ist, zu verarbeiten oder zwischen fehlgeschlagenen Versuchen, Ergebnisse an den Server zu melden, wartet.
schedcmddisabled „Schedcmddisabled“ auf Seite 562	Gibt an, ob die Zeitplanung generischer Befehle, die von Ihrem IBM Spectrum Protect-Administrator angegeben werden, inaktiviert werden soll.
schedcmduser (nur serverdefiniert) „Zeitplanungsoptionen für Befehle“ auf Seite 302	Der Scheduler führt Befehle unter der UID 0 aus; es kann jedoch einige Benutzer geben, die eine andere Benutzer-ID haben. In diesem Fall kann Ihr IBM Spectrum Protect-Administrator mithilfe dieser Option Zeitpläne definieren und zulassen, dass diese Zeitpläne unter einer anderen UID als 0 ausgeführt werden. Die IBM Spectrum Protect-Client-API unterstützt diese Option nicht.
schedlogmax „Schedlogmax“ auf Seite 565	Gibt die maximale Größe des Planungsprotokolls und des Web-Client-Protokolls in Megabyte an.
schedlogname „Schedlogname“ auf Seite 567	Gibt den Pfad und den Namen der Datei an, in der die Planungsprotokolldaten gespeichert werden sollen.
schedlogretention „Schedlogretention“ auf Seite 568	Gibt die Anzahl Tage an, die Einträge im Planungsprotokoll und im Web-Client-Protokoll aufbewahrt werden sollen, und gibt an, ob bereinigte Einträge gesichert werden sollen.

Tabelle 60. Planungsoptionen (Forts.)

Option	Beschreibung
schedmode „Schedmode“ auf Seite 570	Gibt an, welcher Planungsmodus verwendet werden soll, Ausführung bei Clientsendeaufruf (<i>polling</i>) oder servergesteuerte Ausführung (<i>prompted</i>).
schedrestretrdisabled „Schedrestretrdisabled“ auf Seite 572	Gibt an, ob verhindert werden soll, dass der IBM Spectrum Protect-Serveradministrator Planungsoperationen für Zurückschreibung oder Abruf ausführt.
sessioninitiation „Sessioninitiation“ auf Seite 576	Verwenden Sie die Option sessioninitiation, um zu steuern, ob der Server oder der Client Sitzungen durch eine Firewall einleiten soll. Standardwert ist, dass der Client Sitzungen einleiten kann.
srvprepostscheddisabled „Srvprepostscheddisabled“ auf Seite 596	Gibt an, ob verhindert werden soll, dass der IBM Spectrum Protect-Serveradministrator bei der Ausführung geplanter Operationen Befehle vor und nach dem Zeitplan ausführt.
srvprepostsnapdisabled „Srvprepostsnapdisabled“ auf Seite 597	Gibt an, ob verhindert werden soll, dass der IBM Spectrum Protect-Serveradministrator bei der Ausführung geplanter Operationen für Image-Momentaufnahmesicherungen Befehle vor und nach der Momentaufnahme ausführt.
tcpclientaddress „Tcpclientaddress“ auf Seite 611	Gibt eine TCP/IP-Adresse an, wenn Ihr Clientknoten über mehrere Adressen verfügt und der Server eine Verbindung zu einer anderen Adresse herstellen soll als der, mit der die erste Verbindung zum Server hergestellt wurde. Der Server verwendet diese Adresse, wenn er die Operation mit Zeitplanung über Serversystemanfrage beginnt. Details siehe schedmode <i>prompted</i> („Schedmode“ auf Seite 570).
tcpclientport „Tcpclientport“ auf Seite 612	Gibt eine TCP/IP-Anschlussnummer für den Server an, mit der eine Verbindung zum Client hergestellt wird, wenn der Server die Operation mit Zeitplanung über Serversystemanfrage beginnt. Details siehe schedmode <i>prompted</i> („Schedmode“ auf Seite 570).

Optionen für Format und Sprache

Mit Optionen für Format und Sprache können Sie unterschiedliche Datums-, Uhrzeit- und Zahlenformate für verschiedene Sprachen auswählen.

Mit Formatoptionen können Sie unterschiedliche Formate für Datum, Uhrzeit und Zahlen auswählen.

Tabelle 61. Optionen für Format und Sprache

Option	Beschreibung
dateformat „Dateformat“ auf Seite 389	Gibt das Format für das Anzeigen von Datumsangaben an.

Tabelle 61. Optionen für Format und Sprache (Forts.)

Option	Beschreibung
numberformat „Numberformat“ auf Seite 521	Gibt das Format für das Anzeigen von Zahlen an.
timeformat „Timeformat“ auf Seite 616	Gibt das Format für das Anzeigen von Zeitangaben an.

Befehlsverarbeitungsoptionen

In diesem Abschnitt sind die Optionen beschrieben, die Sie mit den Befehlen des Clients für Sichern/Archivieren verwenden können.

Mit Optionen zur Befehlsverarbeitung können Sie einige Aspekte der Formatierung der Daten auf Ihrer Terminalanzeige steuern.

Tabelle 62. Befehlsverarbeitungsoptionen

Option	Beschreibung
quiet „Quiet“ auf Seite 543	Begrenzt die Anzahl der Nachrichten, die während der Verarbeitung auf dem Bildschirm angezeigt werden. Diese Option kann vom Server überschrieben werden.
scrolllines „Scrolllines“ auf Seite 572	Gibt die Anzahl Datenzeilen an, die gleichzeitig auf dem Bildschirm angezeigt werden. Verwenden Sie diese Option nur, wenn scrollprompt auf <i>yes</i> gesetzt ist.
scrollprompt „Scrollprompt“ auf Seite 573	Gibt an, ob der Client für Sichern/Archivieren nach dem Anzeigen der Anzahl Datenzeilen, die Sie mit der Option scrolllines angegeben haben, stoppen und warten soll, oder ob durch alle Zeilen geblättert und am Ende der Datenliste gestoppt werden soll.
setwindowtitle „Setwindowtitle“ auf Seite 578	Gibt an, ob der IBM Spectrum Protect-Servername und der Host-Server-Name im Titel des Befehlsfensters für den Verwaltungsclient angezeigt werden sollen.
verbose „Verbose“ auf Seite 628	Gibt an, dass Verarbeitungsdaten auf Ihrem Bildschirm angezeigt werden sollen. Die Alternative dazu ist quiet. Diese Option kann vom Server überschrieben werden.

Berechtigungsoptionen

Über Berechtigungsoptionen wird der Zugriff auf den IBM Spectrum Protect-Server gesteuert.

In Tabelle 63 sind die verfügbaren Berechtigungsoptionen aufgelistet.

Tabelle 63. Berechtigungsoptionen

Option	Beschreibung
autodeploy „Autodeploy“ auf Seite 365	Gibt an, ob Sie eine automatische Implementierung des Clients aktivieren oder inaktivieren wollen, wenn ein Neustart erforderlich ist.
groups „Groups (veraltet)“ auf Seite 464	Gibt die Gruppen auf Ihrer Workstation an, die Sie berechtigen wollen, IBM Spectrum Protect-Services vom Server anzufordern.
password „Password“ auf Seite 524	Gibt das IBM Spectrum Protect-Kennwort an.

Tabelle 63. Berechtigungsoptionen (Forts.)

Option	Beschreibung
passwordaccess „Passwordaccess“ auf Seite 525	Gibt an, ob Sie bei jedem Start des Clients ein generiertes Kennwort verwenden oder ein Kennwort eingeben wollen.
passworddir „Passworddir“ auf Seite 527	Gibt das Verzeichnis an, in dem Sie das automatisch generierte Kennwort für Ihren Clientknoten speichern wollen. Der Verschlüsselungsschlüssel und das Kennwort werden in der Datei TSM.sth verschlüsselt und gespeichert.
revokeremoteaccess „Revokeremoteaccess“ auf Seite 561	Beschränkt den Zugriff eines Administrators mit Clientzugriffsberechtigung auf Ihre Workstation durch den Web-Client.
users „Users (veraltet)“ auf Seite 627	Erteilt bestimmten Benutzern auf Ihrer Workstation die Berechtigung zum Anfordern von Services von einem Server.

Fehlerverarbeitungsoptionen

Fehlerverarbeitungsoptionen geben den Namen der Fehlerprotokolldatei sowie die Behandlung der Einträge in der Protokolldatei durch den Client für Sichern/Archivieren an.

In Tabelle 64 sind die verfügbaren Fehlerverarbeitungsoptionen aufgelistet.

Tabelle 64. Fehlerverarbeitungsoptionen

Option	Beschreibung
errorlogmax „Errorlogmax“ auf Seite 434	Gibt die maximale Größe des Fehlerprotokolls in Megabyte an.
errorlogname „Errorlogname“ auf Seite 435	Gibt den vollständig qualifizierten Pfad und Dateinamen der Datei an, in der Informationen zu Fehlern gespeichert werden sollen, die während der Verarbeitung auftreten.
errorlogretention „Errorlogretention“ auf Seite 436	Gibt an, wie viele Tage Fehlerprotokolleinträge aufbewahrt werden sollen, bevor sie bereinigt werden, und zeigt an, ob die bereinigten Einträge gesichert werden sollen.

Transaktionsverarbeitungsoptionen

Transaktionsverarbeitungsoptionen steuern, wie Transaktionen zwischen dem IBM Spectrum Protect-Client und -Server verarbeitet werden.

In Tabelle 65 auf Seite 345 sind die verfügbaren Transaktionsverarbeitungsoptionen aufgelistet.

Tabelle 65. Transaktionsverarbeitungsoptionen

Option	Beschreibung
collocatebyfilespec „Collocatebyfilespec“ auf Seite 375	Gibt an, ob der Client für Sichern/Archivieren nur eine einzige Serversitzung verwenden soll, um Objekte zu senden, die von einer einzigen Dateispezifikation generiert wurden. Durch das Setzen der Option collocatebyfilespec auf <i>yes</i> wird das Durchsetzen von Dateien von unterschiedlichen Dateispezifikationen eliminiert, indem der Client auf eine Serversitzung pro Dateispezifikation begrenzt wird. Wenn Sie Daten auf Band speichern, werden Dateien für jede Dateispezifikation deshalb zusammen auf einem Band gespeichert (sofern auf Grund erhöhter Kapazität kein weiteres Band erforderlich ist).
commrestartduration „Commrestartduration“ auf Seite 378	Gibt die maximale Anzahl Minuten an, die der Client nach einem Übertragungsfehler versuchen soll, die Verbindung zum IBM Spectrum Protect-Server wiederherzustellen.
commrestartinterval „Commrestartinterval“ auf Seite 378	Gibt die Anzahl Sekunden an, die der Client nach einem Übertragungsfehler zwischen Versuchen, die Verbindung zum IBM Spectrum Protect-Server wiederherzustellen, warten soll.
diskbuffsize „Diskbuffsize“ auf Seite 405	Gibt die maximale Platten-E/A-Puffergröße (in Kilobyte) an, die der Client beim Lesen von Dateien verwenden kann.
largecommbuffers „Diskbuffsize“ auf Seite 405	Diese Option wurde ersetzt durch die Option diskbuffsize. Derzeit wird largecommbuffers vom Client für Sichern/Archivieren noch akzeptiert, um den Übergang zu der neuen Option zu erleichtern. Der von largecommbuffers angegebene Wert wird jedoch zugunsten der Einstellung für diskbuffsize ignoriert. Wichtig: Verwenden Sie largecommbuffers nicht mehr, da diese Option in zukünftigen Releases des Clients möglicherweise nicht akzeptiert wird.
nfstimeout „Nfstimeout“ auf Seite 516	Gibt die Wartezeit des Servers auf einen Statussystemaufruf für ein NFS-Dateisystem in Sekunden an, bevor eine Zeitlimitüberschreitung auftritt.
resourceutilization „Resourceutilization“ auf Seite 557	Mit der Option resourceutilization in Ihrer Datei dsm.sys können Sie den Umfang der Ressourcen steuern, die der IBM Spectrum Protect-Server und -Client während der Verarbeitung verwenden können.
txnbytelimit „Txnbytelimit“ auf Seite 622	Gibt die Anzahl Kilobyte an, die das Clientprogramm puffert, bevor es eine Transaktion an den Server sendet.

Web-Client-Optionen

Zum Konfigurieren des IBM Spectrum Protect-Web-Clients werden verschiedene Optionen des Clients für Sichern/Archivieren verwendet.

In Tabelle 66 sind die verfügbaren Web-Client-Optionen aufgelistet.

Tabelle 66. Web-Client-Optionen

Option	Beschreibung
httpport „Httpport“ auf Seite 465	Gibt eine TCP/IP-Anschlussadresse für den Web-Client an.
managedservices „Managedservices“ auf Seite 502	Gibt an, ob der Clientakzeptordämon den Web-Client und/oder den Scheduler verwaltet.

Tabelle 66. Web-Client-Optionen (Forts.)

Option	Beschreibung
revokeremoteaccess „Revokeremoteaccess“ auf Seite 561	Beschränkt den Administratorzugriff auf eine Workstation über den Web-Client.
webports „Webports“ auf Seite 680	Aktiviert die Verwendung des Web-Clients außerhalb einer Firewall, indem die TCP/IP-Anschlussnummer angegeben wird, die vom Clientakzeptordämon und dem Web-Client-Agentenservice für die Kommunikation mit dem Web-Client verwendet wird.

Diagnoseoptionen

Verwenden Sie den Befehl **query systeminfo**, um IBM Spectrum Protect-Systeminformationen zusammenzustellen und an der Konsole oder in einer Datei auszugeben.

Der Befehl **query systeminfo** soll hauptsächlich als Diagnosehilfe dienen. Die zusammengestellten Informationen können Sie zur Problemdiagnose an die Mitarbeiter der technischen Unterstützung weiterleiten.

In Tabelle 67 sind die verfügbaren Diagnoseoptionen aufgelistet.

Tabelle 67. Diagnoseoptionen

Option	Beschreibung
console „Console“ auf Seite 382	Verwenden Sie die Option console im Befehl query systeminfo , um die Systeminformationen an der Konsole auszugeben.
filename „Filename“ auf Seite 456	Verwenden Sie die Option filename im Befehl query systeminfo , um den Namen einer Datei anzugeben, in der die Systeminformationen gespeichert werden sollen.

Zugehörige Verweise:

„Query Systeminfo“ auf Seite 766

Optionen in Befehlen verwenden

Sie können einige der Optionen in Ihrer Clientoptionsdatei (dsm.opt) überschreiben, indem Sie sie mit den entsprechenden Befehlen des Clients für Sichern/Archivieren eingeben.

Sie können einige Optionen in Ihrer Datei dsm.sys oder Clientbenutzeroptionsdatei (dsm.opt) überschreiben, indem Sie sie mit den entsprechenden Befehlen des Clients für Sichern/Archivieren eingeben.

Der Client verarbeitet die Optionen in folgender Reihenfolge (Vorrangstellung):

1. Auf dem Server definierte Optionen mit vom Server erzwungenen Clientoptionen. Der Server überschreibt die Clientwerte.
2. Optionen, die lokal in die Befehlszeile eingegeben werden.
3. Optionen, die unter Verwendung der Optionsparameter für einen Zeitplan auf dem Server definiert werden.
4. Optionen, die lokal in die Optionsdatei eingegeben werden.

5. Vom Server empfangene Optionen mit Clientoptionsgruppen, die nicht wie vom Server erzwungen definiert werden. Der Server überschreibt die Clientwerte *nicht*, wenn dies nicht erzwungen wird.
6. Standardoptionswerte.

Der Client enthält außerdem eine Gruppe von Clientbefehlsoptionen, die Sie mit bestimmten Befehlen *nur* in der Befehlszeile eingeben können. Unter Tabelle 68 auf Seite 348 finden Sie eine vollständige Liste der Befehlszeilenoptionen, eine Beschreibung und Verweise auf weitere Informationen.

Optionen mit einem Befehl eingeben

Sie müssen die allgemeinen Regeln für die Eingabe von Optionen mit einem Befehl befolgen.

- Einen Befehl, einen Bindestrich (-), den Optionsnamen, ein Gleichheitszeichen (=) und den Optionswert oder -parameter eingeben. Auf beiden Seiten des Gleichheitszeichens (=) dürfen keine Leerzeichen sein.

Die folgenden Beispiele zeigen diese Syntax für verschiedene Clients:

```
dsmc archive -description="Jahresende 1999" /home/
```

- Bei Optionen, die über keine Parameter verfügen, müssen ein Befehl, ein Bindestrich (-) und der Optionsname eingegeben werden. Beispiel:

```
dsmc incremental -quiet
```

Anmerkung: Verwenden Sie einen führenden Bindestrich (-), um anzuzeigen, dass der folgende Text der Name einer Option ist. Wenn ein Objektname mit einem Bindestrich beginnt, müssen Sie ihn entweder in Hochkommas (') oder in Anführungszeichen (") einschließen. Die meisten Betriebssystem-Befehlszeilenprozessoren entfernen die Hochkommas bzw. Anführungszeichen, bevor die Befehlszeilenargumente an die IBM Spectrum Protect-Clientanwendung übergeben werden. In diesen Fällen müssen Sie Escapezeichen oder doppelte Hochkommas bzw. Anführungszeichen verwenden, damit der Client den Objektnamen in Hochkommas/Anführungszeichen empfangen kann. Im Schleifenmodus schließen Sie solche Objekte entweder in Hochkommas (') oder in Anführungszeichen (") ein.

- Den Optionsnamen oder eine Abkürzung des Optionsnamens eingeben. Für die Option latest kann beispielsweise -lat oder -latest angegeben werden. Die Großbuchstaben in der Optionssyntax zeigen die Mindestabkürzung für den betreffenden Optionsnamen an.
- Optionen vor oder hinter den Befehlsparametern eingeben. Sie können beispielsweise die Option subdir vor oder hinter einer Dateispezifikation eingeben:

```
dsmc selective -subdir=yes "/home/devel/proj1/*"
dsmc selective "/home/devel/proj1/*" -subdir=yes
```

- Wenn Sie mehrere Optionen in einem Befehl eingeben, müssen Sie sie durch eine Leerstelle trennen.
- Schließen Sie den Wert in Anführungszeichen (") ein, wenn der von Ihnen eingegebene Optionswert ein Leerzeichen enthält. Zum Beispiel:

```
dsmc archive -description="Projekt A" "/home/devel/proj1/*"
```

- Die meisten Optionen, die Sie in der Befehlszeile eingeben, überschreiben den in der Vorgabendatei definierten Wert. Wenn Sie jedoch die Option domain mit dem Befehl **incremental** verwenden, wird die Angabe zu der in Ihrer Clientoptionsdatei angegebenen Domäne hinzugefügt, statt den aktuellen Wert zu überschreiben.
- Bei AIX, Solaris, Linux on z und Mac beträgt die maximale Anzahl Zeichen für einen Dateinamen 255. Die maximale Länge der Kombination aus Dateiname

und Pfadname ist 1024 Zeichen. Die Unicode-Darstellung eines Zeichens kann mehrere Byte in Anspruch nehmen, sodass die maximale Anzahl Zeichen, die ein Dateiname enthalten könnte, variieren kann.

- Bei Linux beträgt die maximale Länge für einen Dateinamen 255 Byte. Die maximale Länge der Kombination aus Dateiname und Pfadname beträgt 4096 Byte. Diese Länge entspricht dem vom Betriebssystem unterstützten Wert für `PATH_MAX`. Die Unicode-Darstellung eines Zeichens kann mehrere Byte in Anspruch nehmen, sodass die maximale Anzahl Zeichen, aus denen ein Pfad- und Dateiname besteht, variieren kann. Die tatsächliche Begrenzung ist die Anzahl Byte in den Pfad- und Dateikomponenten, die einer gleichen Anzahl Zeichen entsprechen kann, aber nicht muss.

Bei Linux beträgt die maximale Länge, die Sie für eine Kombination aus Pfad- und Dateiname angeben können, für Archivierungs- oder Abrufoperationen weiterhin 1024 Byte.

- Für Mac OS X: Die maximale Länge eines Dateinamens ist auf 504 Byte (nicht Zeichen) begrenzt. Die Unicode-Darstellung eines Zeichens kann mehrere Byte in Anspruch nehmen, sodass die maximale Anzahl Zeichen, die ein Dateiname enthält, variieren kann.

Tabelle 68 enthält außerdem eine Gruppe von Clientbefehlsoptionen, die Sie nur in der Befehlszeile mit bestimmten Befehlen eingeben können.

Tabelle 68. Clientbefehlsoptionen

Befehlsoption	Beschreibung	Befehle
<code>archmc</code> „Archmc“ auf Seite 357	Verwenden Sie die Option <code>archmc</code> im Befehl archive , um die verfügbare Verwaltungsklasse für Ihre Maßnahmendomäne anzugeben, an die Sie Ihre archivierten Dateien binden wollen.	archive
<code>class</code> „Class“ auf Seite 374	Gibt an, ob bei Verwendung der folgenden Befehle eine Liste der NAS-Objekte oder der Clientobjekte angezeigt werden soll.	query backup delete filespace query filespace
<code>console</code> „Console“ auf Seite 382	Verwenden Sie die Option <code>console</code> im Befehl query systeminfo , um die Systeminformationen an der Konsole auszugeben.	query systeminfo
<code>deletefiles</code> „Deletefiles“ auf Seite 396	Löscht die lokale Kopie der Dateien von Ihrer Workstation, nachdem sie auf dem Server archiviert sind.	archive
<code>deletefiles</code> „Deletefiles“ auf Seite 396	Löscht die lokale Kopie der Dateien von Ihrer Workstation, nachdem sie auf dem Server archiviert sind. Kann auch im Befehl restore image und mit der Option <code>incremental</code> verwendet werden, um Dateien aus dem zurückgeschriebenen Image zu löschen, die nach der Erstellung des Images aus dem Dateibereich gelöscht werden.	archive restore image
<code>description</code> „Description“ auf Seite 397	Ordnet Dateien bei der Ausführung von Archivierungs-, Lösch-, Abruf- oder Archivierungsabfrageoperationen eine Beschreibung zu oder gibt eine Beschreibung für diese Dateien an.	archive delete archive query archive query backupset retrieve
<code>detail</code> „Detail“ auf Seite 398	Zeigt, abhängig vom Befehl, mit dem sie verwendet wird, Angaben zu Verwaltungsklasse, Dateibereich, Sicherung und Archivierung an.	delete filespace query archive query backup query filespace query mgmtclass

Tabelle 68. Clientbefehlsoptionen (Forts.)

Befehlsoption	Beschreibung	Befehle
dirsonly „Dirsonly“ auf Seite 403	Nur Verzeichnisse sichern, zurückschreiben, archivieren, abrufen oder abfragen.	archive incremental query archive query backup restore restore backupset retrieve selective
dynamicimage „Dynamicimage“ auf Seite 423	Führt eine dynamische Imagesicherung aus.	backup image
filelist „Filelist“ auf Seite 453	Gibt eine Liste von Dateien an, die für den Befehl verarbeitet werden sollen. Der Client für Sichern/Archivieren öffnet die angegebene Dateiliste und verarbeitet die darin aufgelisteten Dateien dem Befehl entsprechend.	archive backup group delete archive delete backup expire incremental query archive query backup restore retrieve selective
filename „Filename“ auf Seite 456	Verwenden Sie die Option filename im Befehl query systeminfo , um den Namen einer Datei anzugeben, in der die Systeminformationen gespeichert werden sollen.	query systeminfo
filesonly „Filesonly“ auf Seite 457	Nur Dateien sichern, zurückschreiben, abrufen oder abfragen.	archive incremental query archive query backup restore restore backupset retrieve selective
fromdate „Fromdate“ auf Seite 461	Mit der Option fromdate können Sie in Verbindung mit der Option fromtime ein Datum mit Uhrzeit angeben, ab dem Sie während einer Zurückschreibungs-, Abruf- oder Abfrageoperation nach Sicherungen oder Archivierungen suchen wollen.	delete backup query archive query backup restore restore group retrieve
fromnode „Fromnode“ auf Seite 461	Ermöglicht, dass ein Knoten Befehle für einen anderen Knoten ausführen kann. Ein Benutzer auf einem anderen Knoten muss mit dem Befehl set access die Berechtigung zum Abfragen, Zurückschreiben oder Abrufen von Dateien oder Images für diesen anderen Knoten erteilen.	query archive query backup query filespace query group query image query mgmtclass restore restore group restore image retrieve

Tabelle 68. Clientbefehlsoptionen (Forts.)

Befehlsoption	Beschreibung	Befehle
fromowner „Fromowner“ auf Seite 462	Dateibereiche für einen anderen Eigner anzeigen. Außerdem einen alternativen Eigner angeben, von dem Dateien zurückgeschrieben oder abgerufen werden sollen.	query archive query backup query group query image restore restore group restore image retrieve
fromtime „Fromtime“ auf Seite 463	Eine Anfangszeit am angegebenen Datum festlegen. Wird mit der Option fromdate verwendet. Diese Option wird ignoriert, wenn die Option fromdate fehlt.	query archive query backup restore restore group retrieve
groupname „Groupname“ auf Seite 464	Gibt den vollständig qualifizierten Namen einer Gruppe an.	backup group
ifnewer „Ifnewer“ auf Seite 468	Vorhandene Dateien nur durch die neueste Sicherungsversion ersetzen, wenn die Sicherungsversion aktueller als die vorhandene Version ist.	restore restore backupset restore group retrieve
imagetofile „Imagetofile“ auf Seite 470	Verwenden Sie die Option imagetofile im Befehl restore image , um anzugeben, dass Sie das Quellenimage in eine Datei zurückschreiben wollen. Es kann erforderlich sein, das Image in eine Datei zurückzuschreiben, wenn der Zieldatenträger defekte Sektoren enthält oder die Imagedaten bearbeitet werden sollen. Diese Option ist für AIX-, Linux- und Oracle Solaris-Clients gültig.	restore image
inactive „Inactive“ auf Seite 471	Zeigt bei Verwendung mit der Option pick eine Liste aktiver und inaktiver Dateien an.	delete group query backup query group query image query nas restore restore group restore image restore nas
incrbydate „Incrbydate“ auf Seite 490	Eine Teilsicherung nach Datum anfordern.	incremental
incremental „Incremental“ auf Seite 492	Änderungen des Basisimages unter Verwendung von Informationen aus Teilsicherungen, die nach der ursprünglichen Imagesicherung durchgeführt wurden, vornehmen. Diese Option ist nur für AIX-, Linux x86_64-, Linux on POWER- und Oracle Solaris-Clients gültig.	restore image
latest „Latest“ auf Seite 499	Die letzte Sicherungsversion einer Datei zurückschreiben, unabhängig davon, ob sie aktiv oder inaktiv ist.	restore restore group

Tabelle 68. Clientbefehlsoptionen (Forts.)

Befehlsoption	Beschreibung	Befehle
mode „Mode“ auf Seite 509	<p>Die Option mode ist in den folgenden Befehlen wie folgt zu verwenden:</p> <p>backup image Angaben, ob eine selektive Imagesicherung oder eine Imageteilsicherung von Clientdateisystemen ausgeführt werden soll.</p> <p>backup nas Angaben, ob eine vollständige oder eine differenzielle Imagesicherung von NAS-Dateisystemen ausgeführt werden soll.</p> <p>backup group Angaben, ob eine vollständige oder differenzielle Gruppensicherung einer Liste von Dateien ausgeführt werden soll, die sich in einem oder mehreren Dateibereichen befinden.</p>	backup group backup nas backup image restore nas
monitor „Monitor“ auf Seite 512	<p>Gibt an, ob Sie eine Imagesicherung oder -zurückschreibung mindestens eines Dateisystems, das zu einem NAS-Dateiserver gehört, überwachen wollen.</p> <p>Gibt an, ob Sie eine Zurückschreibung mindestens eines Dateisystems, das zu einem NAS-Dateiserver gehört, überwachen wollen.</p>	backup nas restore nas
nojournal „Nojournal“ auf Seite 519	Verwenden Sie diese Option im Befehl incremental , um anzugeben, dass statt der standardmäßigen urnalgestützten Sicherung die traditionelle vollständige Teilsicherung ausgeführt werden soll.	incremental
noprompt „Noprompt“ auf Seite 519	Unterdrückt die Bestätigungsaufforderung, die von den Befehlen delete group , delete archive , expire und set event angezeigt wird.	delete archive delete backup delete group expire
noprompt „Noprompt“ auf Seite 519	Unterdrückt die Bestätigungsaufforderung, die von den Befehlen delete group , delete archive , expire , restore image und set event angezeigt wird.	delete archive delete backup delete group expire restore image
optfile „Optfile“ auf Seite 523	Gibt die Clientbenutzeroptionsdatei an, die Sie verwenden wollen, wenn Sie eine Sitzung des Clients für Sichern/Archivieren starten.	dsmc
pick „Pick“ auf Seite 528	Erstellt eine Liste der Sicherungsversionen, Images oder Archivierungskopien, die der eingegebenen Dateispezifikation entsprechen. Aus der Liste können die zu verarbeitenden Versionen ausgewählt werden. Fügen Sie die Option inactive ein, um sowohl aktive als auch inaktive Objekte anzuzeigen.	delete archive delete group expire query nas restore restore group restore image restore nas retrieve

Tabelle 68. Clientbefehlsoptionen (Forts.)

Befehlsoption	Beschreibung	Befehle
pitdate „Pitdate“ auf Seite 529	Sie können mit der Option pitdate in Verbindung mit der Option pittime einen Zeitpunkt definieren, für den die aktuellsten Sicherungsversionen angezeigt oder zurückgeschrieben werden sollen.	query backup query group query image query nas restore restore group restore image restore nas
pittime „Pittime“ auf Seite 530	Sie können mit der Option pittime in Verbindung mit der Option pitdate einen Zeitpunkt definieren, für den die aktuellsten Sicherungsversionen angezeigt oder zurückgeschrieben werden sollen.	query backup query image query nas restore restore image restore nas
preservepath „Preservepath“ auf Seite 537	Gibt an, wie viel vom Quellenpfad als Teil des Zielverzeichnispfades wiederherzustellen ist, wenn Dateien an eine neue Position zurückgeschrieben oder abgerufen werden.	restore restore backupset restore group retrieve
removeoperandlimit „Removeoperandlimit“ auf Seite 546	Gibt an, dass IBM Spectrum Protect die Beschränkung auf 20 Operanden entfernt. Wenn Sie die Option removeoperandlimit mit dem Befehl incremental , selective , archive oder backup image angeben, wird die Beschränkung auf 20 Operanden nicht umgesetzt und nur durch die verfügbaren Ressourcen oder andere Begrenzungen des Betriebssystems eingeschränkt.	incremental selective archive backup image
showmembers „Showmembers“ auf Seite 579	Zeigt alle Member einer Gruppe an.	query group restore group
todate „Todate“ auf Seite 621	Mit der Option todater können Sie in Verbindung mit der Option totime ein Enddatum mit einer Endzeit angeben, bis zu dem Sie während einer Zurückschreibungs-, Abruf- oder Abfrageoperation nach Sicherungen oder Archivierungen suchen wollen.	query archive query backup restore restore group retrieve
totime „Totime“ auf Seite 622	Mit der Option totime können Sie in Verbindung mit der Option todater ein Enddatum und eine Endzeit angeben, bis zu der Sie während einer Zurückschreibungs-, Abruf- oder Abfrageoperation nach Sicherungen oder Archivierungen suchen wollen.	query archive query backup restore restore group retrieve
type „Type“ auf Seite 624	Verwenden Sie die Option type im Befehl query node , um den Typ des abzufragenden Knotens anzugeben.	query node
v2archive „V2archive“ auf Seite 627	Verwenden Sie die Option v2archive im Befehl archive , um anzugeben, dass nur Dateien auf dem Server archiviert werden sollen. Der Client verarbeitet keine Verzeichnisse, die in dem Pfad der Quelldateispezifikation vorhanden sind.	archive
verifyimage „Verifyimage“ auf Seite 629	Verwenden Sie die Option verifyimage im Befehl restore image , um anzugeben, dass die Feststellung von defekten Sektoren auf dem Zieldatenträger aktiviert werden soll. Werden defekte Sektoren auf dem Zieldatenträger festgestellt, gibt der Client eine Warnung auf der Konsole und im Fehlerprotokoll aus. Diese Option ist für AIX-, Linux- und Oracle Solaris-Clients gültig.	restore image

Tabelle 68. Clientbefehlsoptionen (Forts.)

Befehlsoption	Beschreibung	Befehle
virtualfsname „Virtualfsname“ auf Seite 630	Gibt den Namen des virtuellen Dateibereichs für die Gruppe an, mit der die Operation ausgeführt werden soll.	backup group

Ausschließlich in der Anfangsbefehlszeile gültige Optionen

Eine Untergruppe von Clientoptionen ist nur in der Anfangsbefehlszeile gültig. Viele dieser Optionen bauen die Laufzeitumgebung auf, wie z. B. die Optionen `commmethod` und `optfile`. Optionen in dieser Kategorie sind im Dialog-, Makro- oder Schedulermodus nicht gültig. Sie generieren einen Fehler und führen dazu, dass die Verarbeitung gestoppt wird.

In Tabelle 69 sind die Optionen aufgelistet, die nur in der Anfangsbefehlszeile gültig sind.

Tabelle 69. Optionen, die nur in der Anfangsbefehlszeile gültig sind

Optionen, die in der Anfangsbefehlszeile gültig sind

<code>commmethod</code>	<code>preschedulecmd/prenschedulecmd</code> (kann in die Zeitplandefinition eingeschlossen werden)
<code>deduplication</code>	
<code>diskbuffsize</code>	
<code>editor</code>	<code>querschedperiod</code>
<code>enablededupcache</code>	<code>resourceutilization</code>
<code>enablelanfree</code>	<code>retryperiod</code>
<code>errorlogmax</code>	<code>schedlogmax</code>
<code>errorlogname</code>	<code>schedlogname</code>
<code>errorlogretention</code>	<code>schedlogretention</code>
<code>lanfreecommmethod</code>	<code>schedmode</code>
<code>lanfreeshmport</code>	<code>servername</code>
<code>lanfreetcppport</code>	<code>sessioninitiation</code>
<code>maxcmdretries</code>	<code>setwindowtitle</code>
<code>nfstimeout</code>	<code>tcpbuffsize</code>
<code>nodename</code>	<code>tcpcadaddress</code>
<code>optfile</code>	<code>tcpclientaddress</code>
<code>password</code>	<code>tcpclientport</code>
<code>postschedulecmd/postnschedulecmd</code> (kann in die Zeitplandefinition eingeschlossen werden)	<code>tcpwindowsize</code>
	<code>txnbytelimit</code>
	<code>virtualnodename</code>

Clientoptionen, die vom IBM Spectrum Protect-Server definiert werden können

Einige Clientoptionen können vom IBM Spectrum Protect-Server definiert werden.

In Tabelle 70 auf Seite 354 sind die Optionen aufgelistet, die vom Server definiert werden können.


Tabelle 70. Optionen, die vom IBM Spectrum Protect-Server definiert werden können
Optionen, die vom IBM Spectrum Protect-Server definiert werden können

- „Afmskipuncachedfiles“ auf Seite 356
- „Archsymlinkasfile“ auf Seite 358
- „Changingretries“ auf Seite 373
- „Collocatebyfilespec“ auf Seite 375
- „Compressalways“ auf Seite 379
- „Compression“ auf Seite 380
- „Deduplication“ auf Seite 394
- „Dirmc“ auf Seite 402
- „Disablenqr“ auf Seite 404
- „Diskcachelocation“ auf Seite 405
- „Domain“ auf Seite 407
- „Domain.image“ auf Seite 412
- „Domain.nas“ auf Seite 413
- „Encryptiontype“ auf Seite 431
- „Encryptkey“ auf Seite 431
- „Exclude-Optionen“ auf Seite 438
- „Incl excl“ auf Seite 471
- „Include-Optionen“ auf Seite 473
- maxcandprocsmaxcandprocs
- maxmigratorsmaxmigrators
- „Memoryefficientbackup“ auf Seite 507
- „Nfstimeout“ auf Seite 516
- „Postschedulecmd/Postnschedulecmd“ auf Seite 531
- „Postsnapshotcmd“ auf Seite 533
- „Preschedulecmd/Prenschedulecmd“ auf Seite 534
- „Preserve lastaccessdate“ auf Seite 536
- „Presnapshotcmd“ auf Seite 540
- „Queryschedperiod“ auf Seite 541
- „Quiet“ auf Seite 543
- „Resourceutilization“ auf Seite 557
- „Retryperiod“ auf Seite 560
- „Schedmode“ auf Seite 570
- „Scrolllines“ auf Seite 572
- „Scrollprompt“ auf Seite 573
- „Snapshotcachesize“ auf Seite 590
- „Snapshotproviderfs“ auf Seite 591
- „Snapshotproviderimage“ auf Seite 592
- „Stagingdirectory“ auf Seite 604
- „Subdir“ auf Seite 605
- „Tapeprompt“ auf Seite 607
- „Txnbytelimit“ auf Seite 622
- „Verbose“ auf Seite 628
- „Vmchost“ auf Seite 637
- „Vmcuser“ auf Seite 640
- „Vmprocessvmwithindependent“ auf Seite 663
- „Vmprocessvmwithprdm“ auf Seite 664

Anmerkung:

1. Siehe die Produktdokumentation zu IBM Spectrum Protect for Space Management im IBM Knowledge Center unter <http://www.ibm.com/support/knowledgecenter/SSERBH/welcome>.
2. Siehe die Produktdokumentation zu IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server im IBM Knowledge Center unter <http://www.ibm.com/support/knowledgecenter/SSERBW/welcome>.

Zugehörige Tasks:

-  Clientoperationen über Clientoptionsgruppen steuern

Clientoptionsreferenz

Die folgenden Abschnitte enthalten detaillierte Informationen über die einzelnen IBM Spectrum Protect-Verarbeitungsoptionen.

Die Informationen zu jeder Option umfassen Folgendes:

- Beschreibung
- Syntaxdiagramm
- Detaillierte Beschreibung der Parameter
- Beispiele für die Verwendung der Option in der Clientoptionsdatei (falls zutreffend)
- Beispiele für die Verwendung der Option in der Befehlszeile (falls zutreffend)

Optionen mit dem Befehlszeilenbeispiel **Nicht zutreffend** können nicht in der Befehlszeile oder mit geplanten Befehlen verwendet werden.

Anmerkung:

1. Schließen Sie einen Optionswert nicht in Hochkommas oder Anführungszeichen ein, es sei denn, der Wert ist eine Dateispezifikation, die Leerzeichen oder Platzhalterzeichen enthält. Die folgende Option ist beispielsweise ungültig:

```
passwordaccess "generate"
```

2. Alle Optionen in der Datei dsm.sys mit Ausnahme der Option defaultserver müssen innerhalb einer Serverzeilengruppe eingefügt werden. Eine Serverzeilengruppe ist eine Gruppe von Optionsanweisungen in dsm.sys, die mit einer Option SERVERName beginnt und entweder bei der nächsten Option SERVERName oder am Dateiende endet.

Absolute

Mit der Option **absolute** im Befehl **incremental** können Sie eine Sicherung aller Dateien und Verzeichnisse erzwingen, die der Dateispezifikation oder **domain** entsprechen, auch wenn die Objekte sich seit der letzten Teilsicherung nicht geändert haben.

Diese Option überschreibt den Parameter mode für Sicherungskopiengruppen der Kopiengruppe in der Verwaltungsklasse. Sie hat weder Einfluss auf den Parameter frequency noch auf andere Sicherungskopiengruppenparameter. **Exclude**-Anweisungen werden von dieser Option nicht überschrieben. Daher können Objekte, die von der Sicherung ausgeschlossen sind, nicht für eine Sicherung ausgewählt werden, auch wenn die Option **absolute** angegeben ist.

Wichtig: Bevor Sie die Option **absolute** verwenden, lesen Sie die folgenden Informationen zu den Auswirkungen, die diese Option auf Sicherungs- und IBM Spectrum Protect-Serveroperationen haben kann:

- Sicherungen benötigen mehr Serverspeicher und Datenbankressourcen.
- Sicherungen erfordern mehr Netzbandbreite.
- Die Ausführung von Serveroperationen (z. B. Bestandsverfall, Speicherpoolsicherung, Speicherpoolumlagerung, Wiederherstellung und Knotenreplikation) nimmt mehr Zeit in Anspruch. Die Datendeduplizierung kann einige dieser Auswirkungen mindern, sie verhindert jedoch nicht die erforderliche Verarbeitung zur Wiederherstellung der deduplizierten Daten zurück in ihre ursprüngliche Form, wenn der Speicherpool in Speicher ohne Deduplizierung umgelagert oder gesichert wird.

Diese Option ist nur als Befehlszeilenparameter für den Befehl **incremental** gültig, wenn Sie folgende Operationen ausführen:

- Vollständige oder partielle progressive Teilsicherungen von Dateisystemen oder Plattenlaufwerken.
- Momentaufnahmedifferenzsicherungen, wenn außerdem `createnewbase=yes` angegeben ist.

Um eine Gesamtsicherung eines Dateisystems zu erzwingen, in dem die journalbasierte Sicherung verwendet wird, geben Sie die Optionen `nojournal` und `absolute` im Befehl **incremental** an.

Damit die Option `absolute` für geplante Teilsicherungen verwendet werden kann, muss der IBM Spectrum Protect-Serveradministrator einen separaten Sicherungszeitplan erstellen, der die Option `absolute` im Parameter `options` des Zeitplans enthält.

Unterstützte Clients

Diese Option ist für alle Clients als Befehlszeilenparameter für den Befehl **incremental** gültig. Diese Option kann nicht einer Clientoptionsgruppe auf dem IBM Spectrum Protect-Server hinzugefügt werden.

Syntax

►►—ABSolute—◄◄

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
dsmc incr -absolute "/Users/sparky/source/*.c"
```

Afmskipuncachedfiles

Die Option `afmskipuncachedfiles` gibt an, ob bei General Parallel File System (GPFS) nicht zwischengespeicherte und genutzte Dateien in Active File Management-Dateigruppen bei Sicherungs-, Archivierungs- und Umlagerungsoperationen verarbeitet werden.

GPFS Active File Management sowie die Dateistatus *nicht zwischengespeichert* und *genutzt* sind in Produktinformation zu IBM Spectrum Scale erläutert.

Die Ausführung von HSM auf GPFS-Dateisystemen, die Active File Management-Dateigruppen verwenden, ist in Anleitung für die Integration von IBM Spectrum Scale AFM mit IBM Spectrum Protect beschrieben.

Definieren Sie `afmskipuncachedfiles=yes`, wenn Sie Dateien aus einem Dateisystem sichern, archivieren oder umlagern, das Active File Management-Dateigruppen enthält.

Einschränkung: Wenn Active File Management im LU-Modus (LU = Local Update) ausgeführt wird, muss die Option **afmskipuncachedfiles** in der Cachedateigruppe auf **No** gesetzt werden.

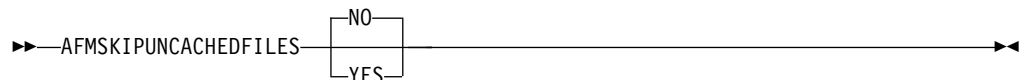
Unterstützte Clients

Diese Option ist für Clients für Sichern/Archivieren gültig, die auf AIX- und Linux-Systemen ausgeführt werden.

Optionsdatei

Fügen Sie diese Option in die Datei `dsm.sys` vor allen Serverzeilengruppen ein.

Syntax



Parameter

NO Der Active File Management-Dateistatus wird bei Sicherungs-, Archivierungs- und Umlagerungsoperationen ignoriert. Umlagerungsoperationen für nicht zwischengespeicherte oder genutzte Dateien schlagen fehl und führen zur Fehlermeldung ANS9525E. Sicherungs- und Archivierungsoperationen für nicht zwischengespeicherte Dateien erfordern Active File Management-Abrufoperationen. Die Abrufoperationen können beträchtlichen Datenaustausch im Netz zwischen der Active File Management-Ausgangsposition und dem Cache verursachen. Dieser Parameter ist der Standardwert.

YES

Nicht zwischengespeicherte oder genutzte Dateien in Active File Management-Dateigruppen werden bei der Sicherungs-, Archivierungs- und Umlagerungsverarbeitung übersprungen.

Archmc

Verwenden Sie die Option **archmc** im Befehl **archive**, um die verfügbare Verwaltungsklasse für Ihre Maßnahmendomäne anzugeben, an die Sie Ihre archivierten Dateien und Verzeichnisse binden wollen.

Wenn Sie eine Datei archivieren, können Sie die zugeordnete Verwaltungsklasse überschreiben, indem Sie die Option **archmc** im Befehl **archive** angeben oder den Web-Client verwenden. Das Überschreiben der Verwaltungsklasse mit dem Web-Client ist äquivalent zur Verwendung der Option **archmc** im Befehl **archive**.

Wenn Sie die Option **archmc** nicht verwenden, bindet der Server archivierte Verzeichnisse an die Standardverwaltungsklasse. Hat die Standardverwaltungsklasse keine Archivierungskopiengruppe, bindet der Server archivierte Verzeichnisse an die Verwaltungsklasse mit dem kürzesten Aufbewahrungszeitraum.

Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

►►—ARCHMc =—*Verwaltungsklasse*—►►

Parameter

Verwaltungsklasse

Gibt den Namen einer verfügbaren Verwaltungsklasse in der aktiven Maßnahmengruppe der Maßnahmendomäne an. Diese Verwaltungsklasse überschreibt die Standardverwaltungsklasse und alle `include`-Anweisungen für die Dateien und Verzeichnisse, die Sie archivieren.

Beispiele

Befehlszeile:

```
dsmc archive -archmc=ret2yrs /Users/van/Documents/budget.jan  
dsmc archive -archmc=ret2yrs /home/plan/proj1/budget.jan
```

Archsymlinkasfile

Die Option `archsymlinkasfile` gibt an, ob der Client für Sichern/Archivieren einer symbolischen Verbindung folgt und die Datei oder das Verzeichnis archiviert, auf die/das die Verbindung zeigt, oder ob nur die symbolische Verbindung archiviert wird. Diese Option ist im Befehl **archive** zu verwenden.

Unterstützte Clients

Diese Option ist für alle UNIX-Clients mit Ausnahme von Mac OS X gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (`dsm.opt`) ein.

Syntax

►►—ARCHSYMLinkasfile ☐ Yes ☐ No—►►

Parameter

Yes

Gibt an, dass der Client einer symbolischen Verbindung folgt und die zugehörige Datei oder das zugehörige Verzeichnis archiviert. Dies ist der Standardwert.

No Gibt an, dass der Client die symbolische Verbindung archiviert und nicht die zugehörige Datei oder das zugehörige Verzeichnis.

Beispiele

Optionsdatei:

```
archsymlinkasfile no
```

Befehlszeile:

```
-archsymb=no
```

Asnodename

Mit der Option `asnodename` können Agentenknoten Daten im Namen eines anderen Knotens (des Zielknotens) sichern oder zurückschreiben. Auf diese Weise sind gleichzeitig ablaufende Operationen von mehreren Knoten möglich, um Daten auf demselben Zielknoten und in demselben Dateibereich parallel zu speichern.

Ihrem Clientknoten muss über den Befehl **grant proxynode** vom Verwaltungsklient des IBM Spectrum Protect-Servers Zugriff auf den Zielknoten erteilt werden und Sie müssen ein Root sein, um die Option `asnodename` zu verwenden.

Wenn der IBM Spectrum Protect-Administrator einem Knoten die Proxy-Berechtigung erteilt und Sie die Option `asnodename` für diesen Knoten verwenden, können Sie alle Dateien abfragen und zurückschreiben, als ob Sie über Rootberechtigung verfügen würden.

Ein Agentenknoten ist ein Clientknoten, dem die Berechtigung erteilt wurde, Clientoperationen im Namen eines Zielknotens auszuführen.

Ein Zielknoten ist ein Clientknoten, der einem oder mehreren Agentenknoten die Berechtigung erteilt, in seinem Namen Clientoperationen auszuführen.

Eine Proxy-Operation verwendet die Einstellungen für den Zielknoten (beispielsweise **maxnummp** und **deduplication**) sowie Zeitpläne, die auf dem Server definiert sind. Die Einstellungen und Zeitpläne für den Agentenknoten auf dem IBM Spectrum Protect-Server werden ignoriert.

Beispielsweise können Sie den folgenden Befehl verwenden, um gemeinsam genutzte Daten für den Dateibereich zu sichern, der unter dem Knotennamen MyCluster gespeichert ist:

```
/cluster1/mydata  
dsmc incremental /Users -asnodename=MyCluster
```

Sie können die Option `asnodename` auch verwenden, um Daten zurückzuschreiben, die unter einem anderen Knotennamen auf dem Server gespeichert sind. Sie können nur Daten zurückschreiben, deren Eigner Sie sind.

Die Option `asnodename` unterscheidet sich wie folgt von der Option `nodename`:

- Bei Verwendung der Option `nodename` müssen Sie das Kennwort für den von Ihnen angegebenen Knotennamen eingeben.
- Bei Verwendung der Option `asnodename` müssen Sie das Kennwort für Ihren Clientagentenknoten angeben, um auf die Daten zugreifen zu können, die für den Zielknoten gespeichert sind.

Einschränkungen: Sie können die Option `asnodename` nicht mit `-fromnode` verwenden und Sie können mit `asnodename` keine NAS-Sicherung ausführen. Außerdem kann `asnodename` für Clustersysteme verwendet werden, auch wenn keine spezifische Cluster-Software unterstützt wird.

Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Datei `dsm.sys` *innerhalb* einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Allgemein** des Profileditors definieren.

Syntax

►—ASNODENAME— *Zielknoten* —►

Parameter

Zielknoten

Gibt den Knotennamen auf dem IBM Spectrum Protect-Server an, unter dem Daten gesichert oder zurückgeschrieben werden sollen.

Beispiele

Optionsdatei:

```
asnodename mycluster
```

Befehlszeile:

```
-asnodename=mycluster
```

Diese Option ist im interaktiven Modus nicht gültig, aber sie kann im Abschnitt Optionen einer Zeitplandefinition definiert werden.

Sitzungseinstellungen und Zeitpläne für eine Proxy-Operation

Eine Proxy-Operation tritt auf, wenn ein Agentenknoten die Option `asnodename Name_des_Zielknotens` verwendet, um Operationen in Namen des angegebenen Zielknotens auszuführen.

Eine Proxy-Operation verwendet die Einstellungen für den Zielknoten (beispielsweise **maxnummp**, **cloptset** und **deduplication**) sowie Zeitpläne, die auf dem IBM Spectrum Protect-Server definiert sind. Die Einstellungen und Zeitpläne für den Agentenknoten auf dem Serverknoten werden ignoriert.

Für Proxy-Operationen gelten die folgenden Hinweise.

- Alle Operationen verwenden selbst dann die Einstellungen und Konstrukte der Maßnahmendomäne des Zielknotens, wenn der Agentenknoten zu einer anderen Domäne gehört. Die Einstellungen und Konstrukte der Maßnahmendomäne des Agentenknotens werden ignoriert.
- Der Agentenknoten authentifiziert sich unter Verwendung des Kennworts des Agentenknotens beim IBM Spectrum Protect-Server.
- Damit Proxy-Operationen ausgeführt werden können, dürfen der Agentenknoten und der Zielknoten auf dem Server nicht gesperrt sein.
- Proxy-Knotenbeziehungen sind nicht transitiv. Wenn ein Zielknoten selbst als Proxy-Knoten für einen anderen Knoten definiert ist, kann der Agentenknoten nicht verwendet werden, um Operationen auf diesem anderen Knoten auszuführen; es sei denn, der Agent ist auch als Proxy-Knoten für diesen anderen Knoten definiert.

Angenommen, die folgenden Proxy-Definitionen gelten für die Knoten TAURUS, SCORPIO und GEMINI:

- TAURUS ist ein Proxy-Knoten für SCORPIO.
- TAURUS ist kein Proxy-Knoten für GEMINI.

- SCORPIO ist ein Proxy-Knoten für GEMINI.

Die Proxy-Definitionen führen zu den folgenden Ergebnissen:

- TAURUS kann Operationen im Namen von SCORPIO ausführen.
- SCORPIO kann Operationen im Namen von GEMINI ausführen.
- TAURUS kann keine Operationen im Namen von GEMINI ausführen.

Auditlogging

Verwenden Sie die Option `auditlogging`, um ein Prüfprotokoll zu generieren, das für jede Datei, die während einer Teilsicherungsoperation, einer selektiven Sicherungsoperation, einer Archivierungs-, Zurückschreibungs- oder Abrufoperation verarbeitet wird, einen Eintrag enthält.

Das Prüfprotokoll kann so konfiguriert werden, dass es entweder eine Basisversion oder eine inklusivere (vollständige) Version an Informationen erfasst.

Die Basisversion der Prüfprotokollierungsfunktion erfasst die Informationen, die sich im Planungsprotokoll befinden und zeichnet die Informationen auf, dass eine Datei während einer Teilsicherungsoperation, einer selektiven Sicherungsoperation, einer Archivierungs-, Zurückschreibungs- oder Abrufoperation gesichert, archiviert, aktualisiert, zurückgeschrieben, abgerufen, gelöscht und übersprungen wurde oder abgelaufen oder fehlgeschlagen ist. Darüber hinaus erfasst die Basisversion der Prüfprotokollierung den Eingabebefehl für die durch den Befehlszeilenclient für Sichern/Archivieren oder den Scheduler-Client ausgeführten Befehle.

Die vollständige Version der Prüfprotokollierung zeichnet für jede Datei, die vom Client für Sichern/Archivieren verarbeitet wird, eine Aktion auf. Zusätzlich zu all den Ereignissen, die von der Basisversion der Prüfprotokollierung aufgezeichnet wird, zeichnet die vollständige Version der Prüfprotokollierung Informationen über eine Datei auf, die ausgeschlossen wurde oder während einer fortlaufenden Teilsicherungsoperation nicht gesendet wurde, weil sich die Datei nicht geändert hat.

Nachfolgend wird ein Beispiel der Nachrichten aufgezeigt, die ausgegeben werden, wenn das Prüfprotokoll so konfiguriert wird, dass es die Basisversion der Informationen erfasst:

```
21.04.07 15:25:05 ANS1650I Befehl:
    sel /home/spike/test/*
21.04.07 15:25:05 ANS1651I Gesichert:
    /home/spike/test/file.txt
21.04.07 15:25:05 ANS1652I Archiviert:
    /home/spike/test/file.txt
21.04.07 15:25:05 ANS1653I Aktualisiert:
    /home/spike/test/file.txt
21.04.07 15:25:05 ANS1654E Fehlgeschlagen:
    /home/spike/test/file.txt
21.04.07 15:25:05 ANS1655I Zurückgeschrieben:
    /home/spike/test/file.txt
21.04.07 15:25:05 ANS1656I Abgerufen:
    /home/spike/test/file.txt
21.04.07 15:25:05 ANS1657I Abgelaufen:
    /home/spike/test/file.txt
21.04.07 15:25:05 ANS1658I Gelöscht:
    /home/spike/test/file.txt
21.04.07 15:25:05 ANS1659I Übersprungen:
    /home/spike/test/file.txt
```

Die folgenden Nachrichten können ausgegeben werden, wenn das Prüfprotokoll so konfiguriert wird, dass es die vollständige Version der Informationen erfasst (zusätzlich zu all den Nachrichten, die für die Basisversion der Prüfprotokollierung ausgegeben werden):

```
21.04.07 15:25:05 ANS1660I Ausgeschlossen:  
/home/spike/test/file.txt  
21.04.07 15:25:05 ANS1661I Unverändert:  
/home/spike/test/file.txt
```

Das Prüfprotokoll ist kein Ersatz oder Vertreter für das Standardfehlerprotokoll (`dsmerror.log`) oder für das Planungsprotokoll (`dsmsched.log`). Tritt ein Fehler auf, der die Verarbeitung einer Datei verhindert, wird eine Nachricht in das Prüfprotokoll geschrieben, die besagt, dass ein Fehler aufgetreten ist. Die Nachricht gibt jedoch nicht die Art des Fehlers an. Zur Fehlerdiagnose muss trotzdem noch das Standardfehlerprotokoll verwendet werden.

Die Prüfprotokolleinträge enthalten nur eine Zeitmarke und den Objektnamen. Es gibt keine Angaben, um zwischen Dateien und Verzeichnissen unterscheiden zu können, oder Informationen über die Größe eines Objekts.

Der Client für Sichern/Archivieren unter Mac OS X erstellt das Prüfprotokoll als Unicode-Datei (UTF-16).

Standardmäßig lautet der Name des Prüfprotokolls `dsmaudit.log`; es ist in demselben Verzeichnis enthalten wie das Fehlerprotokoll `dsmerror.log`. Der Name und Standort des Prüfprotokolls kann mit Hilfe der Option `auditlogname` konfiguriert werden. Es gibt keine Parameter, um die Größe des Prüfprotokolls zu steuern oder das Prüfprotokoll zu bereinigen. Die Option `auditlogname` kann nicht als Option in einer Clientoptionsgruppe des IBM Spectrum Protect-Servers definiert werden.

Der Befehl **auditlogging** wird mit Sicherungsbefehlen unterstützt, die mit Objekten auf Dateiebene interagieren, z. B. **backup groups**.

Der Befehl **auditlogging** wird nicht mit Sicherungsbefehlen unterstützt, die mit Objekten auf Imageebene interagieren, z. B. **backup image** oder **restore image**. Der Befehl **auditlogging** wird mit Sicherungsbefehlen unterstützt, die mit Objekten auf Dateiebene interagieren, z. B. **backup groups**.

Haben Sie die Prüfprotokollierung für eine Operation aktiviert und ist das Schreiben in das Prüfprotokoll nicht möglich (wenn beispielsweise die Platte voll ist, auf der das Prüfprotokoll gespeichert ist), wird die Prüfprotokollierung für den Rest der Operation inaktiviert und der Rückkehrcode für die Operation wird unabhängig vom Ergebnis der Operation auf 12 gesetzt.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientssystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein.

Syntax



Parameter

off

Gibt an, dass die Prüfprotokollierungseinrichtung nicht aktiviert ist. Dies ist der Standardwert.

basic

Gibt an, dass das Prüfprotokoll eine Basisebene an Informationen erfasst.

full

Gibt an, dass das Prüfprotokoll eine umfassendere Ebene an Informationen erfasst.

Beispiele

Eine Teilsicherung mit aktivierter Prüfprotokollierung ausführen.

Befehlszeile:

```
dsmc i -auditlogging=basic
```

Eine Liste von Dateien mit der umfassendsten Protokollierungsstufe sichern, sodass eine separate Anwendung wie ein Perl-Script die Ergebnisse überprüfen kann.

Auditlogname

Die Option `auditlogname` gibt den Pfad und den Namen der Datei an, in der Prüfprotokollinformationen gespeichert werden sollen. Diese Option wird angewendet, wenn die Prüfprotokollierung aktiviert ist.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein.

Syntax



Parameter

Dateispezifikation

Gibt den Pfad und den Namen der Datei an, in der der Client für Sichern/Archivieren Prüfprotokolldaten speichern soll.

Wird nur ein Dateiname angegeben, wird die Datei im aktuellen Verzeichnis gespeichert. Standardwert ist das Installationsverzeichnis mit dem Dateinamen dsmaudit.log. Die Datei dsmaudit.log kann keine symbolische Verbindung sein.

Beispiele

Eine Teilsicherung mit aktivierter Prüfprotokollierung ausführen.

Beispielsausgabe

Nachfolgend wird ein Beispiel für eine Ausführung und Ausgabedatei aufgeführt:

```
> dsmc inc /SMSVT/mfs1 -auditlogging=full
-auditlogname=/home/cliv3/audit.log
IBM Spectrum Protect
Befehlszeilenschnittstelle des Clients für Sichern/Archivieren
Clientversion 8, Release 1, Stufe 0.0
Clientdatum/-zeit: 16.11.2016 12:05:35
(c) Copyright IBM Corporation und andere 1990, 2016.
Alle Rechte vorbehalten.
```

```
Knotenname: NAXOS_CLUSTER
Sitzung hergestellt mit Server
ODINHSMSERV: AIX-RS/6000
Serverversion 8, Release 1, Stufe 0.0
Serverdatum/-zeit: 16.11.2016 12:05:35
Letzter Zugriff: 15.11.2016 12:01:57
```

```
Teilsicherung von Datenträger '/SMSVT/mfs1'
Verzeichnis--> 4.096 /SMSVT
/mfs1/ [Gesendet]
Normale Datei--> 32.768 /SMSVT
/mfs1/test0 [Gesendet]
Normale Datei--> 32.768 /SMSVT
/mfs1/test1 [Gesendet]
Normale Datei--> 32.768 /SMSVT
/mfs1/test2 [Gesendet]
Normale Datei--> 32.768 /SMSVT
/mfs1/test3 [Gesendet]
Normale Datei--> 32.768 /SMSVT
/mfs1/test4 [Gesendet]
Normale Datei--> 32.768 /SMSVT
/mfs1/test5 [Gesendet]
Normale Datei--> 32.768 /SMSVT
/mfs1/test6 [Gesendet]
Normale Datei--> 32.768 /SMSVT
/mfs1/test7 [Gesendet]
Normale Datei--> 32.768 /SMSVT
/mfs1/test8 [Gesendet]
Normale Datei--> 32.768 /SMSVT
/mfs1/test9 [Gesendet]
Erfolgreiche Teilsicherung von '/SMSVT/mfs1'
```

```
Gesamtzahl geprüfter Objekte: 11
Gesamtzahl gesicherter Objekte: 11
Gesamtzahl aktualisierter Objekte: 0
Gesamtzahl erneut gebundener Objekte: 0
Gesamtzahl gelöschter Objekte: 0
Gesamtzahl verfallener Objekte: 0
Gesamtzahl fehlgeschlagener Objekte: 0
Gesamtzahl übertragener Byte: 320,31 KB
Datenübertragungszeit: 0,01 Sek.
Datenübertragungsgeschwindigkeit im Netz: 17.141,84 KB/Sek.
```


Nachfolgend wird der Inhalt des Prüfprotokolls aufgeführt:

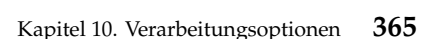
Zugehörige Informationen

Autodeploy

Unterstützte Clients

Optionsdatei

Syntax



Parameter

Yes

Gibt an, dass der Client vom Server automatisch implementiert wird. *Yes* ist der Standardwert.

No Gibt an, dass der Client vom Server nicht automatisch implementiert wird.

Beispiele

Optionsdatei:

autodeploy no

Befehlszeile:

Nicht zutreffend.

Wichtig: Verwenden Sie `schedmode prompted` mit der Option `autodeploy`, um die sofortige Verarbeitung des Clientimplementierungszeitplans durch den Scheduler zu aktivieren.

Zugehörige Konzepte:

„Automatische Implementierung des Clients für Sichern/Archivieren“ auf Seite 2

Autofsrename

Mit der Option `autofsrename` wird ein vorhandener, nicht Unicode-fähiger Dateibereich auf dem IBM Spectrum Protect-Server umbenannt, sodass für die aktuelle Operation ein Unicode-fähiger Dateibereich mit dem ursprünglichen Namen erstellt werden kann.

Wenn Sie `autofsrename yes` in Ihrer Clientoptionsdatei angeben und der Serverwert für `autofsrename` auf `client` gesetzt ist, generiert der IBM Spectrum Protect-Server einen eindeutigen Namen durch Anhängen von `_OLD` an den Dateibereichsnamen, den Sie in der aktuellen Operation angeben. Beispielsweise benennt der Server den Dateibereich `Jaguar` in `Jaguar_OLD` um. Ist der neue Dateibereichsname zu lang, ersetzt das Suffix die letzten Zeichen des Dateibereichsnamens. Beispielsweise wird der Dateibereichsname `mylongfilesystemname` wie folgt umbenannt:

`mylongfilesystem_OLD`

Ist der neue Dateibereich bereits auf dem Server vorhanden, benennt der Server den neuen Dateibereich in `Jaguar_OLDx` um, wobei `x` eine eindeutige Zahl ist.

Der Server erstellt neue Unicode-fähige Dateibereiche, die nur die in der aktuellen Operation angegebenen Daten enthalten. Beispiel: Angenommen, `Jaguar` ist der Name Ihrer Startplatte und Sie archivieren alle `.log`-Dateien im Verzeichnis `/Users/user5/Documents`. Bevor die Archivierung stattfindet, benennt der Server den Dateibereich in `Jaguar_OLD` um. Bei der Archivierung werden die in der aktuellen Operation angegebenen Daten in den Unicode-fähigen Dateibereich mit dem Namen `Jaguar` gestellt. Der neue Unicode-fähige Dateibereich enthält nun nur das Verzeichnis `/Users/user5/logs` und die Dateien `*.log`, die in der Operation angegeben wurden. Der Server speichert alle Daten aus nachfolgenden vollständigen und partiellen Teilsicherungen, selektiven Sicherungen und Archivierungen in den neuen Unicode-fähigen Dateibereichen.

Beispiel: Angenommen, `Jaguar` ist der Name Ihrer Startplatte und Sie archivieren alle `.log`-Dateien im Verzeichnis `/Users/user5/Documents`. Bevor die Archivierung stattfindet, benennt der Server den Dateibereich in `Jaguar_OLD` um. Bei der Archivierung werden die in der aktuellen Operation angegebenen Daten in den Uni-

Parameter

Yes

Gibt an, dass der IBM Spectrum Protect-Server automatisch alle Dateibereiche, die nicht Unicode-fähig sind, in der aktuellen Sicherungs- oder Archivierungsoperation umbenennt.

No Gibt an, dass der Server Dateibereiche, die nicht Unicode-fähig sind, in der aktuellen Sicherungs- oder Archivierungsoperation nicht umbenennt.

Prompt

Gibt an, dass Sie angeben müssen, ob die Dateibereiche, die nicht Unicode-fähig sind, in der aktuellen Operation umbenannt werden sollen. Dies ist der Standardwert.

Hinweise:

- Diese Option wird nur angewendet, wenn der Server die Option `autofsrename` auf `client` setzt.
- Wenn der Client-Scheduler ausgeführt wird, wird standardmäßig keine Bedienerführung angezeigt. Bei der nächsten interaktiven Sitzung werden Sie über eine Bedienerführung gefragt, ob der Dateibereich umbenannt werden soll.
- Der Client zeigt die Bedienerführung *nur* einmal pro Dateibereich an. Wird an der Bedienerführung `no` angegeben, kann der Client die Dateibereiche später nicht mehr umbenennen. Der IBM Spectrum Protect-Administrator kann die Dateibereiche jedoch auf dem Server umbenennen.
- Werden Dateien in einem Dateibereich gesichert, der nicht Unicode-fähig ist, überspringt der Unicode-fähige Client die Dateien und Verzeichnisse mit Namen, die Zeichen aus einer Zeichenumsetzungstabelle enthalten, die von den aktuellen länderspezifischen Angaben abweichen.
- Wurden Dateien und Verzeichnisse mit Namen, die Zeichen aus einer anderen Zeichenumsetzungstabelle als den aktuellen länderspezifischen Angaben enthalten, zuvor mit einem Client gesichert, der nicht Unicode-fähig war, können sie verfallen. Der Unicode-fähige Client lässt diese Dateien verfallen, wenn Sie den Dateibereich nicht in einen Unicode-fähigen Dateibereich migrieren. Sie können diese Dateien in einem Unicode-fähigen Dateibereich sichern und archivieren.

Beispiele

Optionsdatei:

```
autofsrename yes
```

Automount

Die Option `automount` fügt durch Anhängen ein Auto-Mount-Dateisystem in die Domäne ein. Diese Option ist mit der Option `domain` zu verwenden.

Verwenden Sie diese Option, um alle Auto-Mount-Dateisysteme anzugeben, die der Client für Sichern/Archivieren zu folgenden Zeitpunkten anzuhängen versucht:

- Beim Start des Clients
- Beim Start der Sicherung
- Wenn der Client während der Sicherung ein Auto-Mount-Dateisystem erreicht hat

Hängen Sie das Dateisystem an, bevor der Client eine Sicherung dieses Dateisystems ausführt. Wenn das Dateisystem immer vor der Ausführung der Sicherung angehängt wird, ist es nicht erforderlich, explizit ein Auto-Mount-Dateisystem in

der Option automount anzugeben. Sie sollten dieses Dateisystem jedoch der Option automount hinzufügen, um sicherzustellen, dass das Dateisystem zu allen oben aufgeführten Zeitpunkten angehängt wurde. Die Auto-Mount-Dateisysteme werden erneut angehängt, wenn sie zwischenzeitlich während einer Sicherung abgehängt wurden.

Unterstützte Clients

Diese Option ist für alle UNIX-Plattformen außer Mac OS X gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein.

Syntax



Parameter

Dateibereichsname

Gibt mindestens ein vollständig qualifiziertes Auto-Mount-Dateisystem an, das angehängt und in die Domäne eingefügt wird.

Beispiele

Optionsdatei:

automount /home/Fred /home/Sam

Befehlszeile:

Nicht zutreffend.

Zugehörige Informationen

Unter „Domain“ auf Seite 407 finden Sie weitere Informationen zur Verwendung von Auto-Mount-Dateisystemen und zur Option domain.

Backmc

Die Option backmc gibt die Verwaltungsklasse an, die für Aufbewahrungszwecke auf den Befehl **backup fastback** angewendet werden soll.

Verwenden Sie die Option backmc mit dem Befehl **backup fastback**.

Wenn Sie ein Objekt mehrmals sichern und für jede Sicherung eine andere Verwaltungsklasse angeben, werden alle Sicherungsversionen des Objekts erneut an die letzte angegebene Verwaltungsklasse gebunden.

Unterstützte Clients

Diese Option ist für Linux x86_64-Clients gültig.

Optionsdatei

Keine. Sie können diese Option nur in der Befehlszeile oder im Scheduler angeben.

Syntax

►►—BACKMc=*Name der Verwaltungsklasse*—————►◄

Parameter

Name der Verwaltungsklasse

Gibt den Namen der Verwaltungsklasse an.

Beispiele

Befehlszeile:

```
dsmc backup fastback -fbpolicyname=policy1 -fbserver=server1  
-backmc=ret2yrs
```

Backupsetname

Die Option backupsetname gibt den Namen eines Sicherungssatzes auf dem IBM Spectrum Protect-Server an.

Sie können die Option backupsetname in den folgenden Befehlen verwenden:

- **query backup**
- **query filespace**
- **query image**
- **restore image**

Anmerkung: Die folgenden Befehle akzeptieren den Parameter backupsetname zur Angabe einer Position. Der Parameter backupsetname zur Angabe einer Position verhält sich anders als die Option backupsetname. Den Beschreibungen der Befehle können Sie entnehmen, wie der Parameter backupsetname zur Angabe einer Position sich auf jeden dieser Befehle auswirkt:

```
query backupset  
restore  
restore backupset
```

Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Keine. Sie können diese Option nur in der Befehlszeile angeben.

Syntax

►►—BACKUPSETName=*Name des Sicherungssatzes*—————►◄

Parameter

Name des Sicherungssatzes

Gibt den Namen des Sicherungssatzes auf dem IBM Spectrum Protect-Server an. Platzhalterzeichen sind nicht zulässig.

Beispiele

Befehlszeile:

```
dsmc query backup /Volumes/bkSets/file.1
-backupsetname=YEAR_END_ACCOUNTING.12345678
dsmc query backup /usr/projects -subdir=yes
-backupsetname=YEAR_END_ACCOUNTING.12345678
dsmc restore image /home/proj
-backupsetname=ACCOUNTING_2007.12345678
dsmc query image -backupsetname=WEEKLY_BSET.21435678
```

Zugehörige Informationen

„Daten aus einem Sicherungssatz zurückschreiben“ auf Seite 250

Basesnapshotname

Die Option `basesnapshotname` gibt die Momentaufnahme an, die als Basismomentaufnahme verwendet werden soll, wenn Sie eine Momentaufnahmedifferenzsicherung (`snappdiff`) eines NetApp-Dateiserverdatenträgers ausführen. Wenn Sie diese Option angeben, müssen Sie auch die Option `snappdiff` verwenden. Andernfalls tritt ein Fehler auf. Wenn `basesnapshotname` nicht angegeben wird, wählt die Option `useexistingbase` die jüngste Momentaufnahme auf dem Dateiserverdatenträger als Basismomentaufnahme aus.

Wenn die angegebene Momentaufnahme nicht gefunden wird, wird ein Fehler gemeldet und die Sicherungsoperation schlägt fehl.

Unterstützte Clients

Diese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Optionsdatei

Diese Option kann in der Clientoptionsdatei oder in der Befehlszeile angegeben werden.

Syntax

►►—BASESNAPSHOTName— —*Momentaufnahmename*—————►◄

Parameter

Momentaufnahmename

Gibt den Namen einer vorhandenen Momentaufnahme an, die als Basismomentaufnahme verwendet werden soll. Der angegebene Name kann der Name einer Momentaufnahme wie `voll_snap` oder der Name einer geplanten NetApp-Sicherung wie beispielsweise `nightly.x` sein, wobei *x* für die Folgenummer steht (dabei ist `nightly.0` die älteste Momentaufnahme).

Sie können auch ein Muster mit Platzhalterzeichen für die Auswahl einer Momentaufnahme verwenden. Gültige Platzhalterzeichen sind:

* Ein Stern (*) entspricht beliebigen Zeichen.

? Ein Fragezeichen (?) entspricht einem einzelnen Zeichen.

Die Platzhalterzeichen sind nützlich, wenn Ihre Momentaufnahmenamen einem Muster entsprechen, z. B. wenn sie das Datum oder die Uhrzeit enthalten. Eine am 12. November 2012 um 11:10:00 Uhr erstellte Momentaufnahme könnte beispielsweise als UserDataVol_121103111000_snapshot gespeichert werden. Die jüngste Momentaufnahme, die dem Muster entspricht, wird als vorhandene Basis ausgewählt. Wenn beispielsweise die beiden gespeicherten Momentaufnahmen UserDataVol_121103111000_snapshot und UserDataVol_121103231000_snapshot vorhanden sind, wird UserDataVol_121103231100_snapshot ausgewählt, weil diese Momentaufnahme 12 Stunden jünger als die andere Momentaufnahme ist.

```
-basesnapshotname="UserDataVol_*_snapshot"
```

Fragezeichen sind für geplante Sicherungen, die einem konsistenten Namensmuster folgen, gut geeignet. Mit der folgenden Syntax wird die jüngste Sicherung „nightly“ als Momentaufnahme ausgewählt, die als vorhandene Basis verwendet werden soll.

```
-basenameshotname="nightly.?"
```

Beispiele

Optionsdatei:

```
basesnapshotname nightly.?
```

```
basesnapshotname volum_base_snap
```

Befehlszeile:

```
dsmc incr \\DRFiler\UserDataVol_Mirror_Share -snapdiff  
-useexistingbase -basesnapshotname="nightly.?"
```

Zugehörige Informationen

Useexistingbase

Cadlistenonport

Die Option cadlistenonport gibt an, ob ein Empfangsport für den Clientakzeptor geöffnet werden soll.

Wenn ein Empfangsport offen ist, kann er alle eingehenden Verbindungen akzeptieren. Der Port wird jedoch nicht verwendet, wenn der Clientakzeptor nur den Scheduler verwaltet und der Scheduler im Abfragemodus ausgeführt wird. Mit dieser Option können Sie verhindern, dass der Akzeptor den nicht verwendeten Port öffnet.

Die Standardeinstellung für diese Option ist yes. Verwenden Sie cadlistenonport no nur, wenn managedservices schedule und schedmode polling verwendet werden.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Syntax



Parameter

Yes

Gibt an, dass der Clientakzeptor einen Empfangsportal öffnet. Dieser Parameter ist der Standardwert.

No Gibt an, dass der Clientakzeptor keinen Empfangsportal öffnet. Verwenden Sie diese Einstellung, wenn Sie den Clientakzeptor nur zur Verwaltung des Schedulers im Abfragemodus verwenden.

Diese Einstellung bewirkt die effektive Inaktivierung anderer Clientfunktionen, die vom Clientakzeptor abhängig sind, wie beispielsweise Sicherungs- und Zurückschreibungsoperationen des Web-Clients, Operationen der IBM Spectrum Protect for Virtual Environments: Data Protection for VMware vSphere-GUI sowie Sicherungs- und Zurückschreibungsoperationen von IBM Spectrum Protect Snapshot.

Beispiel

Optionsdatei:

```
cadlistenonport no
```

Befehlszeile:

Nicht zutreffend.

Zugehörige Verweise:

„Managedservices“ auf Seite 502

„Schedmode“ auf Seite 570

Changingretries

Mit der Option **changingretries** wird angegeben, wie oft der Client den Versuch, eine im Gebrauch befindliche Datei zu sichern oder zu archivieren, wiederholen soll. Diese Option ist in den Befehlen **archive**, **incremental** und **selective** zu verwenden.

Diese Option ist nur dann zu verwenden, wenn für die Kopiennummerierung (ein Attribut in der Kopiengruppe einer Verwaltungsklasse) Gemeinsam statisch oder Gemeinsam dynamisch angegeben wird.

Ist eine Datei bei der Durchnummerierung Gemeinsam statisch während einer Operation geöffnet, wird die Operation so oft wiederholt, wie Sie angegeben. Ist die Datei bei jedem Versuch geöffnet, wird die Operation nicht durchgeführt.

Ist eine Datei bei der Durchnummerierung Gemeinsam dynamisch während einer Operation geöffnet, wird die Operation so oft wiederholt, wie Sie angeben. Die Sicherung oder Archivierung wird beim letzten Versuch durchgeführt, unabhängig davon, ob die Datei geöffnet ist.

Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Sichern** im Feld **Anzahl Wiederholungen, wenn Datei im Gebrauch ist** des Profileditors definieren.

Syntax

►—CHangingretries— *Anzahl Wiederholungen* —►

Parameter

Anzahl Wiederholungen

Gibt an, wie oft ein Sicherungs- oder Archivierungsversuch wiederholt wird, wenn die Datei im Gebrauch ist. Der Wertebereich ist 0 bis 4; Standardwert ist 4.

Beispiele

Optionsdatei:

```
changingretries 3
```

Befehlszeile:

```
-cha=3
```

Class

Die Option **class** gibt an, ob bei Verwendung der Befehle **delete filespace**, **query backup** und **query filespace** eine Liste der NAS- oder der Clientobjekte angezeigt werden soll.

Wenn Sie z. B. eine Liste der Dateibereiche anzeigen wollen, die zu einem NAS-Knoten gehören, geben Sie folgenden Befehl ein:

```
query filespace -class=nas
```

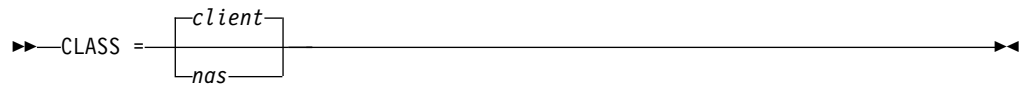
Unterstützte Clients

Diese Option ist nur für AIX-, Linux- und Oracle Solaris-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Keine. Sie können diese Option nur in der Befehlszeile angeben.

Syntax



Parameter

client

Gibt an, dass Sie eine Liste der Dateibereiche für einen Clientknoten anzeigen wollen. Dies ist der Standardwert.

nas

Gibt an, dass Sie eine Liste der Dateibereiche für einen NAS-Knoten anzeigen wollen.

Beispiele

Keine. Sie können diese Option nur in der Befehlszeile angeben.

Befehlszeile:

```
q backup -nasnodename=Knotenname -class=nas
```

Collocatebyfilespec

Verwenden Sie die Option `collocatebyfilespec`, um anzugeben, ob der Client für Sichern/Archivieren nur eine Serversitzung verwenden soll, um Objekte zu senden, die von einer einzigen Dateispezifikation generiert wurden.

Durch das Setzen der Option `collocatebyfilespec` auf `yes` wird versucht, das Durchsetzen von Dateien von unterschiedlichen Dateispezifikationen zu eliminieren, indem der Client auf eine Serversitzung pro Dateispezifikation begrenzt wird. Wenn Sie Daten auf Band speichern, werden Dateien für jede Dateispezifikation deshalb zusammen auf einem Band gespeichert (sofern auf Grund erhöhter Kapazität kein weiteres Band erforderlich ist).

Hinweise:

- Verwenden Sie die Option `collocatebyfilespec` nur, wenn der Speicherpool direkt auf Band geht. Wenn Sie diese Option für einen Plattenspeicherpool verwenden, könnte dies den Lastausgleich und somit das Leistungsverhalten negativ beeinflussen.

Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (`dsm.opt`) ein.

Syntax



Parameter

Yes

Gibt an, ob der Client nur eine Serversitzung verwenden soll, um Objekte zu senden, die von einer einzigen Dateispezifikation generiert wurden. Wenn Sie Daten auf Band speichern, werden Dateien für jede Dateispezifikation deshalb zusammen auf einem Band gespeichert, sofern auf Grund erhöhter Kapazität kein weiteres Band erforderlich ist. Als Ergebnis kann sich die Leistung beim Zurückschreiben erhöhen.

No Gibt an, dass der Client (abhängig von der Ausführungsdynamik und der Einstellung der Option `resourceutilization` auf 3 oder höher) mehrere Serversitzungen verwenden kann, um die Dateien von einer Dateispezifikation zu senden. Dies ist der Standardwert.

Als Ergebnis kann sich die Leistung beim Sichern erhöhen. Wenn die Dateien auf Band gesichert werden, werden sie auf mehreren Bändern gespeichert. Im Allgemeinen sind die in der Dateispezifikation angegebenen Dateien trotzdem zusammenhängend.

Beispiele

Optionsdatei:

```
collocatebyfilespec yes
```

Befehlszeile:

```
-collocatebyfilespec=yes
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Commmethod

Mit der Option `commmethod` wird die verwendete Übertragungsmethode für die Konnektivität der Client/Server-Übertragung angegeben.

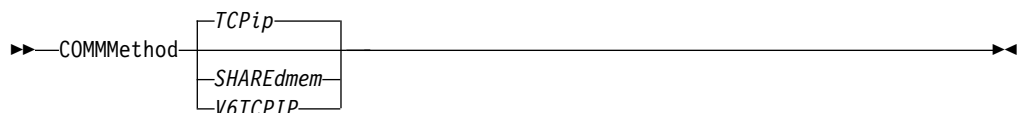
Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Übertragung** des Profileditors definieren.

Syntax



Parameter

TCPip

Die Übertragungsmethode Transmission Control Protocol/Internet Protocol (TCP/IP). Dies ist der Standardwert.

V6Tcip

Gibt an, dass abhängig von der Systemkonfiguration und den Ergebnissen einer DNS-Suche (Domain Name Service - Domännennamensservice) entweder TCP/IP V4 oder V6 verwendet werden soll. Es muss eine gültige DNS-Umgebung verfügbar sein.

SHAREdmem

Die Übertragungsmethode Shared Memory ist zu verwenden, wenn der Client und der Server in demselben System aktiv sind. Dies ermöglicht eine bessere Leistung als das TCP/IP-Protokoll.

Diese Option ist für AIX-, Linux- und Oracle Solaris-Clients gültig.

Wenn Sie diese Übertragungsmethode unter AIX angeben, kann der Client als Root oder Nicht-Root angemeldet sein, solange der Server als Root ausgeführt wird. Wird der Server nicht als Root ausgeführt, muss die Benutzer-ID, die den Client ausführt, mit der Benutzer-ID, die den Server ausführt, übereinstimmen.

Wichtig: Bei Verwendung von `commethod sharedmem` unter Linux wird möglicherweise die Fehlermeldung ANR8294W Shared Memory-Sitzung kann nicht initialisiert werden auf der Konsole des Servers oder Speicheragenten ausgegeben. Standardmäßig ist Linux nicht mit genügend Systemressourcen konfiguriert, um die Nachrichtenwarteschlangen zu erstellen. Sie müssen den Kernelparameter MSGMNI auf 128 erhöhen (der Standardwert ist 16). Sie können diesen Parameter ändern, indem Sie den folgenden Befehl ausführen:

```
echo 128 > /proc/sys/kernel/msgmni
```

Damit dieser Parameter auch nach einem Warmstart für das System permanent beibehalten wird, können Sie stattdessen die folgende Zeile der Datei `/etc/sysctl.conf` hinzufügen und dann einen Warmstart für das System durchführen:

```
kernel.msgmni=128
```

Um die aktuelle ipc-Einstellungen anzuzeigen, führen Sie diesen Befehl aus:

```
ipcs -l
```

Schauen Sie sich jetzt den Wert `max queues system wide` an. Der Standardwert ist 16.

Beispiele

Optionsdatei:

Nur TCP/IP V4 verwenden.

```
commethod tcpip
```

Sowohl TCP/IP V4 als auch V6 verwenden, abhängig von der Systemkonfiguration und den Ergebnissen einer DNS-Suche.

```
commethod V6Tcip
```

Anmerkung: Der Befehl `'dsmc schedule'` kann nicht verwendet werden, wenn `SCHEDMODE` prompt und `commethod V6Tcip` angegeben sind.

Befehlszeile:

```
-comm=tcpip
```

```
-comm=V6Tcip
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Commrestartduration

Mit der Option `commrestartduration` wird die maximale Anzahl Minuten angegeben, die der Client nach einem Übertragungsfehler zwischen Versuchen, die Verbindung zum IBM Spectrum Protect-Server wiederherzustellen, warten soll.

Anmerkung: Ein geplantes Ereignis wird fortgesetzt, wenn der Client die Verbindung zum Server wiederherstellt, bevor der Wert für `commrestartduration` abläuft; dies ist selbst dann der Fall, wenn das Startfenster des Ereignisses abgelaufen ist.

Sie können die Optionen `commrestartduration` und `commrestartinterval` in ausgelasteten oder nicht stabilen Netzumgebungen verwenden, um Verbindungsfehler zu verringern.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Übertragung** im Abschnitt **Allgemeine Optionen** des Profileditors definieren.

Syntax

►►—`COMMRESTARTDuration—Minuten`—►►

Parameter

Minuten

Die maximale Anzahl Minuten, die der Client nach einem Übertragungsfehler versuchen soll, die Verbindung zu einem Server wiederherzustellen. Der Wertebereich ist 0 bis 9999; Standardwert ist 60.

Beispiele

Optionsdatei:

```
commrestartduration 90
```

Befehlszeile:

Nicht zutreffend.

Commrestartinterval

Mit der Option `commrestartinterval` wird die Anzahl Sekunden angegeben, die der Client nach einem Übertragungsfehler zwischen Versuchen, die Verbindung zum IBM Spectrum Protect-Server wiederherzustellen, warten soll.

Anmerkung: Verwenden Sie diese Option nur, wenn für `commrestartduration` ein Wert größer als Null definiert ist.

Sie können die Optionen `commrestartduration` und `commrestartinterval` in ausgelasteten oder nicht stabilen Netzumgebungen verwenden, um Verbindungsfehler zu verringern.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Übertragung** im Abschnitt **Allgemeine Optionen** des Profileditors definieren.

Syntax

►—COMMRESTARTInterval— *Sekunden* —►

Parameter

Sekunden

Die Anzahl Sekunden, die der Client nach einem Übertragungsfehler zwischen den Versuchen, die Verbindung zu einem Server wiederherzustellen, warten soll. Der Wertebereich ist 0 bis 65535; Standardwert ist 15.

Beispiele

Optionsdatei:

commrestartinterval 30

Befehlszeile:

Nicht zutreffend.

Compressalways

Die Option compressalways gibt an, ob die Komprimierung eines Objekts fortgesetzt wird, wenn es während der Komprimierung größer wird.

Verwenden Sie diese Option mit der Option compression und in den Befehlen **archive**, **incremental** und **selective**.

Die Option compressalways wird ignoriert, wenn die clientseitige Deduplizierung aktiviert ist.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte **Sichern** über das Kontrollkästchen **Komprimieren, wenn Objekt anwächst** im Profileditor definieren.

Syntax

►—COMPRESSAlways—

Yes
No

 —►

Parameter

Yes

Die Komprimierung der Datei wird fortgesetzt, auch wenn die Datei durch die Komprimierung größer wird. Dies ist der Standardwert.

No Objekte des Clients für Sichern/Archivieren werden dekomprimiert erneut gesendet, wenn sie während der Komprimierung größer werden. Das API-Verhalten ist von der Anwendung abhängig. Anwendungssicherungen können fehlschlagen.

Beispiele

Optionsdatei:

`compressalways yes`

Befehlszeile:

`-compressa=no`

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Compression

Die Option `compression` komprimiert Dateien, bevor sie an den Server gesendet werden.

Die Komprimierung der Dateien reduziert den erforderlichen Datenspeicherplatz für Sicherungsversionen und Archivierungskopien der Dateien. Das Komprimieren kann sich jedoch auf den IBM Spectrum Protect-Durchsatz auswirken. Bei einem schnellen Prozessor und einer langsamen Netzverbindung ist die Komprimierung von Vorteil, bei einem langsamen Prozessor und einer schnellen Netzverbindung nicht.

Verwenden Sie die Option `compression` in den Befehlen **archive**, **incremental** und **selective**.

Der Befehl **backup image** verwendet den Wert der Option `compression`, der in der Datei `dsm.sys` angegeben ist. Diese Option ist in der Anfangsbefehlszeile und im interaktiven Modus gültig. Diese Option kann auch auf dem Server definiert werden; sie überschreibt dann den Clientwert.

Der Client für Sichern/Archivieren sichert eine Datei mit freien Bereichen als reguläre Datei, wenn die Clientkomprimierung inaktiviert ist. Legen Sie `compression yes` fest, um die Dateikomprimierung bei der Sicherung von Dateien mit freien Bereichen zu aktivieren und dadurch die Netzübertragungszeit zu verringern und den Serverspeicherbereich zu vergrößern.

Wenn Sie `compressalways yes` festlegen, wird die Komprimierung fortgesetzt, selbst wenn die Dateigröße zunimmt. Soll die Komprimierung gestoppt werden, wenn die Dateigröße zunimmt, und soll die Datei dekomprimiert erneut gesendet werden, müssen Sie `compressalways no` festlegen.

Wenn Sie `compression yes` festlegen, können Sie die Komprimierungsverarbeitung auf folgende Weise steuern:

- Verwenden Sie die Option `exclude.compression` in Ihrer Clientsystemoptionsdatei (`dsm.sys`), um bestimmte Dateien oder Dateigruppen von der Komprimierungsverarbeitung auszuschließen.

- Verwenden Sie die Option `include.compression` in Ihrer Clientsystemoptionsdatei (`dsm.sys`), um Dateien innerhalb einer großen Gruppe ausgeschlossener Dateien für die Komprimierungsverarbeitung einzuschließen.

Mit dieser Option kann die Komprimierung nur dann gesteuert werden, wenn Ihr Administrator angibt, dass Ihr Clientknoten Dateien komprimieren kann, bevor sie an den Server gesendet werden.

Der Komprimierungstyp, den der Client verwendet, wird durch die Kombination von Komprimierung und clientseitiger Datendeduplizierung bestimmt, die während der Sicherungs- oder Archivierungsverarbeitung verwendet wird. Die folgenden Komprimierungstypen werden verwendet:

- LZ4** Eine schnellere und effizientere Komprimierungsmethode, die der Client verwendet, wenn vom Client deduplizierte Daten an einen LZ4-kompatiblen Containerspeicherpool auf dem IBM Spectrum Protect-Server gesendet werden. Der Server muss Version 7.1.5 oder höher haben und Containerspeicherpools verwenden. Die clientseitige LZ4-Komprimierung wird nur verwendet, wenn die clientseitige Datendeduplizierung aktiviert ist.
- LZW** Ein traditioneller Komprimierungstyp, den der Client in den folgenden Situationen verwendet:
 - Vom Client deduplizierte Daten werden an traditionelle (Nicht-Container) Speicherpools auf dem Server gesendet.
 - Für die Clientdaten wird keine clientseitige Datendeduplizierung ausgeführt. (Gilt nicht für Data Protection for VMware und Data Protection for Microsoft Hyper-V, bei denen nur vom Client deduplizierte Daten komprimiert werden können.)
 - Für die Clientdaten wird nur eine traditionelle serverseitige Datendeduplizierung ausgeführt. (Gilt nicht für Data Protection for VMware und Data Protection for Microsoft Hyper-V, bei denen nur vom Client deduplizierte Daten komprimiert werden können.)
- Keine** Das Objekt wird vom Client nicht komprimiert. Das Objekt wird nicht komprimiert, da die Option `compression` auf `no` gesetzt ist oder die Option während der Sicherungs- oder Archivierungsverarbeitung nicht angegeben wird. Auch wenn das Objekt nicht vom Client komprimiert wird, kann es vom Server komprimiert werden.

Sie müssen den Komprimierungstyp nicht definieren. Er wird vom Client für Sichern/Archivieren während der Sicherungs- oder Archivierungsverarbeitung bestimmt.

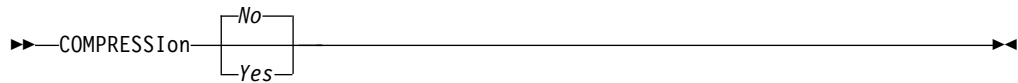
Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Datei `dsm.sys` innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Sichern** über das Kontrollkästchen **Objekte komprimieren** im Profileditor definieren.

Syntax



Parameter

No Dateien werden nicht komprimiert, bevor sie an den Server gesendet werden. Dies ist der Standardwert.

Yes

Dateien werden komprimiert, bevor sie an den Server gesendet werden.

Beispiele

Optionsdatei:

compression yes

Befehlszeile:

-compressi=no

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Zugehörige Verweise:

„Deduplication“ auf Seite 394

„Exclude-Optionen“ auf Seite 438

„Include-Optionen“ auf Seite 473

Console

Verwenden Sie die Option **console** im Befehl **query systeminfo**, um Informationen an der Konsole auszugeben.

- DSMOPTFILE - Der Inhalt der Datei dsm.opt
- DSMSYSFILE - Inhalt der Datei dsm.sys
- ENV - Umgebungsvariablen
- ERRORLOG - IBM Spectrum Protect-Fehlerprotokolldatei
- FILE - Attribute für den angegebenen Dateinamen.
- INCLEXCL - Stellt eine Liste der Include/Exclude-Anweisungen in der Reihenfolge zusammen, in der sie bei Sicherungs- und Archivierungsoperationen verarbeitet werden.
- OPTIONS - Optionen
- OSINFO - Name und Version des Clientbetriebssystems (umfasst ULIMIT-Informationen für UNIX und Linux).
- POLICY - Speicherauszug der Maßnahmengruppe
- SCHEDLOG - Inhalt des IBM Spectrum Protect-Planungsprotokolls (normalerweise dsmsched.log).
- CLUSTER - AIX-Clusterinformationen

Anmerkung: Der Befehl **query systeminfo** ist in erster Linie als Hilfe für die IBM Unterstützungsfunktion bei der Diagnose von Problemen gedacht. Aber Benutzer, die mit den in diesen Informationen angesprochenen Konzepten vertraut sind, finden ihn möglicherweise auch nützlich. Wenn Sie die Option **console** verwenden, wird keine besondere Formatierung der Ausgabe ausgeführt, um die Anzeigenhöhe

oder -breite anzupassen. Aus diesem Grund ist die Konsolausgabe wegen der Länge und des Zeilenumbruchs unter Umständen schwierig zu lesen. In diesem Fall verwenden Sie die Option `filename` mit dem Befehl **query systeminfo**, damit die Ausgabe in eine Datei geschrieben wird, die anschließend an die IBM Unterstützungsfunktion übergeben werden kann.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Syntax

►►—console—►►

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
query systeminfo dsmpoptfile errorlog -console
```

Zugehörige Informationen

„Filename“ auf Seite 456

Createnewbase

Die Option `createnewbase` erstellt eine Basismomentaufnahme und verwendet sie als Quelle für die Ausführung einer vollständigen Teilsicherung.

Einige Dateien werden möglicherweise nicht gesichert, wenn der Befehl zur Ausführung einer Teilsicherung unter Verwendung der Momentaufnahmedifferenz ausgeführt wird. Werden die Dateien übersprungen, können Sie mit der Option `createnewbase` eine Teilsicherung unter Verwendung der Momentaufnahmedifferenz ausführen, um diese Dateien zu sichern. Der Abschnitt „Snapdiff“ auf Seite 581 enthält eine Liste mit Gründen, die angeben, warum eine Datei möglicherweise nicht gesichert wird, wenn der Befehl zur Ausführung einer Teilsicherung unter Verwendung der Momentaufnahmedifferenz ausgeführt wird.

Ein Grund, dass eine Datei während der Sicherungsverarbeitung übersprungen werden kann, liegt darin, dass der Dateiname von NetApp Data ONTAP nicht unterstützt wird. NetApp Data ONTAP-Version 8.0 und Versionen vor Version 7.3.3 unterstützen nur Dateinamen, die sich innerhalb des 7-Bit-ASCII-Z Zeichensatzes befinden. NetApp Data ONTAP-Version 7.3.3 und Versionen höher als 8.0.0 unterstützen Unicode-Dateinamen. Wenn Sie für NetApp Data ONTAP ein Upgrade von einer Version, die keine Unicode-Dateinamen unterstützt, auf eine Version durchgeführt haben, die Unicode-Dateinamen unterstützt, führen Sie eine vollständige Teilsicherung mit der Option `createnewbase=migrate` aus.

Unterstützte Clients

Diese Option ist für die folgenden Clients gültig:

- Linux x86_64-Clients

Geben Sie die Option `createnewbase` in der Befehlszeile ein. Geben Sie diese Option mit der Option `snaptiff` an.

Syntax



Parameter

No Gibt an, dass eine Teilsicherung unter Verwendung der Momentaufnahme-differenz ausgeführt wird. Wenn der Client für Sichern/Archivieren feststellt, dass der NetApp Data ONTAP-Dateiserver von einer Version, die keine Unicode-Dateinamen unterstützt, auf einen Dateiserver migriert wurde, der Unicode-Dateinamen unterstützt, wird eine Warnung im Fehlerprotokoll und im IBM Spectrum Protect-Serveraktivitätenprotokoll aufgezeichnet. Die Warnung gibt an, dass eine vollständige Teilsicherung ausgeführt werden muss, und protokolliert den Rückkehrcode 8, auch wenn die Operation erfolgreich ausgeführt wurde.

Dieser Parameter ist der Standardwert.

Yes

Gibt an, dass eine vollständige Teilsicherung ausgeführt wird, indem eine neue Basismomentaufnahme erstellt und diese für die Ausführung einer scanbasierten Teilsicherung verwendet wird. Verwenden Sie diese Option, um alle Dateiänderungen zu sichern, die von der Momentaufnahme-differenz-API möglicherweise nicht festgestellt wurden.

Wird die Operation erfolgreich beendet, endet der Befehl mit dem Rückkehrcode 0.

Geben Sie die Option `createnewbase=yes` nicht für einen Zeitplan an, mit dem eine tägliche Momentaufnahme-differenzsicherung ausgeführt wird. Erstellen Sie stattdessen einen separaten monatlichen Zeitplan, der über die Option `createnewbase=yes` verfügt.

IGNore

Gibt an, dass eine Teilsicherung unter Verwendung der Momentaufnahme-differenz ausgeführt wird, wenn der Client für Sichern/Archivieren feststellt, dass für den NetApp Data ONTAP-Dateiserver ein Upgrade zur Unterstützung von Unicode-Dateinamen durchgeführt wurde.

Die Option `ignore` unterscheidet sich vom Parameter `no`, da mit der Option `ignore` die Warnung unterdrückt wird. Stattdessen wird im Fehlerprotokoll und im IBM Spectrum Protect-Aktivitätenprotokoll eine Informationsnachricht aufgezeichnet, die angibt, dass eine vollständige Teilsicherung ausgeführt werden soll.

Wird der Befehl erfolgreich beendet, wird der Code 0 zurückgegeben.

Verwenden Sie die Option `ignore`, wenn Sie für den NetApp Data ONTAP-Dateiserver ein Upgrade zur Unterstützung von Unicode durchgeführt, aber noch keine vollständige Teilsicherung ausgeführt haben. Diese Option wird nur verwendet, wenn der Client für Sichern/Archivieren festgestellt hat, dass der Dateiserver migriert und noch keine vollständige Teilsicherung ausgeführt wurde. Zu allen anderen Zeiten wird die Option ignoriert.

MIGRate

Gibt an, dass eine Basismomentaufnahme erstellt und eine scanbasierte Teilsicherung ausgeführt wird, wenn für den NetApp Data ONTAP-Dateiserver ein Upgrade auf eine Version durchgeführt wurde, die Unicode-Dateinamen unterstützt. Die Option migrate unterscheidet sich von der Option yes, da die Option migrate eine Basismomentaufnahme nur erstellt, wenn der Client erkennt, dass die Version des NetApp Data ONTAP-Dateiservers aktualisiert wurde. Mit der Option yes wird bei jeder Ausführung des Befehls eine Basismomentaufnahme erstellt.

Nach der Ausführung der Teilsicherung werden keine zusätzlichen migrationsbezogenen Nachrichten im Fehlerprotokoll oder im Aktivitätenprotokoll des IBM Spectrum Protect-Servers aufgezeichnet. Wird die Operation ausgeführt, wird der Befehl mit dem Rückkehrcode 0 beendet.

Verwenden Sie die Option migrate, wenn Sie für den NetApp Data ONTAP-Dateiserver ein Upgrade zur Unterstützung von Unicode durchgeführt, aber noch keine vollständige Teilsicherung ausgeführt haben. Die Option migrate wird ignoriert, wenn für den NetApp Data ONTAP-Dateiserver kein Upgrade durchgeführt wurde.

Beispiele

Befehlszeile:

```
dsmc incremental -snapdiff -createnewbase=yes /net/home1
```

Zugehörige Tasks:

„NetApp und IBM Spectrum Protect für Teilsicherungen unter Verwendung der Momentaufnahme-Differenz konfigurieren“ auf Seite 119

Zugehörige Verweise:

„Snapdiff“ auf Seite 581

Csv

Mit der Option csv kann auf einem Client eine Datei mit durch Kommas getrennten Werten (CSV-Datei) verwendet werden, um verschiedene Zurückschreibungseinstellungen für eine Reihe von Zurückschreibungsoperationen für virtuelle Maschinen zu definieren und anzuwenden.


In der angegebenen .csv-Datei können Sie Spaltenüberschriften mit Einstellungen definieren, die die entsprechenden Clientoptionen außer Kraft setzen. Bei Spaltennamen muss die Groß-/Kleinschreibung beachtet werden.

Durch die Verwendung einer CSV-Spalte wird die entsprechende Befehlszeilenoption außer Kraft gesetzt. Die entsprechende Option wird ignoriert, wenn sie mit dem Befehl restore vm -csv verwendet wird:

- "New Virtual Machine Name" setzt die Option -vmname bei der Zurückschreibung außer Kraft.
- "New Datastore" setzt die Option -datastore bei der Zurückschreibung außer Kraft.
- "New Datacenter" setzt die Option -datacenter bei der Zurückschreibung außer Kraft.
- "New Host" setzt die Option -host bei der Zurückschreibung außer Kraft.
- "PITDATE" setzt die Option -pitdate bei der Zurückschreibung außer Kraft.
- "PITTIME" setzt die Option -pittime bei der Zurückschreibung außer Kraft.

Unterstützte Clients

Diese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

 Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Optionsdatei

Diese Option ist in der Clientsystemoptionsdatei (dsm.sys) und in der Befehlszeile für **Restore VM** gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profileditor definiert werden.

Syntax

►► —Csv— —CSV-Dateispezifikation— ◀◀

Parameter

CSV-Dateispezifikation

Durch die Verwendung einer CSV-Spalte wird die entsprechende Befehlszeilenoption außer Kraft gesetzt. Jede entsprechende Option wird ignoriert, wenn sie mit dem Befehl `restore vm -csv` verwendet wird.

Geben Sie beispielsweise den Befehl `restore vm "restore_vm_list.csv" -csv -datacenter="Mambo 5"` an und ist die Spalte "Neues Datencenter" bereits in der CSV-Datei angegeben, wird die Option `-datacenter` ignoriert.

Die folgende Liste enthält die CSV-Spalten, die die entsprechenden Clientoptionen außer Kraft setzen:

Tabelle 71. Namen der Spaltenüberschriften

Überschrift	Beschreibung	Verwendung
Virtual Machine Name	Der Name der virtuellen Maschine, die zurückgeschrieben werden soll.	Platzhalterzeichen sind nicht zulässig. Groß-/Kleinschreibung muss beachtet werden. Diese Spalte ist obligatorisch.
New Virtual Machine Name	Der Name der virtuellen Maschine, die zurückgeschrieben wird.	Für diese Spalte gilt dieselbe Syntax wie für die Option '-vmname'. Optional. Sie können diese Spalte leer lassen, wenn Sie den bestehenden Namen wiederverwenden möchten.
New Datastore	Der neue Datenspeicher, in den die virtuellen Festplatten zurückgeschrieben werden.	Für diese Spalte gilt dieselbe Syntax wie für die Option '-datastore'. Optional. Sie können diese Spalte leer lassen, wenn Sie den bestehenden Datenspeicher wiederverwenden möchten.

Tabelle 71. Namen der Spaltenüberschriften (Forts.)

Überschrift	Beschreibung	Verwendung
New Datacenter	Das neue Datacenter, dem die virtuelle Maschine zugeordnet werden soll.	Es gilt dieselbe Syntax wie für die Option '-datacenter'. Optional. Sie können diese Spalte leer lassen, wenn Sie das bestehende Datacenter wiederverwenden möchten.
New Host	Der neue Host, auf den die virtuelle Maschine zurückgeschrieben wird.	Für diese Spalte gilt dieselbe Syntax wie für die Option '-host'. Optional. Sie können diese Spalte leer lassen, wenn Sie den bestehenden Host wiederverwenden möchten.
PITDATE	Das Datum des Zeitpunkts, mit dem die Sicherung angegeben wird.	Für diese Spalte gilt dieselbe Syntax wie für die Option '-pitdate'. Optional. Sie können diese Spalte leer lassen, um anzugeben, dass die aktive Sicherung zurückgeschrieben werden soll. Diese Spalte ist erforderlich, wenn PITTIME in der CSV-Datei angegeben wird. Für Datumsangaben für PITDATE muss das Format verwendet werden, das durch die Option DATEFORMAT definiert ist. Unter Windows variiert der Standardwert je nach Ländereinstellung. Unter Linux ist der Standardwert DATEFORMAT 1.
PITTIME	Die Uhrzeit des Zeitpunkts, mit dem die Sicherung angegeben wird.	Für diese Spalte gilt dieselbe Syntax wie für die Option '-pittime'. Optional. Sie können diese Spalte leer lassen, um anzugeben, dass die aktive Sicherung verwendet werden soll, oder wenn nur PITDATE angegeben wird. Für Zeitangaben für PITTIME muss das Format verwendet werden, das durch die Option TIMEFORMAT definiert ist. Unter Windows variiert der Standardwert je nach Ländereinstellung. Unter Linux ist der Standardwert TIMEFORMAT 1.

Der Stern, *, gibt als Bestandteil eines Platzhalterkonstrukts die Wiederverwendung des ursprünglichen VM-Namens für den Namen einer zurückgeschriebenen VM an.

Darüber hinaus gelten die folgenden Befehlszeilenkonventionen:

- **<date>** wird durch das Datum der Zurückschreibung ersetzt.
- **<time>** wird durch die Uhrzeit der Zurückschreibung ersetzt.
- **<timestamp>** wird durch eine Kombination der Ausgaben von **<date>** und **<time>** ersetzt.

Elemente können in Anführungszeichen eingeschlossen werden, beispielsweise VMs, deren Namen Kommas und Anführungszeichen enthalten.

"Poem Repository "A-F" 20th Century"

Hier werden doppelte Anführungszeichen verwendet, um ein Zeichen " (Anführungszeichen) auszudrücken.

Beispiele

Das folgende Beispiel zeigt eine CSV-Datei, die in einer Arbeitsblattansicht geöffnet ist:

Virtual Machine Name	New Virtual Machine Name	New Host	New Datastore	New Datacenter	NOTES1	NOTES2	PITDATE	PITTIME
VM1	*-DR_restore		esx4.ibm.com	DS_8	DC_RecoverSite1	group1		
VM2	*-DR_restore		esx4.ibm.com	DS_8	DC_RecoverSite1	group1		
VM3	*-DR_restore		esx4.ibm.com	DS_8	DC_RecoverSite1	group1		
VM4	*-DR_restore		esx5.ibm.com	DS_10	DC_RecoverSite1	group2		
VM5	*-DR_restore		esx5.ibm.com	DS_10	DC_RecoverSite1	group2		

Das folgende Beispiel zeigt Textdateien mit durch Kommas getrennten Werten, die aus CSV-Dateien exportiert wurden.

Beispiel 1:

```
Virtual Machine Name,New Virtual Machine Name,New Host,New Datastore,New Datacenter,NOTES1,NOTES2,PITDATE,PITTIME
VM1,*-DR_restore,esx4.ibm.com,DS_8,DC_RecoverSite1,group1
VM2,*-DR_restore,esx4.ibm.com,DS_8,DC_RecoverSite1,group1
VM3,*-DR_restore,esx4.ibm.com,DS_8,DC_RecoverSite1,group1
VM4,*-DR_restore,esx5.ibm.com,DS_10,DC_RecoverSite1,group2
VM5,*-DR_restore,esx5.ibm.com,DS_10,DC_RecoverSite1,group2
```

Beispiel 2:

```
Virtual Machine Name,New Virtual Machine Name,New Host,New Datastore,New Datacenter,NOTES1,NOTES2,PITDATE,PITTIME
Tiny Linux VM,Tiny Linux VM -restore,,,,,,
lucasTestVM10,* -restore,,,,,10/03/2017,10:35 AM
big-cet-4TB,,devesx06.storage.tucson.ibm.com,,,10/05/2017,,
```

Zugehörige Verweise:

„Restore VM“ auf Seite 791

Datacenter

Gibt die Zielposition des Datacenters an, das die zurückgeschriebenen Maschinendaten enthalten soll.

Verwenden Sie diese Option in Befehlen **restore vm**.

Werden Ordner innerhalb des Virtual Center verwendet, um Datacenter zu organisieren, muss der Ordnername in die Datacenterspezifikation (durch einen Schrägstrich getrennt) eingeschlossen werden.

Erfolgt die Zurückschreibung über einen ESX-Server anstelle eines Virtual Center, sollte die Option '-datacenter=ha-datacenter' verwendet werden.

Die Standardzielposition ist das Datacenter, in dem die virtuelle Maschine zum Zeitpunkt der Sicherung gespeichert wurde.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Beispiele

Eine virtuelle Maschine in das Datacenter 'USEast' zurückschreiben, das sich unter einem Ordner mit dem Namen 'Production' im Virtual Center befindet.

```
dsmc restore vm my_vm -datacenter=Production/USEast
```

Die Sicherung einer virtuellen Maschine, die im Virtual Center erstellt wurde, unter Verwendung eines ESX-Servers zurückschreiben.

```
restore vm my_vm -datacenter=ha-datacenter
```

Die virtuelle Maschine in das Datacenter 'USWest' zurückschreiben.

```
restore vm my_vm -datacenter=USWest
```

Datastore

Gibt das Datenspeicherziel an, das während der VMware-Zurückschreibungsoperation verwendet werden soll.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Beispiel

Die virtuelle Maschine in einen Datenspeicher mit dem Namen ds8k_prod1 zurückschreiben:

```
restore vm my_vm -datastore=ds8k_prod1
```

Dateformat

Mit der Option `dateformat` wird das Format angegeben, das für die Anzeige oder Eingabe von Datumsangaben verwendet werden soll.

Der Client für Sichern/Archivieren und der Verwaltungsclient erhalten standardmäßig Formatinformationen aus der Ländereinstellungsdefinition, die beim Starten des Clients aktiv ist. Ausführliche Informationen zur Definition der länderspezifischen Angaben können der Dokumentation auf dem lokalen System entnommen werden.

Anmerkung:

1. Die Option `dateformat` betrifft nicht den Web-Client. Der Web-Client verwendet das Datumsformat der Ländereinstellung, die im Browser aktiv ist. Ist im Browser eine Ländereinstellung aktiv, die nicht unterstützt wird, verwendet der Web-Client das Datumsformat für amerikanisches Englisch.
2. Wenn Sie das Datumsformat ändern und mit der Option `schedlogretention` das Planungsprotokoll bereinigen, entfernt der Client während der Protokollbereinigung alle Einträge im Planungsprotokoll mit einem anderen Datumsformat. Wenn Sie das Datumsformat ändern und das Fehlerprotokoll mit der Option `errorlogretention` bereinigen, entfernt der Client während der Protokollbereinigung alle Einträge im Fehlerprotokoll mit einem anderen Datumsformat. Bei einer Änderung des Datumsformats müssen das Planungs- und das Fehlerprotokoll kopiert werden, wenn Protokolleinträge mit einem anderen Datumsformat aufbewahrt werden sollen.

Sie können die Option `dateformat` mit den folgenden Befehlen verwenden.

- delete archive
- delete backup
- expire
- query archive
- query backup
- query filespace
- query image
- restore
- restore image
- restore nas
- retrieve
- set event

Wenn Sie die Option `dateformat` in einem Befehl angeben, muss sie vor den Optionen `fromdate`, `pitdate` und `todate` stehen.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (`dsm.opt`) ein. Sie können diese Option auf der Registerkarte **Regionale Einstellungen** in der Dropdown-Liste **Datumsformat** im Profileditor definieren.

Syntax

►►—`DATEformat`— —*Formatnummer*—►►

Parameter

Formatnummer

Zeigt das Datum in einem der folgenden Formate an. Die Nummer für das Datumsformat auswählen, das verwendet werden soll:

- 0** Das durch die Ländereinstellung festgelegte Datumsformat verwenden (gilt nicht für Mac OS X).

Für AIX und Solaris: Dies ist der Standardwert, wenn das durch die Ländereinstellung festgelegte Datumsformat aus Ziffern und Trennzeichen besteht.

- 1** MM/TT/JJJJ

Für AIX und Solaris: Dies ist der Standardwert, wenn das durch die Ländereinstellung festgelegte Datumsformat nicht aus Ziffern und Trennzeichen besteht.

Dies ist der Standardwert für die folgenden verfügbaren Übersetzungen:

- Amerikanisches Englisch
- Traditionelles Chinesisch
- Koreanisch

- 2** TT-MM-JJJJ

Dies ist der Standardwert für die folgenden verfügbaren Übersetzungen:

- Brasilianisches Portugiesisch
- Italienisch

- 3** JJJJ-MM-TT

Dies ist der Standardwert für die folgenden verfügbaren Übersetzungen:

- Japanisch
- Vereinfachtes Chinesisch
- Polnisch

4 TT.MM.JJJJ

Dies ist der Standardwert für die folgenden verfügbaren Übersetzungen:

- Deutsch
- Französisch
- Spanisch
- Tschechisch
- Russisch

5 JJJJ.MM.TT

Dies ist der Standardwert für die folgenden verfügbaren Übersetzungen:

- Ungarisch

6 JJJJ/MM/TT

7 TT/MM/JJJJ

Beispiele

Optionsdatei:

dateformat 3

Befehlszeile:

-date=3

Diese Option ist in der Anfangsbefehlszeile und im interaktiven Modus gültig. Wird die Option im interaktiven Modus eingegeben, ist nur der Befehl betroffen, mit dem sie eingegeben wird. Wenn dieser Befehl beendet ist, wird der Wert auf den Wert zu Beginn der interaktiven Sitzung zurückgesetzt. Dies ist der Wert aus der Datei dsm.opt, sofern er nicht durch die Anfangsbefehlszeile oder eine vom Server erzwungene Option überschrieben wurde.

Weitere Hinweise zur Angabe von Datums- und Zeitformaten

Das Datums- oder Zeitformat, das Sie mit dieser Option angeben, muss verwendet werden, wenn Optionen verwendet werden, deren Eingabe aus Datums- und Zeitangaben besteht. Beispiele sind: totime, fromtime, todate, fromdate und pittime.

Wenn Sie beispielsweise die Option timeformat als TIMEFORMAT 4 angeben, muss der Wert, den Sie für die Option fromtime oder totime angeben, als Zeit angegeben werden, wie z. B. 12:24:00pm. Die Angabe 13:24:00 wäre nicht gültig, da TIMEFORMAT 4 als Angabe für die Stunde eine ganze Zahl, die kleiner-gleich 12 ist, erfordert. Wenn in einer Option für die Stunde Werte bis zu 24 angegeben und Kommas als Trennzeichen verwendet werden sollen, müssen Sie TIMEFORMAT 2 angeben.

Datums- und Zeitformate in der Konfigurationsdatei für die Systemländereinstellung konfigurieren

Sie können Datums- und Zeitformate angeben, indem Sie diese in der Ländereinstellungsdatei des Systems konfigurieren. Wenn Sie Datums- und Zeitformate in der Ländereinstellungsdatei angeben, müssen diese mithilfe einer Untermenge von Formatkennungen definiert werden, die Zahlen erstellen und von der Funktion strftime() der Programmiersprache C unterstützt werden. Sie können Datums- und Zeitformate in den Konfigurationseinstellungen für Ihre Ländereinstellung mithilfe der folgenden Kennungen definieren.

Datumskennungen

- %Y - das Jahr, angegeben mit 4 Ziffern, z. B. 2011
- %y - das Jahr, Angabe nur der letzten beiden Ziffern, z. B. 11 (nicht 2011)
- %m - der Monat, angegeben als Dezimalzahl (1-12)
- %d - der Tag des Monats (1-31)

In den Datumskennungen können Sie nur eine einzige Jahreskennung angeben. Sie dürfen %Y und %y nicht gleichzeitig angeben. Der Modifikator E (Großbuchstabe E) kann vor Datumskennungen stehen, um das Alternativformat der Ländereinstellung für das Jahr, den Monat oder den Tag zu erstellen. Wenn kein Alternativformat vorhanden ist, wird der Modifikator E ignoriert. Trennen Sie die Kennungen durch ein einzelnes 7-Bit-ASCII-Zeichen voneinander. Häufig verwendete Trennzeichen umfassen Doppelpunkte (:), Kommas (,), Punkte (.), Bindestriche (-) und Schrägstriche (/). Sie dürfen keine Mehrbytezeichen als Trennzeichen verwenden.

Zeitkennungen

- %H - die Stunde, angegeben im 24-Stunden-Format (00-23)
- %I - die Stunde, angegeben im 12-Stunden-Format (00-12)
- %M - die Minuten nach der Stunde (00-59)
- %S - die Sekunden nach der Minute (00-59)
- %p - fügt den Anzeiger AM (vor 12 Uhr mittags) oder PM (nach 12 Uhr mittags) ein.

In den Zeitkennungen können Sie nur eine einzige Stundenkennung angeben. Sie dürfen %I und %H nicht gleichzeitig angeben.

Der Modifikator O (Großbuchstabe O) kann vor Zeitkennungen stehen, um das Alternativformat der Ländereinstellung für die Stunde, die Minuten oder die Sekunden zu erstellen. Der Modifikator O darf nicht vor der Kennung %p stehen. Trennen Sie die Kennungen durch ein einzelnes 7-Bit-ASCII-Zeichen voneinander. Häufig verwendete Trennzeichen umfassen Doppelpunkte (:), Kommas (,) oder Punkte (.). Sie dürfen keine Mehrbytezeichen als Trennzeichen verwenden. Zwischen der Kennung %p und dem Trennzeichen, das vor oder hinter der Kennung steht, dürfen Sie kein Trennzeichen angeben.

Beispiele für in den Ländereinstellungen konfigurierte Zeitformate

Um ein bestimmtes Zeitformat zu definieren, editieren Sie die Konfigurationsdatei für die Ländereinstellung und ändern Sie die Zeile `t_fmt` gemäß den Anforderungen. Das ausgewählte Zeitformat gilt sowohl für die Ausgabe als auch für die Eingabe. Nachdem die Konfigurationsdatei für die Ländereinstellung editiert wurde, muss der Befehl **localedef** ausgeführt werden, um die endgültige Ländereinstellungsdatei zu erstellen.

Tabelle 72. Mustereinstellungen für das Zeitformat in der Konfigurationsdatei für die Ländereinstellung (Zeile `t_fmt`)

Beispiel	Ergebnis
"%H:%M:%S"	Zeigt die Zeit im Format <i>hh:mm:ss</i> an; <i>hh</i> liegt im Bereich von 0 bis 23.
"%H,%M,%S"	Zeigt die Zeit im Format <i>hh,mm,ss</i> an; <i>hh</i> liegt im Bereich von 0 bis 23.

Tabelle 72. Mustereinstellungen für das Zeitformat in der Konfigurationsdatei für die Ländereinstellung (Zeile *t_fmt*) (Forts.)

Beispiel	Ergebnis
"%I,%M,13p"	Zeigt die Zeit im Format <i>hh,mm,ssA/P</i> an, wobei <i>hh</i> (Stunde) den Bereich 1 bis 12 aufweist und <i>A/P</i> die Abkürzung für ante-meridian (vormittags, AM in Englisch) oder post-meridian (nachmittags, PM in Englisch) ist.

Beispiele für in den Ländereinstellungen konfigurierte Datumsformate

Um ein bestimmtes Datumsformat zu definieren, editieren Sie die Konfigurationsdatei und ändern Sie die Zeile *d_fmt* gemäß Ihren Anforderungen. Das ausgewählte Datumsformat gilt sowohl für die Ausgabe als auch für die Eingabe.

Tabelle 73. Mustereinstellungen für das Datumsformat in der Konfigurationsdatei für die Ländereinstellung (Zeile *d_fmt*)

Beispiel	Ergebnis
"%m/%d/%y"	Zeigt das Datum im Format <i>MM/TT/JJ</i> an.
"%d.%m.%Y"	Zeigt das Datum im Format <i>TT.MM.JJJJ</i> an.

Dedupcachepath

Verwenden Sie die Option *dedupcachepath*, um die Position anzugeben, an der die Cachedatenbank für die clientseitige Deduplizierung von Daten erstellt wird.

Diese Option wird ignoriert, wenn die Option *enablededupcache=no* während der Sicherung- oder Archivierungsverarbeitung definiert wird.

Unterstützte Clients

Diese Option ist für alle Client gültig. Diese Option ist auch für die IBM Spectrum Protect-API gültig.

Optionsdatei

Fügen Sie diese Option in die Systemoptionsdatei (*dsm.sys*) ein. Sie können diese Option im Feld **Position des Deduplizierungscache** des Profileditors definieren. Diese Option kann in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server definiert werden.

Syntax

►►—DEDUPCACHEPath—*Pfad*—————◄◄

Parameter

Pfad

Gibt die Position an, an der die Cachedatenbank für die clientseitige Deduplizierung von Daten erstellt wird, wenn die Option *enablededupcache* auf *yes* gesetzt wird. Die Standardposition für die Erstellung der Cachedatei für die Deduplizierung von Daten ist das Installationsverzeichnis des Clients für Sichern/Archivieren oder der API.

Beispiele

Optionsdatei:

dedupcachepath /volumes/temp

Befehlszeile:

Nicht zutreffend.

Zugehörige Verweise:

„Enablededupcache“ auf Seite 426

Dedupcachesize

Verwenden Sie die Option `dedupcachesize`, um die maximale Größe der Cachedatei für die Deduplizierung von Daten festzulegen. Wenn die Cachedatei ihre maximale Größe erreicht, wird der Inhalt des Cache gelöscht und neue Einträge werden hinzugefügt.

Unterstützte Clients

Diese Option ist für alle Client gültig. Diese Option ist auch für die IBM Spectrum Protect-API gültig.

Optionsdatei

Fügen Sie diese Option in die Systemoptionsdatei (`dsm.sys`) ein. Sie können diese Option im Feld **Deduplizierung > Deduplizierungscache > Maximale Größe** des Profileditors definieren. Diese Option kann in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server definiert werden.

Syntax

►—DEDUPCACHESize—*Größe des Deduplizierungscache*—►

Parameter

Größe des Deduplizierungscache

Gibt die maximale Größe der Cachedatei für die Deduplizierung von Daten in Megabyte an. Der Wertebereich ist 1 - 2048; der Standardwert ist 256.

Beispiele

Optionsdatei:

dedupcachesize 1024

Befehlszeile:

Nicht zutreffend.

Zugehörige Verweise:

„Deduplication“

Deduplication

Verwenden Sie die Option `deduplication`, um anzugeben, ob die clientseitige Entfernung redundanter Daten bei der Übertragung von Daten an IBM Spectrum Protect während der Sicherungs- und Archivierungsverarbeitung aktiviert sein soll.

Die Datendeduplizierung ist inaktiviert, wenn die Option `enablelanfree` festgelegt ist. Vom Client für Sichern/Archivieren verschlüsselte Dateien sind von der client-

seitigen Deduplizierung von Daten ausgeschlossen. Dateien aus verschlüsselten Dateisystemen sind ebenfalls ausgeschlossen.

Für die Unterstützung der clientseitigen Datendeduplizierung müssen die folgenden Bedingungen erfüllt sein:

- Die clientseitige Datendeduplizierung für den Knoten ist auf dem Server aktiviert.
- Der Zielspeicherpool für die Daten muss ein Speicherpool sein, der für die Datendeduplizierung aktiviert ist. Der Speicherpool muss über den Einheitentyp "Datei" verfügen.
- Eine Datei kann von der clientseitigen Datendeduplizierungsverarbeitung ausgeschlossen werden (standardmäßig sind alle Dateien eingeschlossen).
- Der Server kann die maximale Transaktionsgröße für die Datendeduplizierung durch Definieren der Option CLIENTDEDUPTXNLIMIT auf dem Server begrenzen. Weitere Informationen zu der Option finden Sie in der IBM Spectrum Protect-Serverdokumentation.
- Die Datei muss größer als 2 KB sein.

Unterstützte Clients

Diese Option ist für alle Clients gültig und kann auch von der IBM Spectrum Protect-API verwendet werden.

Optionsdatei

Fügen Sie diese Option in die Systemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option definieren, indem Sie das Kontrollkästchen **Deduplizierung > Deduplizierung aktivieren** des Profileditors auswählen. Diese Option kann in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server definiert werden.

Syntax



Parameter

No Gibt an, dass Sie die clientseitige Datendeduplizierung für die Sicherungs- und Archivierungsverarbeitung nicht aktivieren wollen. 'No' ist der Standardwert.

Yes

Gibt an, dass Sie die clientseitige Datendeduplizierung für die Sicherungs- und Archivierungsverarbeitung aktivieren wollen.

Beispiele

Optionsdatei:

deduplication yes

Befehlszeile:

-deduplication=yes

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Zugehörige Verweise:

„Include-Optionen“ auf Seite 473

„Exclude-Optionen“ auf Seite 438

Defaultserver

Verwenden Sie die Option `defaultserver`, um den Namen des IBM Spectrum Protect-Servers anzugeben, zu dem zwecks Sicherungs-/Archivierungsservices der Kontakt hergestellt werden soll, falls mehrere Server in der Datei `dsm.sys` definiert sind.

Standardmäßig stellt die Sicherung/Archivierung den Kontakt zu dem Server her, der in der ersten Zeilengruppe in der Datei `dsm.sys` definiert ist. Diese Option wird nur verwendet, wenn die Option `servername` nicht in der Clientbenutzeroptionsdatei (`dsm.opt`) angegeben ist.

Wenn der Client für die hierarchische Speicherverwaltung (HSM-Client) auf Ihrer Workstation installiert ist und kein Umlagerungsserver mit der Option `migrateserver` angegeben wird, können Sie mit dieser Option den Server angeben, in den Dateien umgelagert werden sollen. Weitere Informationen enthält die Produktdokumentation zu IBM Spectrum Protect for Space Management im IBM Knowledge Center unter <http://www.ibm.com/support/knowledgecenter/SSERBH/welcome>.

Unterstützte Clients

Diese Option ist für alle UNIX-Clients gültig.

Optionsdatei

Fügen Sie diese Option *am Anfang* der Datei `dsm.sys` *vor* allen Serverzeilengruppen ein.

Syntax

►—DEFAULTServer— —*Servername*—►

Parameter

Servername

Gibt den Namen des Standardservers an, auf dem Sie Dateien sichern oder archivieren. Der Server, auf den Dateien von Ihren lokalen Dateisystemen umgelagert werden, kann mit dieser Option ebenfalls angegeben werden.

Beispiele

Optionsdatei:

```
defaults server_a
```

Befehlszeile:

Nicht zutreffend.

Deletefiles

Verwenden Sie die Option `deletefiles` im Befehl **archive**, um Dateien von Ihrer Workstation zu löschen, nachdem Sie sie archiviert haben.

Diese Option kann auch im Befehl **restore image** und mit der Option **incremental** verwendet werden, um Dateien aus dem zurückgeschriebenen Image zu löschen, falls sie nach der Erstellung des Image gelöscht wurden. Das Löschen von Dateien wird ordnungsgemäß ausgeführt, wenn die Sicherungskopiengruppe des IBM Spectrum Protect-Servers über genügend Versionen für vorhandene und gelöschte Dateien verfügt.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

►►—DEletеfiles—►►

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
dsmc archive "/Users/dgordon/Documents/*.c" -deletefiles
dsmc archive "/home/foo/*.c" -deletefiles
dsmc restore image /local/data -incremental -deletefiles
```

Description

Die Option **description** ordnet Dateien beim Ausführen von Archivieren, Archivierung löschen, Abrufen, Archivierung abfragen oder Sicherungssatz abfragen eine Beschreibung zu oder gibt eine Beschreibung für diese Dateien an.

Soll beispielsweise die Datei `budget.jan` archiviert und ihr die Beschreibung „2002 Budget für Proj 1“ zugeordnet werden, geben Sie Folgendes ein:

```
dsmc archive -des="2002 Budget für Proj 1" /home/plan/
proj1/budget.jan
```

Anmerkung:

1. Die maximale Länge einer Beschreibung ist 254 Zeichen.
2. Schließen Sie den Wert in Anführungszeichen (" ") ein, wenn der von Ihnen eingegebene Optionswert ein Leerzeichen enthält.

Die Option **description** kann in den folgenden Befehlen verwendet werden:

- **archive**
- **delete archive**
- **query archive**
- **query backupset**
- **retrieve**

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

►—DEscription —Beschreibung—◄

Parameter

Beschreibung

Ordnet der Datei, die archiviert wird, eine Beschreibung zu. Wenn Sie keine Beschreibung im Befehl **archive** angeben, lautet der Standardwert Archivierungsdatum:x; hierbei gibt x das aktuelle Systemdatum an. Bitte beachten Sie, dass das Datum immer 10 Zeichen lang ist. Wenn Ihr Datumsformat nur zwei Stellen für das Jahr verwendet, sind am Ende des Datums zwei Leerzeichen. Beispiel: Eine Standardbeschreibung mit einer vierstelligen Jahreszahl könnte so aussehen: "Archivierungsdatum: 03.05.2002". Dieselbe Standardbeschreibung mit einer zweistelligen Jahreszahl würde so aussehen: "Archivierungsdatum: 03.05.02 " (beachten Sie die beiden Leerzeichen am Ende). Wenn Sie Dateien mit der zweistelligen Jahreszahlbeschreibung abrufen, können Sie die Zeichenfolge der Option `-description` auf eine der beiden folgenden Arten eingeben:

```
-description="Archivierungsdatum: 03.05.02 "  
oder  
-description="Archivierungsdatum: 03.05.02*"
```

Werden mit dem Befehl **archive** mehrere Dateien archiviert, gilt die eingegebene Beschreibung für jede Datei. Soll beispielsweise eine Dateigruppe archiviert und jeder Datei dieselbe Beschreibung, *Projekt X*, zugeordnet werden, Folgendes eingeben:

```
dsmc archive -description="Projekt X" "/Users/van/Documents/*.x"  
dsmc archive -description="Projekt X" "/home/allproj/*.x"
```

Mit Hilfe der Beschreibung können dann alle Dateien abgerufen werden.

Beispiele

Befehlszeile:

```
dsmc archive "/Users/van/Documents/*.prj" -des="2003 Budget für Proj 1"  
dsmc archive "/home/foo/*.prj" -des="2003 Budget für Proj 1"  
dsmc query backupset -loc=server -descr="Mein Laptop"
```

Detail

Verwenden Sie die Option `detail`, um abhängig vom Befehl, mit dem sie verwendet wird, Angaben zu Verwaltungsklasse, Dateibereich, Sicherung und Archivierung sowie zusätzliche Informationen anzuzeigen.

Verwenden Sie die Option `detail` im Befehl **query mgmtclass**, um ausführliche Informationen zu allen Verwaltungsklassen in Ihrer aktiven Maßnahmengruppe anzuzeigen. Wird die Option `detail` nicht verwendet, werden nur der Name der Verwaltungsklasse und eine Kurzbeschreibung auf dem Bildschirm angezeigt. Wird die Option `detail` angegeben, werden Informationen zu Attributen in jeder Kopiergruppe in allen Verwaltungsklassen auf dem Bildschirm angezeigt. Eine Verwaltungsklasse kann eine Sicherungskopiergruppe und/oder eine Archivierungskopiergruppe oder keine Kopiergruppe enthalten.

Ein Unicode-fähiger Dateibereich wird unter Umständen nicht korrekt angezeigt, wenn der Server den Unicode-Namen nicht anzeigen kann. In diesem Fall müssen

Sie die Dateibereichskennung (FSID) des Dateibereichs verwenden, um diese Dateibereiche auf dem Server zu identifizieren. Verwenden Sie die Option `detail` in den Befehlen **delete filespace** und **query filespace**, um die FSID eines Dateibereichs festzustellen. Die FSID wird auch im Dateiinformationsdialog der GUI des Clients für Sichern/Archivieren angezeigt.

Verwenden Sie die Option `detail` in den Befehlen **query backup** und **query archive**, um die folgenden Attribute für die von Ihnen angegebene Datei anzuzeigen:

- Datum der letzten Änderung
- Datum des letzten Zugriffs
- Komprimierung
- Verschlüsselungstyp
- Clientseitige Deduplizierung von Daten
- Ob der HSM-Client die Datei umgelagert oder vorumgelagert hat

Verwenden Sie die Option `detail` im Befehl **query vm**, um folgende Statistikdaten anzuzeigen:

- Die durchschnittliche Anzahl IBM Spectrum Protect-Objekte, die für die Beschreibung eines einzelnen Megablocks benötigt wird. Dabei werden alle Megablocks in einer Sicherung berücksichtigt.
- Die durchschnittliche Anzahl IBM Spectrum Protect-Objekte, die für die Beschreibung eines einzelnen Megablocks für alle Megablocks in einem Dateibereich benötigt wird.
- Das Verhältnis des von der Überwachung geänderter Blöcke dokumentierten Datenvolumens im Vergleich zu dem Datenvolumen, das in einer bestimmten Sicherung tatsächlich gesichert wurde.
- Das Verhältnis des von der Überwachung geänderter Blöcke dokumentierten Datenvolumens im Vergleich zu dem Datenvolumen, das bei allen Sicherungen in diesem Dateibereich tatsächlich gesichert wurde.
- Die Anzahl der Sicherungen, die seit der Erstellung der letzten Gesamtsicherung von den Produktionsplatten erstellt wurden.

Die für **query vm** zurückgegebenen Werte können Ihnen bei der Optimierung der heuristischen Verfahren helfen (siehe die Optionen `Mbobjrefreshtresh` und `Mbpctrefreshtresh`), um den Wertauslöser für die Aktualisierung von Megablocks zu optimieren.

Verwenden Sie die Option `detail` in den folgenden Befehlen:

- **delete filespace**
- **incremental**
- **query archive**
- **query backup**
- **query filespace**
- **query inclexcl**
- **query mgmtclass**
- **query vm**

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option wird nicht in der Clientoptionsdatei definiert. Sie fügen sie in die Befehlszeile ein, wenn Sie einen der Befehle eingeben, die diese Option unterstützen. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

►►—DETail—◄◄

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
dsmc query mgmtclass -detail
dsmc query filespace -detail
dsmc query backup file1 -detail
dsmc query vm -detail
```

Diffsnapshot

Die Option `diffsnapshot` legt fest, ob der Client für Sichern/Archivieren die Differenzmomentaufnahme erstellt, wenn eine Teilsicherung unter Verwendung der Momentaufnahmedifferenz ausgeführt wird.

Wird die Differenzmomentaufnahme nicht vom Client erstellt, wird die letzte auf dem Datenträger gefundene Momentaufnahme als Differenzmomentaufnahme und als Quelle für die Sicherungsoperation verwendet.

Der Standardwert ist die Erstellung der Differenzmomentaufnahme. Diese Option wird ignoriert, wenn die Option `snapdiff` zum ersten Mal verwendet wird. Bei der ersten Verwendung der Option `snapdiff` für einen Datenträger muss eine Momentaufnahme erstellt und als Quelle für eine vollständige Teilsicherung verwendet werden. Vom Client für Sichern/Archivieren erstellte Momentaufnahmen werden nach Beendigung der nächsten Teilsicherung unter Verwendung der Momentaufnahmedifferenz vom Client gelöscht.

Momentaufnahmen können mit dem Network Appliance FilerView-Tool erstellt werden. Verwenden Sie den Parameter `latest`, wenn der Client die neueste Momentaufnahme verwenden soll, die mit dieser oder einer anderen Methode erstellt wurde. Momentaufnahmen, die mit Methoden außerhalb von IBM Spectrum Protect erstellt werden, werden nie vom Client gelöscht.

Unterstützte Clients

Diese Option ist für Linux x86_64-Clients gültig.

Syntax

►►—DIFFSNAPSHOT—◄◄

create

latest

Parameter

create

Gibt an, dass Sie eine neue, persistente Momentaufnahme erstellen wollen, die als Quellenmomentaufnahme verwendet wird. Dies ist der Standardwert.

latest

Gibt an, dass Sie die neueste Momentaufnahme, die auf dem Dateiserver gefunden wird, als Quellenmomentaufnahme verwenden wollen.

Beispiele

Befehlszeile:

Eine Teilsicherung unter Verwendung der Momentaufnahmedifferenz für das über NFS-Mount angehängte Dateisystem /vol/vol1 ausführen, das sich auf dem Dateiserver homestore.example.com befindet. Dabei ist /net/home1 der Mountpunkt von /vol/vol1.

```
incremental -snapdiff -diffsnapshot=latest /net/home1
```

Der Wert latest der Option -diffsnapshot bedeutet, dass bei der Operation die letzte Momentaufnahme (die aktive Momentaufnahme) verwendet wird.

Zugehörige Konzepte:

„Momentaufnahmedifferenzsicherung mit einer HTTPS-Verbindung“ auf Seite 190

Zugehörige Tasks:

„NetApp und IBM Spectrum Protect für Teilsicherungen unter Verwendung der Momentaufnahmedifferenz konfigurieren“ auf Seite 119

Zugehörige Verweise:

„Snapdiff“ auf Seite 581

„Snapdiffhttps“ auf Seite 588

„Createnewbase“ auf Seite 383

Diffsnapshotname

Mit der Option diffsnapshotname können Sie angeben, welche Differenzmomentaufnahme auf dem Zieldateiserverdatenträger während einer Momentaufnahmedifferenzsicherung verwendet werden soll. Diese Option wird nur angegeben, wenn Sie auch diffsnapshot=latest angeben.

Wird diese Option nicht angegeben, wird bei der Angabe von diffsnapshot=latest die jüngste vorhandene Momentaufnahme auf dem Dateiserverdatenträger ausgewählt und als Differenzmomentaufnahme verwendet.

Unterstützte Clients

Diese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Optionsdatei

Diese Option kann in der Clientoptionsdatei oder in der Befehlszeile angegeben werden.

Syntax

►►—DIFFSNAPSHOTName— —*Momentaufnahmename*—————►►

Parameter

Momentaufnahmename

Gibt den Namen einer vorhandenen Momentaufnahme an, die als Differenzmomentaufnahme verwendet werden soll.

Sie können auch ein Muster mit Platzhalterzeichen für die Auswahl einer Momentaufnahme verwenden. Gültige Platzhalterzeichen sind:

* Ein Stern (*) entspricht beliebigen Zeichen.

? Ein Fragezeichen (?) entspricht einem einzelnen Zeichen.

Die jüngste Momentaufnahme, die dem Platzhaltermuster entspricht, wird als Differenzmomentaufnahme ausgewählt.

Beispiele

Optionsdatei:

```
diffsnapshotname volume_base_snap
diffsnapshotname nightly.?
```

Befehlszeile:

```
dsmc incr \\DRFiler\UserDataVol_Mirror_Share -snapdiff
-useexistingbase -basenameshotname="nightly.?"
-diffsnapshot=latest -diffsnapshotname="nightly.?"
```

Zugehörige Informationen

Basesnapshotname

Useexistingbase

Dirmc

Mit der Option **dirmc** wird die Verwaltungsklasse angegeben, die für Verzeichnisse verwendet werden soll.

Wenn Sie diese Option nicht für die Zuordnung zwischen einer Verwaltungsklasse und Verzeichnissen angeben, verwendet das Clientprogramm die Verwaltungsklasse in der aktiven Maßnahmengruppe Ihrer Maßnahmendomäne mit dem längsten Aufbewahrungszeitraum. Wählen Sie eine Verwaltungsklasse für einzelne Verzeichnisse aus, durch die Verzeichnisse mindestens so lange aufbewahrt werden wie die ihnen zugeordneten Dateien.

Wenn Sie eine Verwaltungsklasse mit dieser Option angeben, sind alle Verzeichnisse, die in einer Sicherungsoperation angegeben werden, an diese Verwaltungsklasse gebunden.

Die Option **dirmc** gibt die Verwaltungsklasse für gesicherte Verzeichnisse an; bei archivierten Verzeichnissen bleibt sie ohne Wirkung. Verwenden Sie die Option **archmc** im Befehl **archive**, um die verfügbare Verwaltungsklasse für Ihre Maßnahmendomäne anzugeben, an die Sie Ihre archivierten Verzeichnisse und Dateien binden wollen. Wenn Sie die Option **archmc** nicht verwenden, bindet der Server archivierte Verzeichnisse an die Standardverwaltungsklasse. Hat die Standardverwaltungsklasse keine Archivierungskopiengruppe, bindet der Server archivierte Verzeichnisse an die Verwaltungsklasse mit dem kürzesten Aufbewahrungszeitraum.

Wichtig: Nur erweiterte Attribute und ACLs werden in Speicherpools gespeichert. Die Verzeichnisinformationen über die erweiterten Attribute und ACLs hinaus verbleiben in der Datenbank. Auf Windows-Systemen belegen Verzeichnisse Speicherbereich im Speicherpool.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Datei `dsm.sys` innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Sichern** im Abschnitt **Verzeichnis für Verwaltungsklasse** im Profileditor definieren.

Syntax

►►—DIRMc— —*Verwaltungsklassenname*—►►

Parameter

Verwaltungsklassenname

Gibt den Namen der Verwaltungsklasse an, die Verzeichnissen zugeordnet werden soll. Der Client verwendet den von Ihnen angegebenen Verwaltungsklassenamen für alle Verzeichnisse, die Sie sichern. Wenn Sie diese Option nicht angeben, wird den Verzeichnissen vom Client die Verwaltungsklasse mit dem längsten Aufbewahrungszeitraum zugeordnet.

Beispiele

Optionsdatei:

`dirm managdir`

Befehlszeile:

Nicht zutreffend.

Zugehörige Informationen

Wenn Sie bestimmte Dateien in einer Verwaltungsklasse sichern wollen, finden Sie in „Dateien einer Verwaltungsklasse zuordnen“ auf Seite 316 weitere Informationen.

Dirsonly

Mit der Option `dirsonly` werden *nur* Verzeichnisse verarbeitet. Der Client verarbeitet keine Dateien.

Die Option `dirsonly` ist in den folgenden Befehlen zu verwenden:

- **archive**
- **incremental**
- **query archive**
- **query backup**
- **restore**
- **restore backupset**
- **retrieve**
- **selective**

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

►►—Dirsonly—►►

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
dsmc query backup -dirsonly "/Users/*"
```

Befehlszeile:

```
dsmc query backup -dirsonly "*"
```

Disablenqr

Die Option `disablenqr` gibt an, ob der Client für Sichern/Archivieren die Methode "Zurückschreiben ohne Abfrage" (No Query Restore) verwenden kann, um Dateien und Verzeichnisse vom Server zurückzuschreiben.

Wenn Sie die Option `disablenqr` auf `no` (Standardwert) setzen, kann der Client den Zurückschreibungsprozess ohne Abfrage verwenden.

Wenn Sie die Option `disablenqr` auf `yes` setzen, kann der Client nur den Standardzurückschreibungsprozess (auch als "klassische Zurückschreibung" bekannt) verwenden.

Anmerkung: Es gibt keine Option bzw. keinen Wert, mit dem angegeben werden kann, dass der Client nur die Zurückschreibungsmethode ohne Abfrage verwenden darf.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Datei `dsm.opt` ein.

Syntax

►►—DISABLENQR—

No
Yes

—►►

Parameter

No Gibt an, dass der Client die Methode "Zurückschreiben ohne Abfrage" verwenden kann. Dies ist der Standardwert.

Yes

Gibt an, dass der Client nur die Standardzurückschreibungsmethode verwendet. Die Methode "Zurückschreiben ohne Abfrage" ist nicht zulässig.

Beispiele

Optionsdatei:

disablenqr yes

Befehlszeile:

-disablenqr=yes

Diskbuffsize

Die Option `diskbuffsize` gibt die maximale Platten-E/A-Puffergröße (in Kilobyte) an, die der Client beim Lesen von Dateien verwenden kann. Die Option `diskbuffsize` ersetzt die Option `largecommbuffers`.

Die optimale Umlagerungsclientleistung beim Sichern, beim Archivieren oder bei HSM kann normalerweise erreicht werden, wenn der Wert dieser Option maximal dem Wert für das Vorauslesen von Dateien entspricht, der für das Clientdateisystem angegeben ist. Für einen größeren Puffer ist mehr Hauptspeicher erforderlich und die Leistung erhöht sich eventuell nicht.

Wichtig: Verwenden Sie die Standardeinstellung, solange die Mitarbeiter der IBM Unterstützungsfunktion keine anderen Anweisungen erteilen.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein.

Syntax

►►—DISKBuffsize— —Größe—————►►

Parameter

Größe

Gibt die maximale Platten-E/A-Puffergröße (in Kilobyte) an, die der Client beim Lesen von Dateien verwendet. Der Wertebereich ist 16 bis 1023; Standardwert ist 32. Für AIX: Ist `enablelanfree no` festgelegt, lautet die Standardeinstellung für `diskbuffsize` 256.

Beispiele

Optionsdatei:

`diskbuffsize 64`

Befehlszeile:

Nicht zutreffend.

Diskcachelocation

Die Option `diskcachelocation` gibt die Position an, an der die Plattencachedatenbank erstellt wird, wenn die Option `memoryefficientbackup=diskcachemethod` bei einer Teilsicherung definiert ist.

Sie können die Option `diskcachelocation` in Ihrer Optionsdatei oder mit der Option `include.fs` angeben. Ist die Option `diskcachelocation` in der Optionsdatei vorhanden, wird ihr Wert für alle Dateisysteme verwendet, für die keine Option `include.fs` zusammen mit der Option `diskcachelocation` angegeben ist.

Der Plattencache ist eine temporäre Datei, die nach der Ausführung des Befehls **incremental** gelöscht wird. Verwenden Sie diese Option für die Auswahl einer der folgenden Angaben:

1. Eine Speicherposition mit mehr freiem Plattenspeicherplatz, wenn Sie bei Verwendung von `memoryefficientbackup=diskcachemethod` die Nachricht erhalten, dass die Plattencachedatei nicht erstellt werden kann, da nicht genügend Plattenspeicherplatz verfügbar ist.
2. Eine Speicherposition auf einem anderen physischen Datenträger, um Konkurrenzsituationen beim Plattenzugriff zu verhindern und somit die Leistung zu verbessern

Wichtig: Verwenden Sie aus Leistungsgründen kein fernes Laufwerk für `diskcachelocation`!

Der tatsächlich erforderliche Plattenspeicherplatz für die Plattencachedatei, die bei Teilsicherungen des Plattencaches erstellt wird, ist von der Anzahl der Dateien und Verzeichnisse abhängig, die in die Sicherung eingeschlossen werden, sowie von der durchschnittlichen Länge der zu sichernden Dateien und Verzeichnisse. Für UNIX und Linux beträgt der Schätzwert 1 Byte pro Zeichen im Pfadnamen. Für Mac OS X beträgt der Schätzwert 4 Byte pro Zeichen im Pfadnamen. Beispiel: Es müssen 1 000 000 Dateien und Verzeichnisse gesichert werden und die durchschnittliche Pfadlänge beträgt 200 Zeichen. In diesem Fall belegt die Datenbank etwa 200 MB für UNIX- und Linux-Clients und 800 MB für Mac OS X-Clients. Ein anderes Schätzverfahren für Planungszwecke besteht darin, die Anzahl der Dateien und Verzeichnisse mit der Länge des längsten Pfads zu multiplizieren, um eine maximale Datenbankgröße zu ermitteln.

Beim Sichern eines über HSM verwalteten Dateisystems wird eine zweite Plattencachedatei für die Liste der umgelagerten Dateien erstellt. Für beide Plattencachedateien zusammen - die bei Teilsicherungen des Plattencaches erstellte Plattencachedatei und die bei Sicherungen von über HSM verwalteten Dateisystemen erstellte Plattencachedatei - können mehr als 400 MB Plattenspeicherplatz pro Million zu sichernder Dateien erforderlich sein. Die Plattencachedatei kann sehr groß werden. Auf dem Dateisystem, das für die Plattencachedatei verwendet wird, muss Unterstützung für große Dateien aktiviert sein.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Datei `dsm.sys` innerhalb einer Serverzeilengruppe ein.

Syntax

►►—DISKCACHELocation— —Pfad—◄◄

Parameter

Pfad

Gibt die Position an, an der die Plattencachedatenbank erstellt wird, wenn `memoryefficientbackup=diskcachemethod` festgelegt ist. Standardmäßig wird die Plattencachedatei im Stammverzeichnis des Dateibereichs erstellt, der gerade verarbeitet wird.

Beispiele

Optionsdatei:

```
diskcachelocation /home  
diskcachelocation /Volumes/hfs2
```

Befehlszeile:

Nicht zutreffend.

Unter „Include-Optionen“ auf Seite 473 finden Sie weitere Informationen über `include.fs`.

Domain

Die Option `domain` gibt an, welche Objekte Sie bei Teilsicherungen einschließen wollen.

Domänenobjekte werden nur gesichert, wenn Sie den Befehl **incremental** ohne Dateispezifikation starten.

Der Client für Sichern/Archivieren verwendet den Wert von 'domain' in den folgenden Situationen, um festzustellen, welche Dateisysteme während einer Teilsicherung zu verarbeiten sind:

- Wenn Sie eine Teilsicherung mithilfe des Befehls **incremental** ausführen und nicht angeben, welche Dateisysteme verarbeitet werden sollen.
- Wenn Ihr IBM Spectrum Protect-Administrator einen Zeitplan für eine Teilsicherung für Sie definiert, aber nicht angibt, welche Dateisysteme verarbeitet werden sollen.
- Wenn Sie die Aktion **Domäne sichern** in der GUI des Clients für Sichern/Archivieren auswählen.
- Wenn Sie eine Teilsicherung mithilfe des Befehls **incremental** ausführen und nicht angeben, welche Laufwerke verarbeitet werden sollen.
- Wenn Ihr IBM Spectrum Protect-Administrator einen Zeitplan für eine Teilsicherung für Sie definiert, aber nicht angibt, welche Laufwerke verarbeitet werden sollen.
- Wenn Sie die Aktion **Domäne sichern** in der GUI des Clients für Sichern/Archivieren auswählen.

Sie können die Option `domain` an den folgenden Positionen definieren:

- In einer Optionsdatei.
- In der Befehlszeile, wenn sie mit einem Clientbefehl eingegeben wird.
- In einer Clientoptionsgruppe, die auf dem Server mit dem Befehl **define client-opt** definiert wird.
- Als Option in einem geplanten Befehl, der auf dem Server mit dem Befehl **define schedule** definiert wird.

Enthält eine dieser Quellen eine Domänendefinition, sichert der Client die entsprechende Domäne. Sind Domänen in mehreren Quellen angegeben, sichert der Client alle angegebenen Domänen. Dasselbe Domänenobjekt kann mehrfach definiert werden; die Auswirkungen unterscheiden sich jedoch nicht von der einmaligen Definition. Wenn Sie keine Domäne angeben, sichert der Client die Standarddomäne, wie unter dem Parameter `all-local` beschrieben.

Sie können Objekte aus der Domäne ausschließen, indem Sie den Ausschlussoperator (-) vor dem Objekt angeben. Wenn ein Objekt in einer Domänendefinition ausgeschlossen ist, wird dieses Objekt von der Domäne ausgeschlossen, auch wenn es in einer anderen Definition eingeschlossen ist. Sie können den Domänenausschlussoperator (-) keinem Domänenschlüsselwort voranstellen, das mit `all-` beginnt.

Wenn eine Domänenanweisung mindestens ein Objekt ausschließt und keine Domänenanweisung Objekte einschließt, ist das Ergebnis eine leere Domäne (nichts wird gesichert). Sie müssen die Objekte, die in der Domäne eingeschlossen sein sollen, angeben, wenn Objekte durch Domänenanweisungen ausgeschlossen werden.

Beispiel 1: In diesem Beispiel werden mit einer Domänenanweisung alle lokalen Dateisysteme außer `/fs1` gesichert:

```
domain all-local -/fs1
```

Beispiel 2: In diesem Beispiel werden mit mehreren Domänenanweisungen alle lokalen Dateisysteme außer `/fs1` gesichert:

```
domain all-local domain -/fs1
```

Beispiel 3: In diesem Beispiel wird `/fs1` während einer Sicherungsoperation ausgeschlossen. Wenn keine andere Domänenanweisung verwendet wird, hat dies eine leere Domäne zur Folge. Nichts wird gesichert.

```
domain -/fs1
```

Wenn Sie den Befehl 'incremental' mit einer Dateispezifikation starten, ignoriert der Client alle Domänendefinitionen und sichert nur die Dateispezifikation.

Sie können einen virtuellen Mountpunkt in Ihre Clientdomäne einschließen.

Wichtig: Wenn Sie GPFS für AIX oder GPFS für Linux x86_64 in einem Cluster mit mehreren Knoten ausführen und alle Knoten ein angehängtes GPFS-Dateisystem gemeinsam nutzen, verarbeitet der Client dieses Dateisystem als lokales Dateisystem. Der Client sichert während einer Teilsicherung das Dateisystem auf jedem Knoten. Um diese Situation zu vermeiden, können Sie eine der folgenden Tasks ausführen:

- Konfigurieren Sie explizit die Anweisung 'domain' in der Clientbenutzeroptionsdatei (`dsm.opt`), sodass die Dateisysteme, die auf diesem Knoten gesichert werden sollen, aufgelistet werden.
- Definieren Sie die Option `exclude.fs` in der Clientsystemoptionsdatei so, dass das GPFS-Dateisystem von den Sicherungsservices ausgeschlossen ist.

Auto-Mount-Dateisysteme

Ist die Option `domain` auf `all-local` gesetzt und wird eine Sicherung ausgeführt, werden vom automatischen Mountprogramm verarbeitete Dateien und Schleifen-dateisysteme nicht gesichert.

Ist die Option `domain` auf `all-local` gesetzt, wenn Sie ein Dateisystem sichern, werden alle Unterverzeichnisse, die Mountpunkte für ein Auto-Mount-Dateisystem (AutoFS) sind, von einer Sicherungsoperation ausgeschlossen. Alle Dateien, die auf dem Server für das Auto-Mount-Unterverzeichnis vorhanden sind, verfallen.

Ist die Option `domain` auf `all-lofs` gesetzt und wird eine Sicherung ausgeführt, werden alle expliziten Schleifendateisysteme (LOFS - Loopback File Systems) gesichert und alle Auto-Mount-Dateisysteme ausgeschlossen. Setzen Sie für Schleifen-einheiten und lokale Dateisysteme, die vom automatischen Mountprogramm verarbeitet werden, die Option `domain` auf `all-auto-lofs`.

Verwenden Sie die Option `automount` mit den Domänenparametern `all-auto-nfs` und `all-auto-lofs`, um mindestens ein Auto-Mount-Dateisystem anzugeben, das angehängt und der Domäne hinzugefügt werden soll. Wenn Sie die Option `automount` angeben, werden Auto-Mount-Dateisysteme erneut angehängt, falls sie während der Ausführung des Befehls **incremental** in den Offlinezustand versetzt wurden.

Virtuelle Mountpunkte können nicht mit Auto-Mount-Dateisystemen verwendet werden.

Wichtig: Bei einigen Linux-Distributionen sind Mountpunkte oder -zuordnungen für Auto-Mount-Dateisysteme (AutoFS) möglicherweise in der aktuellen Mounttabelle nicht aufgelistet. Demzufolge werden die Auto-Mount-Dateisysteme, die während der Sicherungs- oder Archivierungsverarbeitung abgehängt werden, möglicherweise nicht korrekt verarbeitet und als Teil einer falschen Domäne gespeichert (beispielsweise als Teil der Domäne `all-local`, `all-nfs` oder `all-lofs`, abhängig vom tatsächlichen Dateisystemtyp). Aus diesem Grund müssen Sie in derartigen Linux-Distributionsumgebungen die entsprechende Einstellung für die Option `automount` angeben, damit Ihre Einstellung für die Option `'domain'` zu jedem Zeitpunkt korrekt verarbeitet wird.

Für Mac OS X werden Auto-Mount-Dateisysteme nicht unterstützt. Wenn ein Auto-Mount-Dateisystem Teil einer Domänenanweisung ist, schlägt die Sicherung fehl und im Auto-Mount-Dateisystem werden keine Dateien verarbeitet. Sichern Sie das Auto-Mount-Dateisystem auf dem Hostsystem und schreiben Sie es von dort zurück. Führen Sie die Sicherung bzw. die Zurückschreibung des Auto-Mount-Dateisystems nicht über eine Netzverbindung aus.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Optionsdatei, `dsm.opt` oder `dsm.sys`, ein. In der Datei `dsm.sys` müssen Sie diese Option innerhalb einer Serverzeilengruppe einfügen. Sie können diese Option auf der Registerkarte **Sichern** im Abschnitt **Domäne für Sicherung** im Profileditor definieren.

Syntax



Parameter

all-local

Sichert alle lokalen Dateisysteme außer LOFS-Dateisystemen und LOFS durch das automatische Mountprogramm. Dieser Parameter ist der Standardwert. Das Verzeichnis /tmp ist nicht eingeschlossen.

Domäne

Definiert die Dateisysteme, die in Ihre Standardclientdomäne einzuschließen sind.

Wenn Sie *domain* im Befehl **incremental** verwenden, werden diese Dateisysteme zusätzlich zu den Dateisystemen verarbeitet, die in Ihrer Standardclientdomäne angegeben sind.

-Domäne

Definiert die Dateisysteme, die von Ihrer Standardclientdomäne auszuschließen sind.

all-lofs

Sichert alle Schleifendateisysteme mit Ausnahme der durch das automatische Mountprogramm bearbeiteten Dateisysteme. Dieser Parameter wird nicht unter Mac OS X unterstützt.

all-nfs

Sichert alle Netzdateisysteme mit Ausnahme der durch das automatische Mountprogramm bearbeiteten Dateisysteme. Dieser Parameter wird nicht unter Mac OS X unterstützt.

all-auto-nfs

Sichert alle Netzdateisysteme (jedoch nicht die lokalen Dateisysteme), die vom automatischen Mountprogramm verarbeitet werden. Dieser Parameter wird nicht unter Mac OS X unterstützt.

all-auto-lofs

Sichert alle Schleifeneinheiten und lokalen Dateisysteme, die durch ein automatisches Mountprogramm bearbeitet werden. Dieser Parameter wird nicht unter Mac OS X unterstützt.

Objekt

Gibt die Domänenobjekte an, die in die Domäne eingeschlossen werden sollen.

Ein Objektname muss in Anführungszeichen eingeschlossen werden, wenn er Leerzeichen enthält.

-Objekt

Gibt die Domänenobjekte an, die von der Domäne ausgeschlossen werden sollen.

Ein Objektname muss in Anführungszeichen eingeschlossen werden, wenn er Leerzeichen enthält.

Beispiele

Optionsdatei:

Eine Optionsdatei kann mehrere Anweisungen `domain` enthalten. Jede der `domain`-Anweisungen stellt jedoch ein Beispiel für eine einzige Anweisung in einer Optionsdatei dar.

```
domain all-local
domain all-local -/Volumes/volume2
domain all-local '-/Volumes/Macintosh HD'

domain /tst /datasave /joe
"domain all-local"
domain ALL-LOCAL -/home
domain ALL-NFS -/mount/nfs1
```

In einer einzigen Domänenanweisung können ein oder mehrere Objekte für die Domäne aufgelistet sein. Sie können mehrere Domänenanweisungen verwenden. Aus den folgenden beiden Beispielen aus zwei Optionsdateien ergibt sich dieselbe Domäne:

Beispiel 1

```
...
domain fs1
domain all-local
domain -fs3
...
```

Beispiel 2

```
...
domain all-local fs1 -fs3
...
```

Befehlszeile:

```
-domain="/ /Volumes/volume2"
-domain="all-local -/Volumes/volume2"
-domain="/fs1 /fs2"
-domain=/tmp
-domain="ALL-LOCAL -/home"
```

Interaktion zwischen Domänendefinitionen

Domänen können in mehreren Quellen definiert sein und das Ergebnis ist die Summe aller Domänendefinitionen. Als Beispiel für die Interaktion zwischen Domänendefinitionen sehen Sie im Folgenden, wie Domänendefinitionen aus mehreren Quellen zu verschiedenen Ergebnissen bei der Sicherung führen. In der Tabelle ist *FS* gefolgt von einer Zahl (z. B. FS1) ein Dateisystem. Diese Tabelle zeigt nur Befehle, die in die Befehlszeile eingegeben werden. Für geplante Befehle ist die Spalte für die Befehlszeile nicht relevant und die Optionen für den geplanten Befehl müssen beachtet werden.

Tabelle 74. Interaktion zwischen Domänendefinitionen aus mehreren Quellen

Optionsdatei	Befehlszeile:	Clientoptionsgruppe	Mit dem Befehl incremental gesicherte Objekte
domain FS1	incremental -domain=FS2	domain FS3	FS1 FS2 FS3
domain FS1	incremental	domain FS3	FS1 FS3
	incremental -domain=FS2		FS2
	incremental -domain=FS2	domain FS3	FS2 FS3

Tabelle 74. Interaktion zwischen Domänendefinitionen aus mehreren Quellen (Forts.)

Optionsdatei	Befehlszeile:	Clientoptionsgruppe	Mit dem Befehl incremental gesicherte Objekte
	incremental	domain FS3	FS3
	incremental		all-local
domain all-local	incremental	domain FS3	all-local + FS3
domain all-local domain -FS1	incremental		all-local, aber nicht FS1
domain -FS1	incremental		Keine
domain FS1 FS3	incremental	domain -FS3	FS1
domain all-local	incremental	domain -FS3	all-local, aber nicht FS3
	incremental FS1 -domain=all-local		FS1
	incremental FS1	domain all-local	FS1
domain -FS1	incremental FS1		FS1

Zugehörige Informationen

Informationen zum Definieren eines virtuellen Mountpunkts finden Sie unter „Virtualmountpoint“ auf Seite 630.

Informationen zum Angeben mindestens eines Auto-Mount-Dateisystems, das angehängt und der Domäne hinzugefügt werden soll, finden Sie in „Automount“ auf Seite 368.

Domain.image

Die Option **domain.image** gibt an, welche Objekte Sie bei einer Imagesicherung in Ihre Clientdomäne einschließen wollen.

Wenn Sie im Befehl **backup image** kein Dateisystem angeben, werden die Dateisysteme gesichert, die Sie mit der Option **domain.image** angeben.

Wenn Sie ein Dateisystem im Befehl **backup image** angeben, wird die Option **domain.image** ignoriert.

Verwenden Sie in Ihrer Clientoptionsdatei nicht die Option **domain.image** zur Angabe von Dateisystemen und geben Sie kein Dateisystem im Befehl **backup image** an, wird eine Nachricht ausgegeben und keine Sicherung durchgeführt.

Unterstützte Clients

Diese Option ist für AIX, Linux x86_64, Linux on POWER und Solaris gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Diese Option ist für alle unterstützten Windows-Clients gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option im Feld **Sichern > Domäne für Sicherung** im Profileditor definieren.

Syntax



Parameter

Domäne

Definiert die Dateisysteme oder die unformatierten logischen Datenträger, die in Ihre Standardclientimagedomäne eingeschlossen werden sollen.

Beispiele

Optionsdatei:

```
domain.image /fs1 /fs2
```

Befehlszeile:

Nicht zutreffend.

Domain.nas

Die Option `domain.nas` gibt die Datenträger an, die bei Ihren NAS-Imagesicherungen berücksichtigt werden sollen.

Sie können `all-nas` angeben, um alle angehängten Dateisysteme auf dem NAS-Dateiserver zu berücksichtigen. Ausgenommen sind hierbei die mit der Option `exclude.fs.nas` ausgeschlossenen Dateisysteme.

Der Client für Sichern/Archivieren verwendet Ihre Domäne für NAS-Imagesicherungen, wenn Sie den Befehl **backup nas** ausführen und nicht angeben, welche Datenträger zu verarbeiten sind.

Wenn Sie diese Option in Ihrer Clientsystemoptionsdatei (dsm.sys) verwenden, definiert die Option `domain.nas` Ihre Standarddomäne für NAS-Imagesicherungen. Wenn Sie eine NAS-Dateisystemimagesicherung mithilfe des Befehls **backup nas** ausführen, fügt der Client die in der Befehlszeile angegebenen Datenträger den Datenträgern hinzu, die in Ihrer Datei dsm.sys definiert sind. Beispiel: Wenn Sie `domain.nas nas1/vol/vol0 nas1/vol/vol1` in Ihrer Datei dsm.sys angeben und `dsmc backup nas -nasnodename=nas1 /vol/vol2` in die Befehlszeile eingeben, sichert der Client die Datenträger `vol/vol0`, `vol/vol1` und `vol/vol2` auf dem Knoten `nas1`.

Wenn Sie die Option `domain.nas` in der Datei dsm.opt auf `all-nas` setzen, sichert der Client alle angehängten Datenträger auf dem NAS-Dateiserver. Wenn Sie bei einer Sicherung eine Dateispezifikation verwenden und die Option `domain.nas` in der Datei dsm.sys auf `all-nas` setzen, hat die Angabe `all-nas` Vorrang.

Unterstützte Clients

Diese Option ist nur für AIX- und Solaris-Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Syntax



Parameter

Domäne

Definiert die Datenträger, die Sie verarbeiten wollen. Es ist nicht möglich, Datenträger durch Angabe des Operators Bindestrich (-) auszuschließen.

all-nas

Verarbeitet alle angehängten Datenträger auf dem NAS-Dateiserver. Ausgenommen sind hierbei die mit der Option `exclude.fs.nas` ausgeschlossenen Datenträger. Dies ist der Standardwert. Enthält die Datei `dsm.opt` keine Anweisung `domain.nas` und werden keine Datenträger in der Befehlszeile angegeben, sichert der Client alle angehängten Datenträger auf dem NAS-Server.

Beispiele

Optionsdatei:

```
domain.nas nas1/vol/vol0 nas1/vol/vol1
domain.nas all-nas
```

Befehlszeile:

Nicht zutreffend.

Domain.vmfull

Die Option `domain.vmfull` gibt die Imagegesamtsicherungsoperationen für virtuelle Maschinen eingeschlossen werden sollen.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Domain.vmfull für virtuelle VMware-Maschinen

Für Sicherungen virtueller VMware-Maschinen arbeitet die Option `domain.vmfull` mit der Option `vmchost` zusammen. Die Option `vmchost` gibt den vCenter-Server oder ESX-Server an, der die virtuellen Maschinen enthält, die Sie schützen wollen. Mit den Parametern von `domain.vmfull` wird eine Operation auf eine Untergruppe der virtuellen Maschinen beschränkt, die auf dem durch `vmchost` angegebenen System ausgeführt werden.

Sie können die zu verarbeitenden virtuellen Maschinen mit einer der folgenden Methoden angeben:

- Verwenden Sie die Option `VM=` und geben Sie den Namen einer virtuellen Maschine an.
- Geben Sie eine durch Kommas getrennte Liste mit den Namen der virtuellen Maschinen an.
- Verwenden Sie eine Syntax mit Platzhalterzeichen, um die virtuellen Maschinen zu verarbeiten, die dem Namensmuster entsprechen.
- Verwenden Sie einen der folgenden Parameter auf Domänenebene:

```
all-vm
all-windows
schedule-tag
vmhost
vmfolder
vmhostcluster
vmdatastore
vmresourcepool
vmhostfolder
vmdatacenter
```

Wenn Sie Parameter auf Domänenebene verwenden, werden virtuelle Maschinen, die in der Domäne erstellt werden, automatisch eingeschlossen, wenn die nächste Sicherung stattfindet. Wenn Sie beispielsweise den Parameter `vmfolder` verwenden, um alle in einem Ordner enthaltenen virtuellen Maschinen zu sichern, werden alle neuen virtuellen Maschinen, die diesem Ordner hinzugefügt werden, bei der nächsten Sicherung berücksichtigt. Dies gilt auch für die mit einem Muster abgeglichenen Namen, die in einer Syntax mit Platzhalterzeichen eingeschlossen sind.

Die mit der Option `domain.vmfull` angegebenen virtuellen Maschinen werden nur verarbeitet, wenn der Befehl **backup vm** ohne Angabe einer virtuellen Maschine oder eine Liste virtueller Maschinen in die Befehlszeile eingegeben wird.

Unterstützte Clients

Diese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Diese Option kann auch auf dem Server definiert werden.

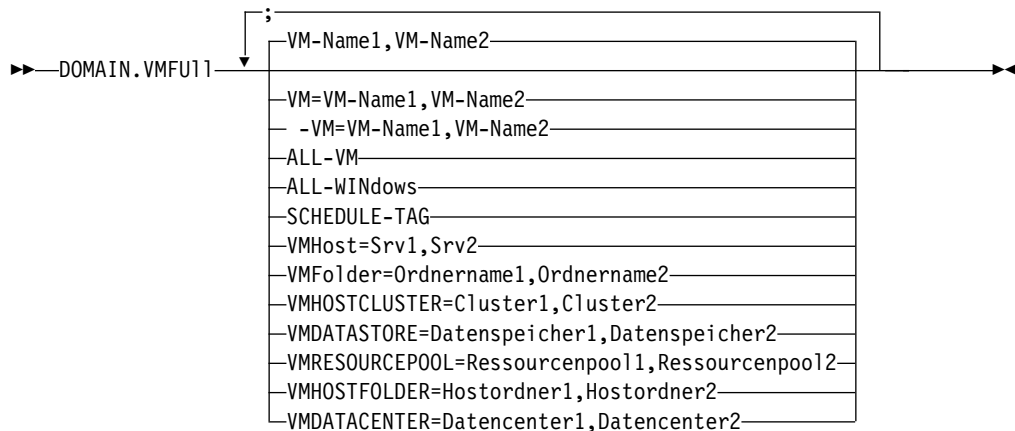
Optionsdatei

Definieren Sie diese Option in den Clientoptionen, über die Befehlszeile oder mithilfe der Registerkarte **VM-Sicherung** im Profileditor.

Einschränkung: Die folgenden Parameter können nicht im Profileditor definiert werden. Schließen Sie diese Einstellung in die Optionsdatei oder in die Befehlszeile ein, wenn Sie einen Befehl **backup vm** ausführen:

```
VM-Name:vmdk=VM-Plattenkennsatz
schedule-tag
vmresourcepool
vmhostfolder
vmdatacenter
```

Syntax für virtuelle VMware-Maschinen



Syntaxregeln: Mehrere Schlüsselwörter müssen jeweils durch ein Semikolon voneinander getrennt werden. Schließen Sie hinter den Semikolons keine Leerzeichen ein. Mehrere Namen virtueller Maschinen oder Domänen müssen durch Kommas und ohne Leerzeichen getrennt werden. Beispiele finden Sie bei `vm=VM-Name`. Die Regel für mehrere Namen virtueller Maschinen oder Domänen gilt nicht, wenn Sie das Schlüsselwort "Schedule-Tag" verwenden.

Parameter

VM-Name

Gibt den Namen der virtuellen Maschine an, die verarbeitet werden soll. Der Name ist der Anzeigename der virtuellen Maschine. Sie können eine Liste mit Hostnamen virtueller Maschinen angeben. Trennen Sie die Namen jeweils durch ein Komma voneinander (`vm1, vm2, vm5`). Bei den Namen muss die Groß-/Kleinschreibung beachtet werden.

vm=VM-Name

Das Schlüsselwort `vm=` gibt an, dass die nächste Gruppe von Werten eine Liste mit Namen virtueller Maschinen ist. Das Schlüsselwort `vm=` ist der Standardwert und ist nicht erforderlich.

In diesem Beispiel ist `vm=` nicht angegeben und die Maschinennamen sind durch Kommas getrennt.

```
domain.vmfull my_vm1, my_vm2
```

Wenn Sie mehrere Schlüsselwörter angeben, z. B. `vm=` und `vmfolder=`, müssen die Werte, auf die sich die Schlüsselwörter beziehen, durch Semikolons und ohne Zwischenleerschritte getrennt werden:

```
domain.vmfull vm=my_vm1; vm=my_vm2
domain.vmfull vm=my_vm1; vmfolder=folder1; vmfolder=folder2
```

Für die Auswahl von Namen virtueller Maschinen, die einem Muster entsprechen, können Platzhalterzeichen verwendet werden. Ein Stern (*) entspricht einer beliebigen Zeichenfolge. Ein Fragezeichen (?) entspricht einem beliebigen einzelnen Zeichen. Zum Beispiel:

- Alle Dateien ausschließen, deren Hostname die Zeichenfolge „test“ enthält:
`-vm=*test*`
- Alle virtuellen Maschinen mit Namen wie den folgenden einschließen:
„test20“, „test25“, „test29“, „test2A“: `vm=test2?`

Sie können eine virtuelle Maschine von einer Sicherungsoperation ausschließen, indem Sie den Ausschlussoperator (-) vor dem Schlüsselwort `vm=` angeben. Beispielsweise wird `-vm` für den Ausschluss einer bestimmten Maschine oder mehrerer Maschinen von einer Sicherung auf Domänenebene (z. B. ALL-Windows, ALL-VM und VMFolder) verwendet. Ist „vm1“ der Name einer virtuellen Maschine im Ordner mit dem Namen „accountingDept“, können Sie alle virtuellen Maschinen im dem Ordner sichern, aber die virtuelle Maschine „vm1“ von der Sicherung ausschließen. Definieren Sie die folgende Option:

```
domain.vmfull VMFolder=accountingDept;-vm=vm1
```

Sie können mit dem Ausschlussoperator (-) keine Domäne ausschließen (z. B. ALL-VM, ALL-Windows oder VMFolder). Der Ausschlussoperator funktioniert nur auf der Ebene der Namen der virtuellen Maschinen.

VM-Name:vmdk=VM-Plattenkennsatz

Das Schlüsselwort `:vmdk=` gilt nur für virtuelle VMware-Maschinen. Für die Verwendung dieses Schlüsselworts ist eine Lizenz für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware erforderlich.

Diese Option wird in der Regel verwendet, um Platten von der Sicherung auszuschließen (siehe Syntax `:-vmdk`). Sie können auch Platten virtueller Maschine einschließen, indem Sie die Option `INCLUDE.VMDISK` verwenden, oder Platten virtueller Maschine ausschließen, indem Sie die Option `EXCLUDE.VMDISK` verwenden.

Die virtuellen Platten in einer virtuellen Maschine verfügen über Plattenkennsätze, die jede virtuelle Platte eindeutig identifizieren. Mit dem Schlüsselwort `:vmdk=` geben Sie die Kennsätze der virtuellen Platten an, die bei einer VM-Sicherungsoperation (**Backup VM**) berücksichtigt werden sollen. Wenn Sie `:vmdk=` und einen Plattenkennsatz nicht angeben, werden alle virtuellen Platten in der virtuellen Maschine gesichert.

Beispiel: Es gibt eine virtuelle Maschine mit dem Namen „my_vm_example“. Diese virtuelle Maschine verfügt über vier Platten (Hard Disk 1, Hard Disk 2, Hard Disk 3, Hard Disk 4). Sollen nur 'Hard Disk 2' und 'Hard Disk 3' bei einer Sicherung berücksichtigt werden, fügen Sie das Schlüsselwort `:vmdk=` und den Plattenkennsatz für diese Platten hinzu. Da die Plattenkennsätze Leerzeichen enthalten, müssen die Parameter zwischen Anführungszeichen stehen. Beispiel:

```
domain.vmfull "my_vm_example:vmdk=Hard Disk 2:vmdk=Hard Disk 3"
```

Mit dem folgenden Beispiel werden 'Hard Disk 1' und 'Hard Disk 2' auf VM1 sowie 'Hard Disk 3' und 'Hard Disk 4' auf VM2 gesichert. Ein Komma wird als Trennzeichen für die Informationen der virtuellen Maschinen verwendet.

```
domain.vmfull "vm1:vmdk=Hard Disk 1:vmdk=Hard Disk 2",  
              "vm2:vmdk=Hard Disk 3:vmdk=Hard Disk 4"
```

Wie bei dem Schlüsselwort `-vm=` können Sie auch bei `:vmdk=` den Ausschlussoperator (-) verwenden, um Platten von einer Sicherungsoperation auszuschließen.

Verwenden Sie folgende Syntax, um eine virtuelle Maschine (vm1) zu sichern und die Platten 'Hard Disk 3' und 'Hard Disk 4' auszuschließen:

```
domain.vmfull "vm1:-vmdk=Hard Disk 3:-vmdk=Hard Disk 4"
```

Sollen zwei virtuelle Maschinen (vm1 und vm2) gesichert und die beiden ersten Platten auf jeder Maschine ausgeschlossen werden, verwenden Sie folgende Syntax:

```
domain.vmfull "vm1:-vmdk=Hard Disk 1:-vmdk=Hard Disk 2",  
"vm2:-vmdk=Hard Disk 1:-vmdk=Hard Disk 2"
```

Sie können eine oder mehrere Platten in einer Anweisung `domain.vmfull` einschließen. Sie können eine oder mehrere Platten in einer Anweisung `domain.vmfull` ausschließen. Sie können das Einschließen und Ausschließen von Platten in einer Anweisung kombinieren. Die folgende Anweisung ist beispielsweise gültig:

```
domain.vmfull  
"vm1:vmdk=Hard Disk 1:-vmdk=Hard Disk 2:vmdk=Hard Disk 3:vmdk=Hard Disk 4"
```

Wenn eine Einschlussanweisung vorhanden ist, werden alle anderen Platten in der virtuellen Maschine von einer Sicherungsoperation ausgeschlossen, sofern die anderen Platten nicht auch in einer Einschlussanweisung angegeben sind. Mit der folgenden Anweisung werden beispielsweise alle Festplatten (Hard Disks) in `vm1` ausgeschlossen, außer 'Hard Disk 1':

```
domain.vmfull "vm1:vmdk=Hard Disk 1"
```

Mit jedem der folgenden Beispiele wird 'Hard Disk 4' von einer Sicherung von `vm1` ausgeschlossen:

```
domain.vmfull "vm1:vmdk=Hard Disk 1:vmdk=Hard Disk 2:vmdk=Hard Disk 3"  
domain.vmfull "vm1:-vmdk=Hard Disk 4"
```

all-vm

Für virtuelle VMware-Maschinen. Mit dieser Option werden alle virtuellen Maschinen verarbeitet, die für den Virtual Center- oder ESX-Server definiert sind, der in der Option `vmchost` angegeben ist.

all-windows

Für virtuelle VMware-Maschinen. Mit dieser Option werden alle virtuellen Maschinen verarbeitet, die für den Virtual Center- oder ESX-Server definiert sind, der in der Option `vmchost` angegeben ist. Die virtuellen Maschinen müssen außerdem über den Gastbetriebssystemtyp Windows verfügen.

schedule-tag

Für geplante Sicherungen virtueller VMware-Maschinen. Mit dieser Option werden alle virtuellen Maschinen verarbeitet, die für den Virtual Center-Server definiert sind, der in der Option `vmchost` angegeben ist.

Der IBM Spectrum Protect-Serveradministrator kann diese Option einer Zeitplandefinition hinzufügen, um anzugeben, dass der Zeitplan mit der Kategorie und dem Tag Schedule (IBM Spectrum Protect) kompatibel ist. Virtuelle Maschinen in VMware-Objekten, denen der Tag Schedule zugeordnet ist, werden gemäß dem Zeitplan gesichert.

Voraussetzung: Damit die Option `-domain.vmfull` für das Tagging kompatibel ist, darf sie außer dem Parameter `Schedule-Tag` in der Zeitplandefinition keine weiteren Parameter auf Domänenebene enthalten. Andernfalls wird der Tag Schedule (IBM Spectrum Protect) ignoriert. Bei der Option muss die Groß-/Kleinschreibung nicht beachtet werden und die Option darf keine Leerzeichen enthalten. Die Anführungszeichen, die den Parameter `Schedule-Tag` einschließen, sind optional. Virtuelle Maschinen in VMware-Containern, die mit Tags versehen sind, die inkompatible Zeitpläne angeben, werden nicht gesichert.

Weitere Informationen zum Tag Schedule finden Sie in "Unterstützte Datenschutztags".

vmhost=Hostname

Für virtuelle VMware-Maschinen. Mit dieser Option werden alle virtuellen Maschinen verarbeitet, die für den Virtual Center- oder ESX-Server definiert sind, der in der Option `vmchost` angegeben ist. Der angegebene Hostname muss mit

dem vollständig qualifizierten Hostnamen oder der IP-Adresse übereinstimmen, der/die in der vCenter-Serveransicht **Hosts und Cluster** angegeben ist.

Alle diesem Host hinzugefügten virtuellen Maschinen werden bei der Sicherungs- und Zurückschreibungsverarbeitung automatisch berücksichtigt. Die virtuellen Maschinen müssen darüber hinaus auf dem ESX-Server ausgeführt werden, der durch den Hostnamen angegeben ist, damit sie berücksichtigt werden. Sie dürfen nicht ausgeschaltet sein.

Dieser Parameter kann mehrere durch Kommas getrennte ESX-Server umfassen. Wenn das Virtual Center mehrere ESX-Server enthält, kann mit dieser Option nicht der ESX-Server bestimmt werden, auf dem eine Momentaufnahme erstellt wird. Der ESX-Server, auf dem eine Momentaufnahme erstellt wird, wird durch den VMware VirtualCenter-Web-Service bestimmt.

Wenn Sie eine direkte Verbindung zu einem ESXi- oder ESX-Host herstellen, ist die Option `vmhost` nur gültig, wenn **vmhost** der Server ist, zu dem Sie eine Verbindung herstellen. Andernfalls wird eine Warnung an die Konsole gesendet und in der Datei `dsmserror.log` aufgezeichnet; sie wird auch als Serverereignisnachricht aufgezeichnet.

Wenn die Option `vmnablenamebackups` auf `yes` gesetzt ist und VM-Schablonen Teil der Domäne sind, werden sie bei der Sicherung berücksichtigt.

Einschränkung: VMware-Schablonen für virtuelle Maschinen können nicht gesichert werden, wenn sie sich auf einem ESX- oder ESXi-Host befinden, weil ESX- und ESXi-Hosts Schablonen nicht unterstützen.

`vmfolder=Ordnername`

Für virtuelle VMware-Maschinen. Mit dieser Option werden alle virtuellen Maschinen verarbeitet, die für den Virtual Center- oder ESX-Server definiert sind, der in der Option `vmhost` angegeben ist. Die virtuellen Maschinen müssen sich außerdem in dem VMware-Ordner befinden, der durch den Ordnernamen angegeben ist. Der Ordnername kann mehrere VMware-Ordner umfassen, die durch Kommas getrennt sind.

`vmhostcluster=Host-Cluster-Name`

Für virtuelle VMware-Maschinen. Mit dieser Option werden alle virtuellen Maschinen verarbeitet, die für den Virtual Center- oder ESX-Server definiert sind, der in der Option `vmhost` angegeben ist. Die virtuellen Maschinen müssen darüber hinaus auf dem ESX-Host-Cluster ausgeführt werden, der durch den Host-Cluster-Namen angegeben ist. Sollen mehrere Host-Cluster-Namen angegeben werden, trennen Sie die Clusternamen durch Kommas:

`VMHOSTCLUSTER=cluster1,cluster2.`

Wenn die Option `vmnablenamebackups` auf `yes` gesetzt ist und VM-Schablonen Teil der Domäne sind, werden sie bei der Sicherung berücksichtigt. Ein VMware-Host-Cluster ist nicht verfügbar, wenn Sie eine direkte Verbindung zu einem ESXi- oder ESX-Host herstellen. Wenn Sie eine direkte Verbindung zu einem ESXi-/ESX-Host herstellen und eine Domäne verarbeitet wird, die einen Host-Cluster enthält, wird eine Warnung an die Konsole gesendet und in der Datei `dsmserror.log` aufgezeichnet; sie wird auch als Serverereignisnachricht aufgezeichnet.

`vmdatastore=Datenspeichername`

Für virtuelle VMware-Maschinen. Mit dieser Option werden alle virtuellen Maschinen verarbeitet, die für den Virtual Center- oder ESX-Server definiert sind, der in der Option `vmhost` angegeben ist. Die konfigurierte Datenspeicherposition für eine virtuelle Maschine muss dem durch *Datenspeichername* angegebe-

nen Datenspeichernamen entsprechen. Der Datenspeichernamen kann mehrere durch Kommas getrennte Datenspeicher umfassen:

`VMDATASTORE=datastore1,datastore2`

Die Platte (vmdk-Dateien) virtueller Maschinen kann sich in mehreren Datenspeichern befinden, es gibt jedoch nur eine Standarddatenspeicherposition. Diese Standarddatenspeicherposition ist in der Konfiguration der virtuellen Maschine definiert und ist immer mit der Position der Konfigurationsdatei der virtuellen Maschine (.vmx-Datei) identisch. Wird eine Maschine mithilfe eines Domänenschlüsselworts für die Sicherung ausgewählt, werden die Konfigurationsdatei der virtuellen Maschine und alle Platten der virtuellen Maschine in die Sicherung eingeschlossen, einschließlich der Platten, die sich nicht in dem als Domäne angegebenen Datenspeicher, sondern in einem anderen Datenspeicher befinden.

vmresourcepool=Name_des_Ressourcenpools

Für virtuelle VMware-Maschinen. Mit dieser Option werden alle virtuellen Maschinen verarbeitet, die für den Virtual Center-Server definiert sind, der in der Option `vmhost` angegeben ist. Die virtuellen Maschinen müssen auch in dem VMware-Ressourcenpool vorhanden sein, der durch den Ressourcenpoolnamen angegeben ist. Der Name des Ressourcenpools kann mehrere durch Kommas getrennte Namen von Ressourcenpools umfassen, beispielsweise:

`VMRESOURCEPOOL=Ressourcenpool1, Ressourcenpool2`

vmhostfolder=Name_des_Hostordners

Für virtuelle VMware-Maschinen. Mit dieser Option werden alle virtuellen Maschinen verarbeitet, die für den Virtual Center-Server definiert sind, der in der Option `vmhost` angegeben ist. Die virtuellen Maschinen müssen sich außerdem in dem VMware-Hostordner befinden, der durch den Hostordnernamen angegeben ist. Der Name des Hostordners kann mehrere durch Kommas getrennte Namen von VMware-Hostordnern umfassen, beispielsweise:

`VMHOSTFOLDER=Hostordner1,Hostordner2`

vmdatacenter=Datencentername

Für virtuelle VMware-Maschinen. Mit dieser Option werden alle virtuellen Maschinen verarbeitet, die für den Virtual Center-Server definiert sind, der in der Option `vmhost` angegeben ist. Die virtuellen Maschinen müssen sich außerdem in dem VMware-Datencenter befinden, das durch den Datencenternamen angegeben ist. Der Datencentername kann mehrere durch Kommas getrennte Namen von Datencentern umfassen, beispielsweise:

`VMDATACENTER=Datencenter1,Datencenter2`

Tipp: Wenn Sie mehr als einen Containertyp angeben, beispielsweise `vmfolder=Ordner1` und `vmhostcluster=Cluster2`, werden alle virtuellen Maschinen, die in `Ordner1` und `Cluster2` enthalten sind, geschützt. Die virtuellen Maschinen müssen nicht sowohl in `Ordner1` als auch in `Cluster2` vorhanden sein.

Sie können die virtuellen Maschinen wie in diesem Beispiel gezeigt angeben:
`domain.vmfull=vmfolder=Ordner1;vmhostcluster=Cluster2`

Beispiele für virtuelle VMware-Maschinen

Optionsdatei:

Alle virtuellen Maschinen in VM-Gesamtsicherungsoperationen einschließen.

`domain.vmfull all-vm`

Alle virtuellen Maschinen mit Ausnahme der Maschinen mit dem Namenssuffix `_test` in VM-Gesamtsicherungsoperationen einschließen.

```
domain.vmfull all-vm;-vm=*_test
```

Alle virtuellen Maschinen mit dem Betriebssystem Windows in VM-Gesamtsicherungsoperationen einschließen.

```
domain.vmfull all-windows
```

Alle virtuellen Maschinen in den Cluster-Servern 1, 2 und 3 in VM-Gesamtsicherungsoperationen einschließen.

```
domain.vmfull vmhostcluster=cluster1,cluster2,cluster3
```

Alle Daten virtueller Maschinen in dem Datenspeicher `datastore1` in VM-Gesamtsicherungsoperationen einschließen.

```
domain.vmfull vmdatastore=datastore1
```

Alle virtuellen Maschinen in VM-Gesamtsicherungsoperationen einschließen, jedoch die virtuellen Maschinen `testvm1` und `testvm2` ausschließen.

```
domain.vmfull all-vm;-VM=testvm1,testvm2
```

Die virtuellen Maschinen, die in den VM-Ordnern mit den Namen `lab1` und `lab2` definiert sind, in VM-Gesamtsicherungsoperationen einschließen.

```
domain.vmfull vmfolder=lab1,lab2
```

Alle virtuellen Maschinen auf den ESX-Hosts mit den Namen „brovar“, „doomzoo“ und „kepler“ in VM-Gesamtsicherungsoperationen einschließen.

```
domain.vmfull vmhost=brovar.example.com,  
doomzoo.example.com,kepler.example.com
```

Alle virtuellen Maschinen in den VMware-Ressourcenpools `Ressourcenpool_A` und `Ressourcenpool_B` in VM-Gesamtsicherungsoperationen einschließen.

```
domain.vmfull vmresourcepool=Ressourcenpool_A,Ressourcenpool_B
```

Die virtuellen Maschinen, die in den VMware-Hostordnern mit den Namen `Hostordner1` und `Hostordner2` definiert sind, in VM-Gesamtsicherungsoperationen einschließen.

```
domain.vmfull vmhostfolder=Hostordner1,Hostordner2
```

Alle virtuellen Maschinen im VMware-Datencenter `dc1` in VM-Gesamtsicherungsoperationen einschließen.

```
domain.vmfull vmdatacenter=dc1
```

Zugehörige Verweise:

„Unterstützte Datenschutztags“ auf Seite 829

„Exclude.vmdisk“ auf Seite 443

„Include.vmdisk“ auf Seite 482

Dontload

Linux-x86_64-Clients können mit der Option `dontload` das Laden bestimmter Plugin-Bibliotheken beim Starten des Clients für Sichern/Archivieren unterdrücken.

Das Paket `TIVsm_BAhdw.x86_64`, das in Verteilungen von Linux x86_64 bereitgestellt wird, enthält Software, die zur Unterstützung von Momentaufnahmeteilsicherungen für NetAPP- und N-Series-Dateiserver benötigt wird. Wenn dieses Paket auf einem Linux x86_64-System installiert wird, das zur Ausführung von Operationen einer Einheit zum Versetzen von Daten für eine virtuelle Maschine verwendet

wird, haben die Dateien in diesem Paket zur Folge, dass alle VMware-Sicherungsoperationen fehlschlagen. Wenn diese Fehler auftreten, wird die folgende Nachricht angezeigt:

ANS8811E

VMware-Operationen können nicht ausgeführt werden, wenn das Hardware-Plug-in-Produkt TIVsm-BAhdw installiert und geladen ist. Deinstallieren Sie das Hardwareprodukt TIVsm-BAhdw oder definieren Sie die Option DONTLOAD PIHDW in der Optionsdatei, um zu verhindern, dass das Hardware-Plug-in geladen wird.

Verwenden Sie diese Option, um das Laden der Plug-in-Bibliothek in den Arbeitsspeicher (RAM) beim Starten des Clients zu verhindern. Alternativ können Sie das Paket TIVsm_BAhdw deinstallieren, falls es nicht für Momentaufnahmeoperationen benötigt wird.

Unterstützte Clients

Diese Option ist nur für Linux-x86_64-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Syntax

►► DONTLoad PIHDW ◀◀

Parameter

PIHDW

Gibt an, dass das Hardware-Plug-in (TIVsm-BAhdw) beim Starten des Clients nicht in den Arbeitsspeicher (RAM) geladen wird. Verwenden Sie diese Option bei Clients für Sichern/Archivieren, bei denen das Hardware-Plug-in installiert ist, um zu verhindern, dass das Plug-in Fehler verursacht, wenn Sicherungs-/Archivierungsoperationen auf virtuellen VMware-Maschinen ausgeführt werden. Für die Option dontload gibt es keinen Standardwert.

Um festzustellen, ob das Plug-in installiert ist, geben Sie den folgenden Befehl ein und prüfen Sie die Ausgabe.

```
rpm -q -a | grep TIV
```

Falls die Ausgabe ein Paket enthält, das mit der Angabe „TIVsm-BAhdw“ (gefolgt von einer Versionszeichenfolge) beginnt, ist das Paket für das Hardware-Plug-in installiert.

Beispiele

Optionsdatei:

```
DONTLoad PIHDW
```

Befehlszeile:

Nicht zutreffend. Verwenden Sie diese Option nicht in der Befehlszeile.

Zugehörige Verweise:

„Backup VM“ auf Seite 710

Dynamicimage

Verwenden Sie die Option `dynamicimage` im Befehl **backup image** oder mit der Option `include.image`, um anzugeben, dass Sie eine dynamische Imagesicherung ausführen wollen.

Unterstützte Clients

Diese Option ist für AIX-, Solaris- und alle Linux-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie die Anweisung `include.image` mit dem Wert `dynamicimage` in die Serverzeilengruppe Ihrer Systemoptionsdatei `dsm.sys` ein. Sie können diese Option auch mit Hilfe des Profileditors setzen.

Syntax

►►—`DYNAMICImage`— *Wert* —◄◄

Parameter

Wert

Gibt einen der folgenden Werte an:

yes

Verwenden Sie diese Option nur, wenn der Datenträger nicht abgehängt und mit Lesezugriff erneut angehängt werden kann. Der Client sichert den Datenträger unverändert, ohne erneutes schreibgeschütztes Anhängen. Die Sicherung kann beschädigt werden, wenn Anwendungen auf den Datenträger schreiben, während die Sicherung ausgeführt wird. Führen Sie in diesem Fall `fsck` nach einer Zurückschreibung aus und hängen Sie das Dateisystem manuell an, um wieder Zugriff auf den Datenträger zu erlangen. Diese Option ist für AIX-, Solaris- und alle Linux-Clients gültig.

Anmerkung: Diese Option ist für AIX JFS2-Dateisysteme nicht zulässig.

- no** Verwenden Sie diese Option, wenn Sie keine dynamische Imagesicherung ausführen wollen. Dies ist der Standardwert. Das Standardverhalten hängt von der Plattform und dem Dateisystemtyp ab. Für Plattformen und Dateisysteme, die Momentaufnahmen unterstützen, namentlich AIX JFS2-Dateisysteme und LINUX LVM-Dateisysteme, ist der Standardwert die Imagesicherung auf Momentaufnahmebasis. Für alle anderen UNIX-Plattformen und Dateisystemen ist der Standardwert die statische Imagesicherung.

Beispiele

Optionsdatei:

```
include.image /kalafs1 dynamicimage=yes
```

Befehlszeile im Sicherungsimage:

```
dynamicimage=yes
```

Efsdecrypt

Mit der Option `efsdecrypt` können Sie steuern, ob Dateien, die von einem verschlüsselten AIX-Dateisystem (AIX-EFS) verschlüsselt wurden, in verschlüsseltem oder in entschlüsseltem Format gelesen werden sollen.

Der Standardwert der Option `efsdecrypt` ist `no`, d. h., die verschlüsselten oder unformatierten Daten werden gesichert. Wenn Sie `yes` angeben, werden die Dateien im Klartext gesichert. Dies bedeutet, dass sie als normale Dateien gesichert werden, als ob sie in unverschlüsseltem Format im Dateisystem gespeichert wären.

Wichtig: Immer, wenn Sie eine Sicherung ausführen, die auf einem EFS verschlüsselte Dateien einschließt, müssen Sie sicherstellen, dass Sie die korrekte Spezifikation der Option `efsdecrypt` verwenden. Falls sich der Optionswert `efsdecrypt` zwischen zwei Teilsicherungen ändert, werden alle verschlüsselten Dateien auf EFS-Dateisystemen erneut gesichert, selbst wenn sie sich seit der letzten Sicherung nicht geändert haben. Wenn Sie z. B. eine Teilsicherung verschlüsselter Dateien ausführen, die zuvor als "unformatiert" gesichert wurden, müssen Sie sicherstellen, dass für `efsdecrypt` der Wert `no` angegeben wird. Wenn Sie für `efsdecrypt` den Wert `yes` angeben, werden alle Dateien im Klartext erneut gesichert, selbst wenn sie unverändert sind. Verwenden Sie diese Option also mit Vorsicht.

Anmerkung: Dies ist eine globale Option, die auf die gesamte Sicherung angewendet wird. Es sind zwei separate Aufrufe des Clients erforderlich, um einige verschlüsselte Dateien als unformatierte Daten und andere als Klartext zu sichern.

Unterstützte Clients

Diese Option ist für AIX-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Datei `dsm.sys` oder in die Clientbenutzeroptionsdatei (`dsm.opt`) ein. In der Datei `dsm.sys` müssen Sie diese Option innerhalb einer Ser-verzeilengruppe einfügen.

Syntax



Parameter

No Verschlüsselte Dateien werden in verschlüsseltem oder unformatiertem Datenformat gelesen, und die Verschlüsselung und Komprimierung von IBM Spectrum Protect ist zwangsweise unterbrochen. Dies ist der Standardwert.

Yes Verschlüsselte Dateien werden in entschlüsseltem Format oder Klartextformat gelesen.

Beispiele

Optionsdatei:

```
EFSDecrypt yes
```

Befehlszeile:
-EFSDecrypt=no

Enablearchiveretentionprotection

Mit der Option `enablearchiveretentionprotection` kann der Client eine Verbindung zum IBM Spectrum Protect for Data Retention-Server herstellen. Dieser stellt sicher, dass Archivierungsobjekte erst dann auf dem Server gelöscht werden, wenn auf Richtlinien basierende Aufbewahrungskriterien für dieses Objekt erfüllt wurden.

Diese Option wird ignoriert, wenn der Client eine Verbindung mit einem Server herstellt, der nicht für Aufbewahrungsschutz aktiviert ist. Lautet die Option `no` (der Standardwert) und wird ein Versuch unternommen, eine Verbindung zum Datenaufbewahrungsserver herzustellen, wird die Verbindung zurückgewiesen.

Der Datenaufbewahrungsserver ist speziell für diese Aufgabe konfiguriert, d. h., die normale Sicherungs- oder Zurückschreibungsverarbeitung wird vom Server zurückgewiesen. Ist ein Client mit einem Datenaufbewahrungsserver verbunden, sind die folgenden Befehle nicht verfügbar. Wenn Sie versuchen, diese Befehle zu verwenden, wird eine Nachricht angezeigt, die besagt, dass sie mit diesem Server nicht gültig sind.

- **incremental**
- **backup** (alle Unterbefehle)
- **selective**
- **restore** (alle Unterbefehle mit Ausnahme von **restore backupset** -location=file oder -location=tape)

Anmerkung: Bei **restore backupset** -location=file oder -location=tape wird keinerlei Verbindung zu einem Server (außer dem virtuellen Server) hergestellt und somit wird der Befehl unter keinen Umständen blockiert.

- **restart restore**
- **delete backup**
- **delete group**
- **expire**
- Alle Abfragen *außer*
 - **query access**
 - **query archive**
 - **query filespace**
 - **query inclexcl**
 - **query managementclass**
 - **query node**
 - **query options**
 - **query schedule**
 - **query session**
 - **query systeminfo**
 - **query tracestatus**

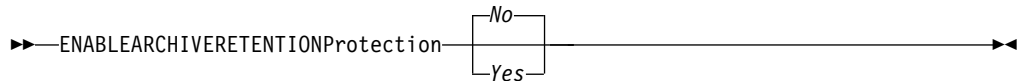
Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Diese Option ist nur in der Datei `dsm.sys` *innerhalb* einer Serverzeilengruppe gültig und nicht in einer Clientoptionsgruppe des Servers. Sie ist auch nicht in der Befehlszeile gültig.

Syntax



Parameter

No Die Verbindung zum Datenaufbewahrungsserver wird zurückgewiesen. Dies ist der Standardwert.

Yes

Der Client stellt eine Verbindung zu einem Datenaufbewahrungsserver her.

Enablededupcache

Mit der Option `enablededupcache` geben Sie an, ob bei der clientseitigen Deduplizierung von Daten ein Cache verwendet werden soll. Die Verwendung eines lokalen Cache kann den Datenaustausch im Netz zwischen dem IBM Spectrum Protect-Server und dem Client reduzieren.

Wenn Sie eine Sicherungs- oder Archivierungsoperation mit aktiviertem Cache für die Deduplizierung von Daten ausführen, wird die Spezifikation der gesicherten oder archivierten Datenbereiche in der Cachedatenbank gespeichert. Bei der nächsten Ausführung einer Sicherung oder Archivierung fragt der Client den Cache für die Deduplizierung von Daten ab und ermittelt die Datenbereiche, die bereits zuvor auf dem Server gespeichert wurden. Datenbereiche, die mit Datenbereichen auf dem Server identisch sind, werden nicht erneut an den Server gesendet.

Wenn der Server und der Cache nicht synchronisiert sind, wird der Cache entfernt und ein neuer Cache erstellt.

Zu jedem Zeitpunkt kann nur jeweils ein Prozess auf den verteilten Cache für die Deduplizierung von Daten zugreifen. Parallele Sicherungsinstanzen auf einer Workstation, die denselben Server und Speicherpool verwenden, müssen entweder eindeutige Knotennamen oder eindeutige Cachespezifikationen benutzen. Auf diese Weise können alle Instanzen lokale Caches verwenden und die clientseitige Deduplizierung von Daten optimieren.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Auch die IBM Spectrum Protect-API unterstützt diese Option.

Optionsdatei

Fügen Sie diese Option in die Systemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein. Sie können diese Option mit dem Kontrollkästchen **Deduplizierung > Deduplizierungscache aktivieren** im Profileditor definieren. Diese Option kann in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server definiert werden.

Syntax



Parameter

Yes

Gibt an, dass Sie den Cache für die Deduplizierung von Daten aktivieren wollen. Ist die Deduplizierung von Daten nicht aktiviert, ist diese Einstellung nicht gültig. Yes ist der Standardwert für den Client für Sichern/Archivieren. No ist der Standardwert für die IBM Spectrum Protect-API.

No Gibt an, dass Sie den Cache für die Deduplizierung von Daten nicht aktivieren wollen.

Beispiele

Optionsdatei:

```
enablededupcache no
```

Befehlszeile:

```
-enablededupcache=no
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Zugehörige Verweise:

„Deduplication“ auf Seite 394

„Dedupcachepath“ auf Seite 393

„Dedupcachesize“ auf Seite 394

Enableinstrumentation

Standardmäßig werden Instrumentierungsdaten automatisch vom Client für Sichern/Archivieren und von der IBM Spectrum Protect-API erfasst, um Leistungsengpässe während der Sicherungs- und Zurückschreibungsverarbeitung zu identifizieren. Um die Instrumentierung zu inaktivieren oder später zu aktivieren, verwenden Sie die Option `enableinstrumentation`.

Wenn diese Option aktiviert ist, müssen Sie nicht darauf warten, dass Sie vom IBM Kundendienst aufgefordert werden, Leistungsdaten zu erfassen, wenn ein Problem auftritt. Stattdessen können die Daten bei jeder Ausführung einer Sicherungs- oder Zurückschreibungsoperation erfasst werden. Diese Funktion kann nützlich sein, da Sie das Problem nicht reproduzieren müssen, um Leistungsdaten zu erfassen. Die Informationen werden bereits vom Client erfasst.

Diese Option ersetzt die Optionen `-TESTFLAG=instrument:detail`, `-TESTFLAG=instrument:API` und `-TESTFLAG=instrument:detail/API`, die in vorherigen Versionen des Clients und der API verwendet werden.

Für jeden Prozess werden die folgenden Typen von Leistungsinstrumentierungsdaten erfasst:

- Die Aktivitätsnamen für jeden Thread (wie beispielsweise File I/O, Data Verb, Compression und Transaction), die durchschnittliche abgelaufene Zeit pro Aktivität und die Häufigkeit der Aktivität.

- Die Gesamtzeit der Aktivität für jeden Thread.
- Der Befehl, der ausgegeben wurde, und die Optionen, die verwendet wurden.
- Die Zusammenfassung des Sicherungs-, Zurückschreibungs- oder Abfragebefehls.

Standardmäßig werden die Leistungsdaten in der Instrumentierungsprotokolldatei (`dsminstr.log`) in dem Verzeichnis gespeichert, das mit der Umgebungsvariablen `DSM_LOG` (oder der Umgebungsvariablen `DSMI_LOG` für API-abhängige Produkte wie z. B. IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server und IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server) angegeben wird. Wenn Sie die Umgebungsvariable `DSM_LOG` nicht definiert haben, wird die Instrumentierungsprotokolldatei im aktuellen Verzeichnis gespeichert (das Verzeichnis, in dem der Befehl **dsmc** ausgegeben wurde).

Sie können wahlweise den Namen und die Position der Instrumentierungsprotokolldatei mit der Option `instrlogname` ändern. Sie können auch die Größe der Protokolldatei steuern, indem Sie die Option `instrlogmax` angeben.

Leistungsdaten werden nicht für die GUI des Clients für Sichern/Archivieren oder die GUI des Web-Clients erfasst.

Leistungsdaten werden für die folgenden Produkte erfasst, wenn die Option `enableinstrumentation` in der Clientoptionsdatei angegeben wird:

- Geplante Sicherungsoperationen auf Dateiebene mit dem Client für Sichern/Archivieren
- Sicherungen mit IBM Spectrum Protect for Virtual Environments: Data Protection for VMware
- Sicherungen mit IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V
- Sicherungen mit IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server
- Sicherungen mit IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server

Leistungsdaten werden auch während der Archivierungs- und Abrufverarbeitung erfasst.

Unterstützte Clients

Diese Option ist für alle Clients und die IBM Spectrum Protect-API gültig.

Optionsdatei

Fügen Sie diese Option in die Clientssystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein.

Tipp: Diese Option ist standardmäßig aktiviert. Daher müssen Sie diese Option normalerweise nicht in die Clientoptionsdatei einfügen, es sei denn, die Option muss inaktiviert werden.

Syntax



Parameter

Yes

Gibt an, dass während der Ausführung von Sicherungs- und Zurückschreibungsoperationen Leistungsdaten erfasst werden sollen. Der Standardwert ist Yes. Er bedeutet, dass Leistungsdaten auch dann erfasst werden, wenn diese Option nicht angegeben wird.

Standardmäßig werden die Leistungsdaten in der Instrumentierungsprotokoll-datei (`dsminstr.log`) in dem Verzeichnis gespeichert, das mit der Umgebungsvariablen `DSM_LOG` angegeben wird. Wenn Sie die Umgebungsvariable `DSM_LOG` nicht definiert haben, wird die Instrumentierungsprotokoll-datei im aktuellen Verzeichnis gespeichert (das Verzeichnis, in dem der Befehl **dsmc** ausgegeben wurde). Ist die Datei nicht vorhanden, erstellt der Client die Datei und fügt der Datei Leistungsdaten hinzu.

No Gibt an, dass während der Ausführung von Sicherungs- und Zurückschreibungsoperationen keine Leistungsdaten erfasst werden sollen. Ist das Instrumentierungsprotokoll vorhanden, werden der Datei keine weiteren Daten hinzugefügt.

Beispiele

Optionsdatei:

```
enableinstrumentation yes
```

Befehlszeile:

```
dsmc sel /home/mydir/* -subdir=yes -enableinstrumentation=yes
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Zugehörige Tasks:

☞ Clientinstrumentierungsdaten erfassen

☞ API-Instrumentierungsdaten erfassen

Zugehörige Verweise:

„Instrlogmax“ auf Seite 492

„Instrlogname“ auf Seite 493

Enablelanfree

Die Option `enablelanfree` gibt an, ob ein verfügbarer LAN-freier Pfad zu einer an ein Speicherbereichsnetz (SAN) angeschlossenen Speichereinheit aktiviert werden soll.

Ein LAN-freier Pfad ermöglicht die Verarbeitung von Sicherungen, Zurückschreibungen, Archivierungen und Abrufen zwischen dem Client für Sichern/Archivieren und der an ein SAN angeschlossenen Speichereinheit.

Zur Unterstützung der LAN-freien Datenversetzung müssen Sie das Programm IBM Spectrum Protect for SAN Storage Agent auf der Client-Workstation installieren und konfigurieren.

Anmerkung:

1. Wenn Sie die Option `enablelanfree` in die Clientoptionsdatei (`dsm.opt`) stellen, während einer Operation jedoch Null (0) Byte über das SAN übertragen wurden, müssen Sie sicherstellen, dass Sie die Daten an eine Verwaltungsklasse binden, die für LAN-frei aktiviert ist.
2. Weitere Informationen über das Zurückschreiben von Sicherungssätzen in einer SAN-Umgebung enthält „**Restore Backupset**“ auf Seite 777.
3. Wenn ein LAN-freier Pfad aktiviert ist, überschreiben die Einstellungen des SAN-Speicheragenten die Clientoptionen `tcpserveraddress`, `tcpport` und `ssl`. Mit dieser Überschreibungsaktion soll sichergestellt werden, dass der Client und der Speicheragent dieselben Serverkommunikationsoptionen verwenden.

Unterstützte Clients

Diese Option ist für AIX- Linux x86_64-, Linux on Power Systems-, Linux on z Systems- und Solaris-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Datei `dsm.sys` innerhalb einer Serverzeilengruppe ein. Sie können diese Option auch durch Auswahl des Kontrollkästchens **LAN-frei aktivieren** auf der Registerkarte **Allgemein** des Profileditors definieren.

Syntax



Parameter

Yes

Gibt an, dass Sie einen verfügbaren LAN-unabhängigen Pfad zu einer an ein Speicherbereichsnetz (SAN) angeschlossenen Speichereinheit aktivieren wollen.

No Gibt an, dass Sie einen LAN-unabhängigen Pfad zu einer an ein Speicherbereichsnetz (SAN) angeschlossenen Speichereinheit nicht aktivieren wollen. Dies ist der Standardwert.

Beispiele

Optionsdatei:

```
enablelanfree yes
```

Befehlszeile:

```
-enablelanfree=yes
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Zugehörige Informationen

Weitere Informationen zur Angabe eines Übertragungsprotokolls zwischen dem Client für Sichern/Archivieren und dem Speicheragenten finden Sie unter „Lanfreemethod“ auf Seite 495.

Encryptiontype

Verwenden Sie die Option `encryptiontype`, um den Algorithmus für die Datenverschlüsselung anzugeben.

Die Option `encryptiontype` wirkt sich nur auf Sicherungs- und Archivierungsoperationen aus. Die Daten, die Sie einschließen, werden in verschlüsselter Form gespeichert; die Verschlüsselung hat keine Auswirkungen auf das gesendete oder empfangene Datenvolumen. Während der Zurückschreibungs- und Abrufoperationen werden die verschlüsselten Daten mit dem entsprechenden Verschlüsselungsalgorithmus entschlüsselt. Die Einstellung dieser Option spielt dabei keine Rolle.

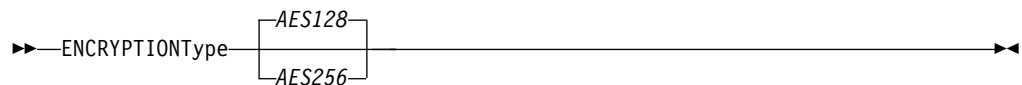
Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auch auf der Registerkarte **Berechtigung** des Profileditors definieren. Der Server kann dies überschreiben.

Syntax



Parameter

AES128

128-Bit-AES-Datenverschlüsselung. 128-Bit-AES ist der Standardwert.

AES256

256-Bit-AES-Datenverschlüsselung. Die 256-Bit-AES-Datenverschlüsselung bietet die stärkste Datenverschlüsselung, die für Sicherungs- und Archivierungsoperationen verfügbar ist.

Beispiele

Optionsdatei:

```
encryptiontype aes128
```

Befehlszeile:

Nicht zutreffend.

Encryptkey

Der Client für Sichern/Archivieren unterstützt die Option zum Verschlüsseln von Dateien, die auf dem IBM Spectrum Protect-Server gesichert oder archiviert werden. Diese Option wird mit der Option `include.encrypt` aktiviert.

Alle Dateien, die mit dem Muster in der Spezifikation `include.encrypt` übereinstimmen, werden verschlüsselt, bevor die Daten an den Server gesendet werden. Es gibt drei Optionen zum Steuern des Schlüssels, mit dem die Dateien verschlüsselt werden (`prompt`, `save` und `generate`). Alle drei Optionen können entweder mit dem Client für Sichern/Archivieren oder mit der IBM Spectrum Protect-API verwendet werden.

Bei dem Chiffrierschlüsselkennwort muss die Groß-/Kleinschreibung beachtet werden und es kann maximal 64 Zeichen enthalten.

Das Chiffrierschlüsselkennwort darf folgende Zeichen enthalten:

A-Z	Alle Buchstaben von A bis Z in Groß- oder Kleinschreibung. Sie können keine Zeichen in der Landessprache angeben.
0-9	Alle Zahlen von 0 bis 9
+	Plus
.	Punkt
_	Unterstreich
-	Silbentrennungsstrich
&	Et-Zeichen

Anmerkung:

1. Die API verfügt über eine alternative Methode für die Angabe von `encryptkey=generate`; die vorherige Option `enableclientencryptkey=yes` kann ebenfalls angegeben werden, um das Generieren der Verschlüsselungsverarbeitung anzufordern.
2. Die API-Option `enableclientencryptkey=yes` wird noch immer unterstützt; daher ist es möglich, beim Verwenden der API eine unzulässige Kombination von Optionen anzugeben. Beispiel: `enableclientencryptkey=yes` und `encryptkey=prompt` oder `encryptkey=save`.
3. Wenn sich widersprechende Werte angegeben werden, gibt die API eine Fehlermeldung zurück.

Achtung: Bei Verwendung der Option `'prompt'` wird Ihr Chiffrierschlüssel nicht in der IBM Spectrum Protect-Kennwortdatei unter UNIX gesichert. Wenn Sie den Schlüssel vergessen, können Ihre Daten nicht wiederhergestellt werden.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientssystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Berechtigung** im Abschnitt **Chiffrierschlüsselkennwort** des Profileditors definieren.

Syntax



Parameter

save

Das Chiffrierschlüsselkennwort wird in der Kennwortdatei des Clients für Sichern/Archivieren gespeichert. Es wird eine Bedienerführung für ein anfängliches Chiffrierschlüsselkennwort ausgegeben und nach der anfänglichen Bedienerführung wird das in der Kennwortdatei gespeicherte Chiffrierschlüsselkennwort für die Sicherungen und Archivierungen der Dateien verwendet, die mit der Spezifikation `include.encrypt` übereinstimmen. Der Schlüssel wird bei Zurückschreibungs- und Abrufoperationen aus der Kennwortdatei abgerufen.

Das Kennwort kann maximal 64 Byte umfassen.

Wird für eine API-Anwendung die Option `save` angegeben, muss das anfängliche Schlüsselkennwort von der Anwendung, die die API verwendet, im Funktionsaufruf `dsmInitEx` zur Verfügung gestellt werden. Die API selbst gibt keine Bedienerführung an den Benutzer aus, sondern verlässt sich darauf, dass die Anwendung den Benutzer, falls notwendig, durch Bedienerführung zur Eingabe auffordert.

Dieser Parameter ist der Standardwert.

Anmerkung: Es gelten die folgenden Einschränkungen:

- Diese Option kann nur verwendet werden, wenn zusätzlich `passwordaccess generate` angegeben ist.
- Der Rootbenutzer oder ein berechtigter Benutzer muss das anfängliche Chiffrierschlüsselkennwort angeben.

prompt

Die Verwaltung des Chiffrierschlüsselkennworts wird vom Benutzer zur Verfügung gestellt. Der Benutzer muss das Chiffrierschlüsselkennwort angeben, wenn der Client eine Sicherung oder Archivierung startet. Eine Bedienerführung für dasselbe Kennwort wird ausgegeben, wenn die verschlüsselte Datei zurückgeschrieben oder abgerufen wird.

Dieses Kennwort kann maximal 64 Byte umfassen.

Wird für eine API-Anwendung die Option `prompt` angegeben, muss das Schlüsselkennwort von der Anwendung, die die API verwendet, im Funktionsaufruf `dsmInitEx` zur Verfügung gestellt werden. Die API selbst gibt keine Bedienerführung an den Benutzer aus, sondern verlässt sich darauf, dass die Anwendung den Benutzer, falls notwendig, durch Bedienerführung zur Eingabe auffordert.

generate

Ein Chiffrierschlüsselkennwort wird dynamisch generiert, wenn der Client eine Sicherung oder Archivierung startet. Dieses generierte Schlüsselkennwort wird für die Sicherungen der Dateien verwendet, die mit der Spezifikation `include.encrypt` übereinstimmen. Das generierte Schlüsselkennwort wird in verschlüsselter Form auf dem IBM Spectrum Protect-Server aufbewahrt. Das Schlüsselkennwort wird an den Client zurückgegeben, damit die Datei in Zurückschreibungs- und Abrufoperationen entschlüsselt werden kann.

Beispiele

Optionsdatei:

`encryptkey prompt`

Befehlszeile:

Nicht zutreffend.

Errorlogmax

Die Option `errorlogmax` gibt die maximale Größe des Fehlerprotokolls in Megabyte an. Der Standardname des Fehlerprotokolls lautet `dsmerror.log`.

Der Protokollumlauf wird durch die Option `errorlogmax` gesteuert. Wenn `errorlogmax` auf null (0) gesetzt ist, ist die Größe des Protokolls unbegrenzt. Es gibt keinen „Umlauf“ protokollierter Einträge, wodurch auch keine älteren protokollierten Einträge überschrieben werden. Wenn `errorlogmax` nicht auf null gesetzt ist, überschreiben die neuesten Protokolleinträge die ältesten Protokolleinträge, sobald die Protokolldatei ihre maximale Größe erreicht.

Die Protokollbereinigung wird durch die Option `errorlogretention` gesteuert. Für bereinigte Protokolle wird kein Umlauf durchgeführt. Stattdessen werden Protokolleinträge, deren Alter die mit der Option `errorlogretention` angegebene Anzahl von Tagen übersteigt, aus der Protokolldatei entfernt.

Wenn Sie vom Protokollumlauf (Option `errorlogmax`) zur Protokollbereinigung (Option `errorlogretention`) wechseln, werden alle vorhandenen Protokolleinträge aufbewahrt, und das Protokoll wird mit den neuen Kriterien von `errorlogretention` bereinigt. Bereinigte Protokolleinträge werden in einer Datei mit dem Namen `dsmerlog.pru` gespeichert.

Wenn Sie von der Protokollbereinigung (Option `errorlogretention`) zum Protokollumlauf (Option `errorlogmax`) wechseln, werden alle Sätze im vorhandenen Protokoll in die Protokolldatei `dsmerlog.pru` kopiert, das vorhandene Protokoll wird geleert und die Protokollierung beginnt dann mit den neuen Protokollumlaufbedingungen.

Wenn Sie lediglich den Wert der Option `errorlogmax` ändern, wird das vorhandene Protokoll erweitert oder gekürzt, um der neuen Größe zu entsprechen. Wird der Wert verkleinert, werden die ältesten Einträge gelöscht, um die Datei auf die neue Größe zu verkleinern.

Wird weder `errorlogmax` noch `errorlogretention` angegeben, kann das Fehlerprotokoll uneingeschränkt wachsen. Sie müssen den Protokollinhalt manuell verwalten, um zu verhindern, dass das Protokoll die Plattenressourcen verbraucht. Wenn das Protokoll ohne eine der beiden Optionen erstellt wurde und wenn Sie später einen Befehl mit der Option `errorlogretention` ausgeben, wird das Protokoll mit dem angegebenen Wert für die Aufbewahrungsdauer bereinigt. Wenn das Protokoll ohne eine der beiden Optionen erstellt wurde und wenn Sie später einen Befehl mit der Option `errorlogmax` ausgeben, wird das vorhandene Protokoll als bereinigtes Protokoll behandelt. Das heißt, der Inhalt der Datei `dsmerror.log` wird in eine Datei mit dem Namen `dsmerlog.pru` kopiert, in `dsmerror.log` werden neue Protokolleinträge erstellt und es findet ein Protokollumlauf statt, wenn das Protokoll seine maximale Größe erreicht.

Anmerkung: Wenn Sie für `errorlogmax` einen Wert ungleich null angeben (wodurch der Protokollumlauf aktiviert wird), können Sie nicht die Option `errorlogretention` verwenden, um bereinigte Protokolle zu erstellen. Für Protokolle kann entweder eine Bereinigung oder ein Umlauf durchgeführt werden, aber nicht beides.

Mit der Option `errorlogmax` erstellte Protokolle enthalten einen Protokollkopfsatz, der Informationen wie in dem folgenden Beispieldatensatz enthält:

```
LOGHEADERREC 661 104857600 IBM Spectrum Protect 8.1.0 Fri Dec 9 06:46:53 2011
```

Beachten Sie, dass die Datums- und Zeitmarkenangaben im Text von LOGHEADERREC nicht mithilfe der Einstellungen übersetzt oder formatiert werden, die in den Optionen `dateformat` und `timeformat` angegeben sind.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein.

Sie können diese Option auch auf der Registerkarte **Clientvorgaben** in der grafischen Benutzerschnittstelle definieren. Wählen Sie hierfür **Umlauf für Fehlerprotokolldatei aktivieren** aus und geben Sie einen Wert ungleich null für die **maximale Größe** der Protokolldatei an. Geben Sie für die **maximale Größe** null an, um den Umlauf der Protokolldatei zu verhindern. Wenn die maximale Größe auf null gesetzt ist, bleibt die Option **Umlauf für Fehlerprotokolldatei aktivieren** wirkungslos. Es findet kein Protokollumlauf statt, wenn die **maximale Größe** auf null gesetzt ist.

Syntax

►►—ERRORLOGMAX— —*Größe*—►►

Parameter

Größe

Gibt die maximale Größe für die Protokolldatei in Megabyte an. Der Wertebereich ist 0 bis 2047. Der Standardwert ist 0, wodurch der Protokolldateiumlauf inaktiviert und die Größe der Protokolldatei unbeschränkt wird.

Beispiele

Optionsdatei:

```
errorlogmax 2000
```

Befehlszeile:

```
-errorlogmax=2000
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Errorlogname

Diese Option gibt den vollständig qualifizierten Pfad und Dateinamen der Datei an, die die Fehlernachrichten enthält.

Der Wert für diese Option überschreibt die Umgebungsvariable `DSM_LOG`. Die Dateien `dsmwebcl.log` und `dsm sched.log` werden in demselben Verzeichnis erstellt wie die Fehlerprotokolldatei, die Sie mit der Option `errorlogname` angeben.

Für Mac OS X ist die Standardposition eine der folgenden Positionen:

```
~/Library/Logs/tivoli/tsm/  
/Library/Logs/tivoli/tsm/
```

dsmerror.log kann keine symbolische Verbindung sein.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Allgemein** über die Schaltfläche **Fehlerprotokoll auswählen** im Profileditor definieren.

Syntax

►—ERRORLOGName— *—Dateispezifikation—* ◀

Parameter

Dateispezifikation

Der vollständig qualifizierte Pfad und Name der Datei, in der Fehlerprotokollinformationen gespeichert werden sollen. Wenn ein Teil des von Ihnen angegebenen Pfads nicht vorhanden ist, versucht der Client, ihn zu erstellen.

Die Datei dsmerror.log kann keine symbolische Verbindung sein.

Beispiele

Optionsdatei:

```
errorlogname /tmp/tsmerror.log
```

Befehlszeile:

```
-errorlogname=/tmp/tsmerror.log
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Errorlogretention

Die Option errorlogretention legt fest, wieviele Tage Fehlerprotokolleinträge aufbewahrt werden sollen, bevor sie bereinigt werden, und ob die bereinigten Einträge in anderen Dateien gespeichert werden sollen.

Das Fehlerprotokoll wird bereinigt, wenn der erste Fehler in das Protokoll geschrieben wird, nachdem eine Clientsitzung gestartet wurde. Wenn als einzige Sitzung der Client-Scheduler täglich ununterbrochen aktiv ist, wird das Fehlerprotokoll möglicherweise nicht erwartungsgemäß bereinigt. Stoppen Sie die Sitzung und starten Sie sie erneut, damit der Scheduler das Fehlerprotokoll bereinigen kann.

Wenn Sie von der Protokollbereinigung (Option errorlogretention) zum Protokollumlauf (Option errorlogmax) wechseln, werden alle Sätze im vorhandenen Protokoll in die Protokolldatei dsmerlog.pru kopiert, das vorhandene Protokoll wird geleert und die Protokollierung beginnt dann mit den neuen Protokollumlaufbedingungen.

Wenn Sie vom Protokollumlauf (Option errorlogmax) zur Protokollbereinigung (Option errorlogretention) wechseln, werden alle vorhandenen Protokolleinträge aufbewahrt, und das Protokoll wird mit den neuen Kriterien von

errorlogretention bereinigt. Bereinigte Protokolleinträge werden in einer Datei mit dem Namen dsmerlog.pru gespeichert.

Wird weder errologmax noch errorlogretention angegeben, kann das Fehlerprotokoll uneingeschränkt wachsen. Sie müssen den Protokollinhalt manuell verwalten, um zu verhindern, dass das Protokoll die Plattenressourcen verbraucht. Wenn das Protokoll ohne eine der beiden Optionen erstellt wurde und wenn Sie später einen Befehl mit der Option errorlogretention ausgeben, wird das Protokoll mit dem angegebenen Wert für die Aufbewahrungsdauer bereinigt. Wenn das Protokoll ohne eine der beiden Optionen erstellt wurde und wenn Sie später einen Befehl mit der Option errologmax ausgeben, wird das vorhandene Protokoll als bereinigtes Protokoll behandelt. Das heißt, der Inhalt der Datei dsmerror.log wird in eine Datei mit dem Namen dsmerlog.pru kopiert, in dsmerror.log werden neue Protokolleinträge erstellt und es findet ein Protokollumlauf statt, wenn das Protokoll seine maximale Größe erreicht.

Anmerkung: Wenn Sie die Option errorlogretention angeben, um bereinigte Protokolle zu erstellen, können Sie die Option errologmax nicht angeben. Für Protokolle kann entweder eine Bereinigung oder ein Umlauf durchgeführt werden, aber nicht beides.

Unterstützte Clients

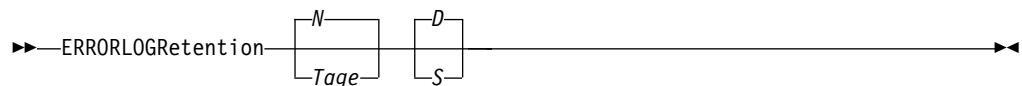
Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Sie können diese Option auch auf der Registerkarte **Clientvorgaben** in der grafischen Benutzerschnittstelle definieren. Wählen Sie hierfür **Alte Einträge bereinigen** aus und geben Sie einen Wert für **Einträge bereinigen, die älter sind als** an. Durch Auswahl der Option **Bereinigte Einträge sichern** werden die bereinigten Protokolleinträge in der Protokolldatei dsmerlog.pru gespeichert.

Syntax



Parameter

N oder Tage

Gibt die Wartezeit vor dem Bereinigen des Fehlerprotokolls an.

N Das Fehlerprotokoll nicht bereinigen. Das Fehlerprotokoll kann unendlich groß werden. Dies ist der Standardwert.

Tage

Die Anzahl Tage, die Protokolldateieinträge aufbewahrt werden sollen, bevor das Protokoll bereinigt wird. Der Wertebereich ist 0 bis 9999.

D oder S

Gibt an, ob bereinigte Einträge gesichert werden sollen. Ein Leerzeichen oder ein Komma eingeben, um diesen Parameter vom vorherigen zu trennen.

- D* Die Fehlerprotokolleinträge löschen, wenn das Protokoll bereinigt wird. Dies ist der Standardwert.
- S* Die Fehlerprotokolleinträge sichern, wenn das Protokoll bereinigt wird. Die bereinigten Einträge werden aus dem Fehlerprotokoll in die Datei `dsmerlog.pru` kopiert, die sich in demselben Verzeichnis wie die Datei `dsmerror.log` befindet.

Beispiele

Optionsdatei:

Protokolleinträge in der Datei `dsmerror.log`, die älter als 365 Tage sind, bereinigen und die bereinigten Einträge in `dsmerlog.pru` speichern.
`errorlogretention 365 S`

Befehlszeile:

`-errorlogr=365,S`

Optionsdatei:

Protokolleinträge in der Datei `dsmerror.log`, die älter als 365 Tage sind, bereinigen und die bereinigten Einträge nicht speichern.
`errorlogretention 365 D`

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Exclude-Optionen

Verwenden Sie die Exclude-Optionen, um Objekte von den Sicherungs-, Image- oder Archivierungsservices auszuschließen.

Beispielsweise können Sie die folgenden Informationstypen ausschließen:

- Alle temporären Dateien
- Alle lokalen Caches von Netzdateien
- Alle Dateien, die kompilierten Objektcode enthalten, den Sie auf einfache Weise mit anderen Methoden erneut erstellen können
- Ihre Betriebssystemdateien

Sie können bestimmte Dateien von der Verschlüsselungsverarbeitung während einer Sicherung ausschließen.

Anmerkung:

1. Mit Ausnahme von `exclude.fs` werden vorhandene Sicherungsversionen bei der nächsten Teilsicherung inaktiv, wenn Sie eine Datei ausschließen, die zuvor eingeschlossen war.
2. Auf dem Server können Exclude-Optionen mit der Option `incl excl` definiert werden.

Schließen Sie alle Systemdateien oder Images aus, die bei ihrer Wiederherstellung das Betriebssystem beschädigen könnten. Schließen Sie außerdem das Verzeichnis mit den IBM Spectrum Protect-Clientdateien aus.

Sehr viele Dateien können mit Hilfe von Platzhalterzeichen auf einmal ausgeschlossen werden.

Soll ein vollständiges Verzeichnis mit dem Namen `/any/test` ausgeschlossen werden, geben Sie Folgendes ein:

```
exclude.dir /any/test
```

Sollen Unterverzeichnisse unter dem Verzeichnis `/any/` ausgeschlossen werden, deren Name mit `test` beginnt, geben Sie Folgendes ein:

```
exclude.dir /any/test*
```

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein. Sie können diese Optionen auf der Registerkarte **Einschluss/Ausschluss** im Abschnitt **Include/Exclude-Optionen definieren** im Profileditor definieren.

Syntax

►—*Optionen*—*Muster*—◄

exclude, exclude.backup, exclude.file, exclude.file.backup

Mit diesen Optionen können Sie eine Datei oder Dateigruppe von den Sicherungsservices und von den Speicherverwaltungsservices (wenn der HSM-Client installiert ist) ausschließen. Die Option `exclude.backup` schließt Dateien nur von der normalen Sicherung aus, nicht von HSM.

exclude.archive

Schließt eine dem Muster entsprechende Datei oder Dateigruppe *nur* von den Archivierungsservices aus.

exclude.attribute.symlink

Schließt eine Datei oder Dateigruppe, bei denen es sich um symbolische Verbindungen oder Aliasnamen handelt (Aliasnamen gelten für Mac OS X), nur von der Sicherungsverarbeitung aus.

Anmerkung: Bei Mac OS X sind Aliasnamen ausgeschlossen.

exclude.compression

Schließt Dateien von der Komprimierungsverarbeitung aus, wenn die Option `compression` auf `yes` gesetzt ist. Diese Option gilt für Sicherungen und Archivierungen.

exclude.dedup

Schließt Dateien von der clientseitigen Deduplizierung von Daten aus. Zum Steuern einer clientseitigen Operation für die Deduplizierung von Daten können Sie `ieobjtype` als Wert der Option `exclude.dedup` angeben.

Gültige Parameter für `ieobjtype` sind:

File
Image

Der Standardwert ist File.

exclude.dir

Schließt ein Verzeichnis, seine Dateien sowie alle zugehörigen Unterverzeichnisse und ihre Dateien von der Sicherungsverarbeitung aus. Beispiel: Die An-

weisung `exclude.dir /test/dan/data1` schließt das Verzeichnis `/test/dan/data1`, dessen Dateien und Unterverzeichnisse sowie die Dateien in den Unterverzeichnissen aus.

Wenn Sie ein zuvor eingeschlossenes Verzeichnis ausschließen, kennzeichnet der Server vorhandene Sicherungsversionen der darin enthaltenen Dateien und Verzeichnisse während der nächsten Teilsicherung als verfallen. Verwenden Sie diese Option, um einen Abschnitt Ihrer Daten auszuschließen, die keine zugrunde liegende Dateien für die Sicherung aufweisen.

Anmerkung: Vermeiden Sie die Ausführung einer selektiven Sicherung oder einer partiellen Teilsicherung für eine einzelne Datei innerhalb eines ausgeschlossenen Verzeichnisses. Bei der nächsten Ausführung einer Teilsicherung verfallen alle Dateien, die auf diese Art gesichert wurden.

exclude.encrypt

Schließt die angegebenen Dateien von der Verschlüsselungsverarbeitung aus. Diese Option hat keine Auswirkungen darauf, ob Dateien von der Sicherungs- oder Archivierungsverarbeitung ausgeschlossen werden, sondern nur, ob sie von der Komprimierungsverarbeitung ausgeschlossen werden.

exclude.fs

Schließt Dateisysteme, die mit dem angegebenen Muster übereinstimmen, von Sicherungsoperationen, Imageteilsicherungsoperationen und Archivierungsoperationen aus. Wenn Dateien aus den ausgeschlossenen Dateisystemen jemals gesichert wurden, findet kein erneutes Binden für die Verwaltungsklasse und keine Verfallsverarbeitung für gelöschte Dateien statt. Vorhandene Sicherungsversionen verbleiben jedoch auf dem Server und unterliegen den Einstellungen zugeordneter Verwaltungsklassen. Die Dateien, die zuvor von den ausgeschlossenen Dateisystemen archiviert wurden, verbleiben als Archivierungskopien auf dem Server.

Die Option `exclude.fs` verhindert NICHT die Sicherung oder Archivierung virtueller Mountpunkte, die Unterverzeichnisse des ausgeschlossenen Dateisystems sind.

Verwenden Sie `exclude.image`, um Dateisysteme von Imagegesamtsicherungsoperationen auszuschließen.

exclude.fs.nas

Bei Verwendung im Befehl **backup nas** werden Dateisysteme auf dem NAS-Dateiserver von der Imagesicherung ausgeschlossen. Der NAS-Knotenname muss vor dem Dateisystemnamen stehen, z. B.: `netappsj1/vol/vol1`. Um den Ausschluss auf alle NAS-Knoten anzuwenden, müssen Sie den NAS-Knotenname durch ein Platzhalterzeichen ersetzen, z. B.: `*/vol/vol1`. Der Befehl **backup nas** ignoriert alle anderen Exclude-Anweisungen einschließlich der Anweisungen `exclude.fs` und `exclude.dir`. Diese Option ist *nur* für AIX- und Solaris-Clients gültig.

exclude.image

Schließt angehängte Dateisysteme und unformatierte logische Datenträger, die dem angegebenen Muster entsprechen, von den Imagegesamtsicherungsoperationen aus. Diese Option ist nur für AIX-, Solaris- und alle Linux-Clients gültig. Verwenden Sie `exclude.fs`, um Dateisysteme von Imageteilsicherungsoperationen auszuschließen.

Einschränkung: Diese Option gilt nicht für Mac OS X.

Parameter

Muster

Gibt die Datei oder Dateigruppe an, die ausgeschlossen werden soll.

Anmerkung: Für NAS-Dateisysteme: Sie müssen den NAS-Knotennamen als Präfix vor die Dateispezifikation setzen, um den Dateiserver anzugeben, für den die Ausschlussanweisung gilt. Wenn Sie keinen NAS-Knotennamen angeben, bezieht sich das identifizierte Dateisystem auf den NAS-Knotennamen, der in der Clientsystemoptionsdatei (dsm.sys) oder in der Befehlszeile angegeben ist.

Wenn das Muster mit einem einfachen oder doppelten Anführungszeichen beginnt oder eingebettete Leerzeichen oder Gleichheitszeichen enthält, muss der Wert in einfache (') oder doppelte (") Anführungszeichen eingeschlossen werden. Die Anführungszeichen am Anfang und am Ende müssen identisch sein.

Für die Option `exclude.image` ist das Muster der Name eines angehängten Dateisystems oder eines unformatierten logischen Datenträgers.

Beispiele

Optionsdatei:

```
exclude /unix/
exclude ../../core
exclude /home/jones/proj1/*
exclude.archive ../../core
exclude.backup /home/jones/proj1/devplan/
exclude.dir /home/jones/tmp
exclude.backup /users/home1/file1
exclude.image /usr/*/*
exclude.encrypt /users/home2/file1
exclude.compression /home/gordon/proj1/*
exclude.fs.nas netappsj/vol/vol0
exclude.attribute.symlink ../../*
exclude.dedup /Users/Administrator/Documents/Important/../../*
```

Befehlszeile:

Nicht zutreffend.

Zugehörige Informationen

Eine Liste der Dateien, die Sie immer ausschließen sollten, finden Sie in „Auszuschließende Systemdateien“ auf Seite 134.

„Incl excl“ auf Seite 471

Unter „Dateigruppen mit Platzhalterzeichen einschließen und ausschließen“ auf Seite 136 finden Sie eine Liste der Platzhalterzeichen, die Sie verwenden können. Anschließend können mithilfe der Option `include` Ausnahmen festgelegt werden.

Die Verarbeitung symbolischer Verbindungen und Aliasnamen steuern

Der Client für Sichern/Archivieren behandelt symbolische Verbindungen und Aliasnamen (Aliasnamen gelten nur für Mac OS X) als tatsächliche Dateien und sichert sie. Die Datei, auf die durch die symbolische Verbindung verwiesen wird, wird jedoch nicht gesichert. In einigen Fällen können symbolische Verbindungen problemlos reproduziert werden und müssen nicht gesichert werden.

Darüber hinaus kann durch das Sichern dieser symbolischen Verbindungen die Sicherungsverarbeitungszeit zunehmen und ein wesentlicher Bereich des Speichers auf dem IBM Spectrum Protect-Server eingenommen werden. Sie können die Option `exclude.attribute.symlink` verwenden, um eine Datei oder Dateigruppe, bei denen es sich um symbolische Verbindungen handelt, von der Sicherungsverarbeitung auszuschließen. Falls notwendig, können Sie mit Hilfe der Option `include.attribute.symlink` symbolische Verbindungen innerhalb einer breiten Gruppe ausgeschlossener Dateien für die Sicherungsverarbeitung einschließen.

Sollen beispielsweise alle symbolischen Verbindungen von der Sicherungsverarbeitung ausgeschlossen werden, mit Ausnahme derjenigen, die sich unter dem Verzeichnis `/home/spike` befinden, geben Sie die folgenden Anweisungen in Ihre Datei `dsm.sys` ein:

```
exclude.attribute.symlink  /.../*
include.attribute.symlink  /home/spike/.../*
```

Zugehörige Verweise:

„Include-Optionen“ auf Seite 473

Steuerung der Komprimierungsverarbeitung

In diesem Abschnitt sind einige Hinweise aufgeführt, die Sie beachten sollten, wenn Sie bestimmte Dateien oder Dateigruppen während einer Sicherungs- oder Archivierungsoperation von der Komprimierungsverarbeitung ausschließen wollen.

- Denken Sie daran, dass der Client für Sichern/Archivieren die Dateien, die verarbeitet werden, mit den in den Einschluss-/Ausschlussanweisungen angegebenen Mustern vergleicht, wobei in der Optionsdatei von unten nach oben gelesen wird.
- Sie müssen die Option `compression` auf `yes` setzen, um die Komprimierungsverarbeitung zu aktivieren. Wenn Sie die Option `compression` nicht angeben oder die Option `compression` auf `no` setzen, führt der Client keine Komprimierungsverarbeitung aus.

Wenn Sie die Option `compression` auf `yes` setzen und keine Anweisungen `exclude.compression` vorhanden sind, berücksichtigt der Client alle Dateien für die Komprimierungsverarbeitung.

- Der Client verarbeitet `exclude.fs`, `exclude.dir` und andere Einschluss-/Ausschlussanweisungen zuerst. Danach berücksichtigt der Client alle Anweisungen `exclude.compression`. Wenn beispielsweise folgende Einschluss-/Ausschlussliste eingegeben wird:

```
exclude /home/jones/proj1/*.*
exclude.compression /home/jones/proj1/file.txt
include /home/jones/proj1/file.txt
```

Der Client prüft die Anweisungen (von unten nach oben gelesen) und stellt fest, dass die Datei `/home/jones/proj1/file.txt` ein Kandidat für die Sicherung, jedoch kein Kandidat für die Komprimierungsverarbeitung ist.

- Die Komprimierungsverarbeitung von Einschluss-/Ausschlussdateien ist nur für die Sicherungs- und Archivierungsverarbeitung gültig. Die Option `exclude.compression` hat keine Auswirkungen darauf, ob Dateien von der Sicherungs- oder Archivierungsverarbeitung ausgeschlossen werden, sondern nur, ob sie von der Komprimierungsverarbeitung ausgeschlossen werden.

Zugehörige Verweise:

„Compression“ auf Seite 380

Verarbeitung von NAS-Dateisystemen

Mit Hilfe der Option `exclude.fs.nas` können Sie Dateisysteme von der NAS-Imagesicherungsverarbeitung ausschließen.

Anmerkung: Die Option `exclude.fs.nas` gilt nicht für eine Teilsicherung unter Verwendung der Momentaufnahmedifferenz.

Für eine NAS-Dateisystemspezifikation werden folgende Konventionen verwendet:

- NAS-Knoten stellen einen eindeutigen Knotentyp dar. Der Name des NAS-Knotens identifiziert einen NAS-Dateiserver und seine Daten eindeutig für den Client für Sichern/Archivieren. Sie können den NAS-Knotennamen als Präfix vor die Dateispezifikation setzen, um den Dateiserver anzugeben, für den die Ausschlussanweisung gilt. Wenn Sie keinen NAS-Knotennamen angeben, gilt das angegebene Dateisystem für alle NAS-Dateiserver.
- Unabhängig von der Clientplattform wird in NAS-Dateisystemspezifikationen der Schrägstrich (/) als Trennzeichen verwendet. Zum Beispiel: `/vol/vol0`.

Geben Sie beispielsweise folgende Ausschlussanweisung an, um `/vol/vol1` auf allen NAS-Knoten von den Sicherungsservices auszuschließen:

```
exclude.fs.nas */vol/vol1
```

Exclude-Optionen für virtuelle Maschinen

Einschluss- und Ausschlussoptionen für virtuelle Maschinen wirken sich auf das Verhalten von Sicherungs- und Zurückschreibungsoperationen für virtuelle Maschinen aus. Diese Optionen werden vor allen Befehlszeilenoptionen verarbeitet. Daher können Optionen in der Befehlszeile Optionen überschreiben, die in den Einschluss- oder Ausschlussoptionen für virtuelle Maschinen angegebenen sind. Informationen zu den Optionen finden Sie in der jeweiligen Optionsbeschreibung.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Zugehörige Verweise:

„Exclude.vmdisk“

Exclude.vmdisk:

Mit der Option `EXCLUDE.VMDISK` wird eine Platte einer virtuellen Maschine von Sicherungsoperationen ausgeschlossen.

Die Option `EXCLUDE.VMDISK` gibt den Kennsatz einer VM-Platte an, die von einer Operation **backup vm** ausgeschlossen werden soll. Wenn Sie im Befehl **backup vm** eine Platte ausschließen, überschreiben die Befehlszeilenparameter alle Anweisungen `EXCLUDE.VMDISK` in der Optionsdatei.

Diese Option ist nur verfügbar, wenn Sie das lizenzierte Produkt 'IBM Spectrum Protect for Virtual Environments' verwenden. Weitere Informationen zu dieser Option finden Sie in der Produktdokumentation zu IBM Spectrum Protect for Virtual Environments im IBM Knowledge Center unter <http://www.ibm.com/support/knowledgecenter/SSERB6/welcome>.

EXCLUDE.VMDISK für virtuelle VMware-Maschinen

Verwenden Sie die Option `EXCLUDE.VMDISK`, um eine virtuelle VMware-Maschine von Sicherungsoperationen auszuschließen.

Unterstützte Clients

Diese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Optionsdatei

Definieren Sie diese Option in der Clientoptionsdatei. Befehlszeilenparameter überschreiben Anweisungen in der Optionsdatei.

Syntax für virtuelle VMware-Maschinen

►—EXCLUDE.VMDISK—*VM-Name*—*VM-Plattenkennsatz*—►

Parameter

VM-Name

Gibt den Namen der virtuellen Maschine an, die eine Platte enthält, die von einer Operation **Backup VM** ausgeschlossen werden soll. Der Name ist der Anzeigename der virtuellen Maschine. In jeder Anweisung EXCLUDE.VMDISK können Sie nur den Namen einer einzigen virtuellen Maschine angeben. Geben Sie weitere Anweisungen EXCLUDE.VMDISK für jede VM-Platte an, die ausgeschlossen werden soll.

Der Name der virtuellen Maschine kann einen Stern (*) enthalten, der einer beliebigen Zeichenfolge entspricht, und ein Fragezeichen (?), das einem beliebigen einzelnen Zeichen entspricht. Schließen Sie den VM-Namen in Anführungszeichen („ ") ein, wenn der VM-Name Leerzeichen enthält.

Tipp: Enthält der Name der virtuellen Maschine Sonderzeichen, wie beispielsweise eckige Klammern ([oder]), wird der Name der virtuellen Maschine möglicherweise nicht korrekt abgeglichen. Enthält der Name der virtuellen Maschine Sonderzeichen, müssen Sie möglicherweise ein Fragezeichen (?) verwenden, um die Sonderzeichen im VM-Namen abzugleichen.

Soll z. B. Hard Disk 1 bei der Sicherung der virtuellen Maschine "Windows VM3 [2012R2]" ausgeschlossen werden, verwenden Sie diese Syntax in der Optionsdatei: EXCLUDE.VMDISK "Windows VM3 ?2012R2?" "Hard Disk 1"

VM-Plattenkennsatz

Gibt den Plattenkennsatz der Platte an, die ausgeschlossen werden soll. Platzhalterzeichen sind nicht zulässig. Verwenden Sie den Befehl **Backup VM** mit der Option -preview, um die Plattenkennsätze der Platten in einer bestimmten virtuellen Maschine zu bestimmen. Informationen zur Syntax finden Sie in der Beschreibung des Befehls "**Backup VM**".

Schließen Sie keine Platten in virtuellen Maschinen aus, die mit der Option INCLUDE.VMTSMVSS geschützt werden, wenn die Platten Anwendungsdaten enthalten.

Beispiele

Optionsdatei

Beispiel: Eine virtuelle Maschine mit dem Namen vm1 enthält vier Platten mit den Kennsätzen "Festplatte 1", "Festplatte 2", "Festplatte 3" und "Festplatte 4". Um Festplatte 2 von Operationen **Backup VM** auszuschließen, geben Sie in der Optionsdatei die folgende Anweisung an:

```
EXCLUDE.VMDISK "vm1" "Festplatte 2"
```

Festplatte 2 und Festplatte 3 von Operationen **Backup VM** ausschließen:

```
EXCLUDE.VMDISK "vm1" "Festplatte 2"  
EXCLUDE.VMDISK "vm1" "Festplatte 3"
```


Befehlszeile:

Die Befehlszeilenbeispiele zeigen die Verwendung des Ausschlussoperators (-) vor dem Schlüsselwort `vmdk=`, um anzugeben, dass die Platte ausgeschlossen werden soll.

Einzelne Platte ausschließen:

```
dsmc backup vm "vm1:-vmdk=Festplatte 1"
```

Festplatte 2 und Festplatte 3 ausschließen:

```
dsmc backup vm "vm1:-vmdk=Festplatte 2:-vmdk=Festplatte 3"
```

Festplatte 1 und Festplatte 2 bei der Sicherung von vm1 ausschließen:

```
dsmc backup vm "vm1:-vmdk=Festplatte 1:-vmdk=Festplatte 2"
```

Zugehörige Verweise:

„Backup VM“ auf Seite 710

„Restore VM“ auf Seite 791

„Domain.vmfull“ auf Seite 414

„Include.vmdisk“ auf Seite 482

„INCLUDE.VMTSMVSS“ auf Seite 488

Exclude.vmlocalsnapshot:

Mit dieser Option wird eine virtuelle VMware-Maschine von lokalen Sicherungsoperationen ausgeschlossen.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Sie können diese Option nur für virtuelle Maschinen verwenden, die in einem Datenspeicher für virtuelle Datenträger (VVOL) gespeichert werden.

Unterstützte Clients

Diese Option kann für unterstützte Linux-Clients verwendet werden, die für die Sicherung von virtuellen VMware-Maschinen konfiguriert sind.

Optionsdatei

Definieren Sie diese Option in der Clientoptionsdatei.

Syntax

►►—EXCLUDE.VMLOCALSNAPSHOT— —*VM-Name*—————►

Parameter

VM-Name

Gibt den Namen einer virtuellen Maschine an, die Sie von lokalen Sicherungsoperationen ausschließen wollen. Der Name ist der Anzeigename der virtuellen Maschine.

In einer Anweisung EXCLUDE.VMLOCALSNAPSHOT kann nur jeweils eine virtuelle Maschine angegeben werden. Sie können jedoch so viele EXCLUDE.VMLOCALSNAPSHOT-Anweisungen angeben wie für das Ausschließen mehrerer virtueller Maschinen benötigt werden.

Sie können Platzhalterzeichen im Namen der virtuellen Maschine verwenden. Ein Stern (*) entspricht einer beliebigen Zeichenfolge. Ein Fragezeichen (?) entspricht einem einzelnen Zeichen. Wenn der Name der virtuellen Maschine ein Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen (") ein.

Tipp: Wenn der Name der virtuellen Maschine Sonderzeichen enthält, ersetzen Sie die Sonderzeichen durch das Platzhalterzeichen ? (Fragezeichen), wenn Sie den Namen der virtuellen Maschine angeben.

Beispiel

Mit der folgenden Anweisung `EXCLUDE.VMLOCALSNAPSHOT` in der Clientoptionsdatei wird die virtuelle Maschine VM1 von lokalen Sicherungsoperationen ausgeschlossen:

```
exclude.vmlocalsnapshot VM1
```

Zugehörige Verweise:

„Backup VM“ auf Seite 710

Fbbranch

Verwenden Sie die Option `fbbranch` mit dem Befehl **backup fastback** oder **archive fastback**.

Die Option `fbbranch` gibt die Filialen-ID des fernen FastBack-Servers an, der gesichert oder archiviert werden soll. Die Option `fbbranch` ist nur erforderlich, wenn der Client für Sichern/Archivieren auf dem FastBack Disaster Recovery Hub installiert ist oder wenn ein dedizierter Proxy eine Verbindung zu einem replizierten FastBack Disaster Recovery Hub-Repository herstellt. Geben Sie die Option `fbbranch` nicht an, wenn der Client für Sichern/Archivieren auf dem FastBack-Server installiert ist.

Unterstützte Clients

Diese Option ist für Linux x86_64-Clients gültig.

Optionsdatei

Keine. Sie können diese Option nur in der Befehlszeile angeben. Diese Option kann auch auf dem Server definiert oder vom Server überschrieben werden.

Syntax

►►—FBBBranch=*Filialen-ID*—————►►

Parameter

Filialen-ID

Gibt die Filialen-ID des FastBack-Servers an. Der Wert ist Teil der Disaster Recovery-Konfiguration des FastBack-Servers.

Beispiele

Befehlszeile:

```
-FBBBranch=oracle
```

Auf einem Client für Sichern/Archivieren, der auf dem FastBack Disaster Recovery Hub installiert ist:

```
dsmc backup fastback -fbpolicyname=policy1 -fbserver=myFbServer  
-fbbranch=oracle
```

Befehlszeile:

Auf einem Client für Sichern/Archivieren, der eine Verbindung zu einem Repository auf einem fernen FastBack Disaster Recovery Hub herstellt:

```
dsmc backup fastback -fbpolicyname=policy1 -fbserver=server1  
-Fbreposlocation=\\myDrHub.company.com\\REP  
-fbbranch=oracle
```

Wenn die Option `fbbranch` auf einer Workstation des Clients für Sichern/Archivieren angegeben wird, die auf dem FastBack-Server installiert ist, wird die Option `fbbranch` ignoriert.

Fbclientname

Verwenden Sie die Option `fbclientname` mit dem Befehl **backup fastback** oder **archive fastback**.

Mit der Option `fbclientname` können Sie den Namen eines Clients oder mehrere durch Kommas getrennte Namen von Clients in FastBack angeben, die vom Sicherungsproxy gesichert oder archiviert werden sollen. Die Werte für die Option `fbclientname` sind ungültig, wenn mehrere Maßnahmen in der Option `fbpolicyname` angegeben sind.

Sie können keine Leerzeichen in den Werten der Option `fbclientname` angeben.

Wenn Sie keine Werte für die Option `fbvolumename` angeben, werden alle Datenträger von allen FastBack-Clients in der angegebenen Maßnahme gesichert. Wenn Sie mehrere FastBack-Clients in der Option `fbclientname` angeben, können Sie keine Werte für die Option `fbvolumename` angeben.

Unterstützte Clients

Diese Option ist für Linux x86_64-Clients gültig.

Optionsdatei

Keine. Sie können diese Option nur in der Befehlszeile angeben.

Syntax



Parameter

Clientname

Gibt den/die Namen eines oder mehrerer FastBack-Clients an. Sie können bis zu 10 FastBack-Clientnamen angeben.

Wichtig:

Wenn Sie den Befehl **archive fastback** oder **backup fastback** angeben:

1. Mindestens ein Wert für FBpolicyName ist immer erforderlich.
2. Sie können bis zu 10 Werte für FBPolicyName angeben, wenn weder für FBClientName noch für FBVolumeName Werte angegeben sind.
3. Wenn Sie einen Wert für FBClientName angeben, darf nur ein Wert für FBPolicyName vorhanden sein.
4. Sie können bis zu 10 Werte für FBClientName angeben, wenn nur ein Wert für PolicyName angegeben ist und keine Werte für FBVolumeName angegeben sind.
5. Wenn Sie die Option FBVolumeName angeben, kann nur ein Wert für FBPolicy und nur ein Wert für FBClientName angegeben werden.
6. Sie können mehrere Werte für FBVolumeName angeben, wenn Bedingung 5 erfüllt ist.
7. Sie müssen immer die Option FBReposLocation für Linux angeben.

Beispiele

Befehlszeile:

```
dsmc backup fastback -fbpolicyname=Policy1  
-fbclientname=fbclient1,fbclient2  
-fbserver=myFbServer  
-fbreposlocation=/mnt/FBLocation
```

Sichert alle Datenträger für die FastBack-Clients fbclient1 und fbclient2, die sich in der Maßnahme Policy1 befinden.

Fbpolicyname

Verwenden Sie die Option fbpolicyname mit dem Befehl **backup fastback** oder **archive fastback**.

Mit der Option fbpolicyname können Sie den Namen einer Maßnahme oder mehrere durch Kommas getrennte Namen von Maßnahmen in FastBack angeben, die vom Sicherungsproxy gesichert oder archiviert werden sollen. Sie müssen mindestens einen Maßnahmennamen angeben. Mehrere Maßnahmennamen können Sie über eine durch Kommas begrenzte Liste von Maßnahmen angeben. Es gibt keinen Standardwert.

Wenn mindestens ein FB-Maßnahmename Leerzeichen enthält, müssen Sie die Namen in Anführungszeichen einschließen. Hier ein Beispiel: „FB Policy NAME1, FBPolicy Name 2“.

Wenn Sie keine Werte für die Optionen fbclientname und fbvolumeName angeben, werden alle Datenträger von allen FastBack-Clients in den angegebenen Maßnahmen gesichert. Wenn Sie mehrere Maßnahmen in der Option fbpolicyname angeben, können Sie keine Werte für die Optionen fbclientname und fbvolumeName angeben.

Wenn eine Maßnahmenspezifikation sowohl Windows als auch Linux FastBack-Clients enthält, werden nur die Linux-Datenträger vom Linux-Client für Sichern/Archivieren auf dem IBM Spectrum Protect-Server gesichert oder archiviert.

Bei Ausgabe des Befehls **dsmc** sollte mindestens eine Momentaufnahme für die zu archivierenden oder zu sichernden FastBack-Maßnahmen im FastBack-Repository vorhanden sein.

Unterstützte Clients

Diese Option ist für Linux x86_64-Clients gültig.

Optionsdatei

Keine. Sie können diese Option nur in der Befehlszeile angeben.

Syntax



Parameter

Maßnahmenname

Gibt die Namen der FastBack-Maßnahmen an. Sie können bis zu 10 FastBack-Maßnahmennamen angeben.

Wichtig:

Wenn Sie den Befehl **archive fastback** oder **backup fastback** angeben:

1. Mindestens ein Wert für FBpolicyName ist immer erforderlich.
2. Sie können bis zu 10 Werte für FBPolicyName angeben, wenn weder für FBClientName noch für FBVolumeName Werte angegeben sind.
3. Wenn Sie einen Wert für FBClientName angeben, darf nur ein Wert für FBPolicyName vorhanden sein.
4. Sie können bis zu 10 Werte für FBClientName angeben, wenn nur ein Wert für PolicyName angegeben ist und keine Werte für FBVolumeName angegeben sind.
5. Wenn Sie die Option FBVolumeName angeben, kann nur ein Wert für FBPolicy und nur ein Wert für FBClientName angegeben werden. Sie müssen genau einen Wert für FBClientName angeben. Der Wert kann nicht übergangen werden.
6. Sie können mehrere Werte für FBVolumeName angeben, wenn Bedingung 5 erfüllt ist.
7. Sie müssen immer die Option FBReposLocation für Linux angeben.

Beispiele

Befehlszeile:

```
dsmc backup fastback -fbpolicyname=Policy1,Policy2,Policy3  
-fbserver=myFbServer  
-fbreposlocation=\\myFbServer.company.com\REP
```

Sichert alle Datenträger für alle FastBack-Clients, die sich in den Maßnahmen Policy1, Policy2 und Policy3 befinden.

Zum Angeben von Maßnahmennamen mit Leerzeichen schließen Sie diese in Anführungszeichen ein, z. B.:

```
-fbpolicyname="Policy 1,Policy2,Policy3"
```

Fbreposlocation

Verwenden Sie die Option fbreposlocation mit dem Befehl **backup fastback** oder **archive fastback**.

Die Option `fbreposlocation` gibt die Position des Tivoli Storage Manager FastBack-Repositorys an, zu dem der Proxy des Clients für Sichern/Archivieren eine Verbindung herstellen soll, um Tivoli Storage Manager FastBack-Shellbefehle auszugeben, die zum Bereitstellen der entsprechenden Momentaufnahmen erforderlich sind.

Diese Option ist auf Linux-Systemen erforderlich. Es gibt keine Standardposition.

Wenn Sie die Option `fbreposlocation` für eine Momentaufnahme auf dem FastBack-Server angeben, müssen Sie das Format `Servername@WORKGROUP` verwenden.

Für die Angabe der FastBack-Repository-Position auf dem FastBack Disaster Recovery Hub gibt es zwei Möglichkeiten:

- Geben Sie die vollständige Repository-Position über die Option `-fbreposlocation=\\DR_Hub\rep_server` an. Wenn Sie dieses Format verwenden, ist `DR_Hub` der Name der FastBack Disaster Recovery Hub-Maschine und `rep_server` ist der Name des replizierten FastBack-Server-Repositorys auf dem DR Hub.
- Geben Sie die Repository-Position über eine Kombination der Optionen `-fbreposlocation=` und `-fbbranch` an. Wenn Sie dieses Format verwenden, geben Sie die Position des DR Hub-Repositorys über die Option `-fbreposlocation=DR_Hub@WORKGROUP` und den Namen des replizierten FastBack-Server-Repositorys auf dem DR Hub über die Option `-fbbranch` an.

Bei Verwendung des Formats `-fbr=\\<fbserver>\REP` müssen Sie zwei umgekehrte Schrägstriche vor der Zeichenfolge `<fbserver>` und einen umgekehrten Schrägstrich vor der Zeichenfolge `'REP'` angeben, wenn Sie den Client für Sichern/Archivieren im interaktiven Modus ausführen. Wenn Sie dieses Format als Linux-Befehl `dsmc backup fastback -fbr=\\\\<fbserver>\\REP` verwenden, müssen Sie vier umgekehrte Schrägstriche vor der Zeichenfolge `<fbserver>` und zwei umgekehrte Schrägstriche vor der Zeichenfolge `'REP'` angeben. Die Ursache dafür ist, dass die Linux-Shell einen umgekehrten Schrägstrich als Escapezeichen interpretiert; der erste umgekehrte Schrägstrich wird als Escapezeichen für den darauffolgenden umgekehrten Schrägstrich behandelt.

Unterstützte Clients

Diese Option ist für Linux x86_64-Clients gültig.

Optionsdatei

Keine. Sie können diese Option nur in der Befehlszeile angeben. Diese Option kann auch auf dem Server definiert oder vom Server überschrieben werden.

Syntax

►►—FBReposlocation—*Repository-Position*—————◄◄

Parameter

Repository-Position

Gibt die Tivoli Storage Manager FastBack-Repository-Position an.

Beispiele

Befehlszeile:

```
dsmc backup fastback -fbpolicyname=Policy1  
-fbclientname=fbclient1,fbclient2 -fbserver=myFbDrHub  
-fbreposlocation=\\myFbDrHub\\rep_myFbServer
```

Anmerkung: Da Linux nur als dedizierte Proxy-Konfiguration unterstützt wird, ist unter Linux immer eine Repository-Position erforderlich.

Befehlszeile:

```
dsmc backup fastback -fbpolicyname=Policy1  
-fbclientname=fbclient1,fbclient2 -fbserver=myFbDrHub  
-fbreposlocation=myFbDrHub -fbbranch=rep_myFbServer
```

Anmerkung: Da Linux nur als dedizierte Proxy-Konfiguration unterstützt wird, ist unter Linux immer eine Repository-Position erforderlich.

Fbserver

Verwenden Sie die Option **fbserver** mit dem Befehl **backup fastback** oder **archive fastback**.

Mit der Option **fbserver** können Sie den kurzen Hostnamen der Tivoli Storage Manager FastBack-Server-Workstation angeben, die der Eigner des durch die Option **fbreposlocation** angegebenen Repositorys ist. Für einen DR Hub gibt die Option **fbserver** den Kurznamen der FastBack-Server-Workstation an, zu deren Repository einer Filiale der Client für Sichern/Archivieren eine Verbindung herstellt.

Die Option **fbserver** stellt einen Schlüssel zum Abrufen der Benutzerberechtigungs-nachweise dar, die erforderlich sind, um für die Mountverarbeitung eine Verbindung zum FastBack-Server-Repository oder DR Hub-Server-Repository herzustellen.

Unterstützte Clients

Diese Option ist für Linux x86_64-Clients gültig.

Optionsdatei

Keine. Sie können diese Option nur in der Befehlszeile angeben.

Syntax

►► — -FBServer — *Servername* —————►►

Parameter

Servername

Gibt den kurzen Hostnamen der Maschine an, auf der der FastBack-Server installiert ist.

Beispiele

Befehlszeile:

Der Client für Sichern/Archivieren ist auf einer Linux-Proxy-Client-Ma-

schine installiert. Verwenden Sie diesen Befehl, um alle FastBack-Datenträger für alle Linux FastBack-Clients zu archivieren, die für die FastBack-Maßnahme Policy1 definiert sind:

```
dsmc archive fastback -fbpolicyname=Policy1  
-fbserver=myfbserver  
-fbreposlocation=myfbserver@WORKGROUP
```

Die Repository-Position ist erforderlich. Wenn Sie die Repository-Position nicht angeben, schlägt der Befehl fehl.

Der FastBack-Servername -myfbserver ist der kurze Hostname des FastBack-Servers, auf dem sich das Repository befindet.

Befehlszeile:

Das Repository rep_server1 befindet sich auf dem FastBack Disaster Recovery Hub myFbDrHub.

```
dsmc archive fastback -fbpolicyname="Policy 1"  
-fbserver=myFbDrHub  
-fbreposlocation=\\myFbDrHub\\rep_server1
```

Der FastBack-Servername -myFbDrHub ist der kurze Hostname des FastBack Disaster Recovery Hub-Servers, auf dem sich das Repository befindet.

Die Option -fbreposlocation gibt die Position des Repositories an. Die Repository-Position ist erforderlich. Wenn Sie die Repository-Position nicht angeben, schlägt der Befehl fehl.

In diesem Fall sollte -fbserver auf den kurzen Hostnamen des FastBack DR Hub verweisen.

Befehlszeile:

Alle Datenträger, die durch die FastBack-Maßnahme mit dem Namen policy1 geschützt sind, für den FastBack-Server mit dem Namen basil archivieren:

```
dsmc archive fastback -Fbpolicyname=policy1  
-FBServer=basil -ARCHMC="my_tsm_mgmt_class"  
-fbreposlocation=basil@WORKGROUP
```

Fbvolumename

Verwenden Sie die Option fbvolumename mit dem Befehl **backup fastback** oder **archive fastback**.

Mit der Option fbvolumename können Sie den Namen eines Datenträgers oder mehrere durch Kommas getrennte Namen von Datenträgern in Tivoli Storage Manager FastBack angeben, die vom Sicherungsproxy gesichert oder archiviert werden sollen. Werte für die Option fbvolumename sind nicht gültig, wenn mehr als ein FastBack-Client in der Option fbclientname angegeben ist.

Wenn Sie mehrere FastBack-Clients in der Option fbclientname angeben, können Sie keine Werte für die Option fbvolumename angeben.

Unterstützte Clients

Diese Option ist für Linux x86_64-Clients gültig.

Optionsdatei

Keine. Sie können diese Option nur in der Befehlszeile angeben.

Syntax



Parameter

Datenträgername

Gibt die Namen der Tivoli Storage Manager FastBack-Datenträger an. Sie können bis zu 10 FastBack-Datenträgernamen angeben.

Wichtig:

Wenn Sie den Befehl **archive fastback** oder **backup fastback** angeben:

1. Mindestens ein Wert für FBpolicyName ist immer erforderlich.
2. Sie können bis zu 10 Werte für FBPolicyName angeben, wenn weder für FBClientName noch für FBVolumeName Werte angegeben sind.
3. Wenn Sie einen Wert für FBClientName angeben, darf nur ein Wert für FBPolicyName vorhanden sein.
4. Sie können bis zu 10 Werte für FBClientName angeben, wenn nur ein Wert für PolicyName angegeben ist und keine Werte für FBVolumeName angegeben sind.
5. Wenn Sie die Option FBVolumeName angeben, kann nur ein Wert für FBPolicy und nur ein Wert für FBClientName angegeben werden. Sie müssen genau einen Wert für FBClientName angeben. Der Wert kann nicht übergangen werden.
6. Sie können mehrere Werte für FBVolumeName angeben, wenn Bedingung 5 erfüllt ist.
7. Sie müssen die Option FBReposLocation angeben.

Beispiele

Befehlszeile:

```
dsmc backup fastback -fbpolicyname=Policy1 -fbclientname=client1  
-fbvolumename=data1,data2 -fbserver=myFbDrHub  
-fbreposlocation=\\myFbDrHub\\rep_server1
```

Sichert die Datenträger data1 und data2 des FastBack-Clients client1, der in der Maßnahme Policy1 vorhanden ist.

Filelist

Verwenden Sie die Option filelist, um eine Liste von Dateien zu verarbeiten.

Die Option filelist können Sie in folgenden Befehlen verwenden:

- **archive**
- **backup group**
- **delete archive**
- **delete backup**
- **expire**
- **incremental**
- **query archive**
- **query backup**
- **restore**
- **retrieve**

- **selective**

Der Client für Sichern/Archivieren öffnet die Datei, die Sie mit dieser Option angeben, und verarbeitet die darin enthaltene Liste der Dateien dem jeweiligen Befehl entsprechend. Außer für die Befehle **restore** und **retrieve** ignoriert der Client alle anderen Dateispezifikationen in der Befehlszeile, wenn Sie die Option **filelist** verwenden.

Für die in der Dateiliste aufgeführten Dateien (Einträge) gelten folgende Regeln:

- Jeder Eintrag muss ein vollständig qualifizierter oder relativer Pfad zu einer Datei oder einem Verzeichnis sein. Wenn Sie ein Verzeichnis in einen Dateilisteneintrag einschließen, wird das Verzeichnis gesichert, aber der Inhalt des Verzeichnisses wird nicht gesichert.
- Jeder Pfad muss in einer einzelnen Zeile angegeben werden. Eine Zeile kann nur einen Pfad enthalten.
- Pfade dürfen keine Steuerzeichen enthalten, wie beispielsweise 0x18 (STRG-X), 0x19 (STRG-Y) und 0x0A (neue Zeile).
- Standardmäßig dürfen die Pfade keine Platzhalterzeichen enthalten. Geben Sie keinen Stern (*) und kein Fragezeichen (?) in einem Pfad an. Diese Einschränkung kann durch Aktivierung der Option **wildcardsareliteral** außer Kraft gesetzt werden. Weitere Informationen zu dieser Option finden Sie in „Wildcardsareliteral“ auf Seite 681.
- Die Dateiliste kann eine MBCS-Datei oder eine Unicode-Datei mit allen Unicode-Einträgen sein. Für Mac OS X kann die Dateiliste in der aktuellen Betriebssystemsprache oder in UTF-16 codiert sein.
- Wenn die Clientoption **quotessareliteral** definiert ist, können Anführungszeichen in einer Dateispezifikation buchstabengetreu als Anführungszeichen und nicht als Begrenzungszeichen interpretiert werden. Weitere Informationen zu dieser Option finden Sie in „Quotesareliteral“ auf Seite 544. Wenn **quotessareliteral** und **wildcardsareliteral** nicht definiert sind, findet die Verarbeitung von Anführungszeichen und Platzhalterzeichen wie folgt statt:
 - Wenn ein Pfad oder ein Dateiname ein Leerzeichen enthält, schließen Sie den vollständigen Pfad in Anführungszeichen (") oder Hochkommas (') ein. Beispiel: "C:\My Documents\spreadsheet.xls" oder 'C:\My documents\spreadsheet.xls'.
 - Enthält ein Pfad ein oder mehrere Hochkommas ('), schließen Sie den vollständigen Eintrag in Anführungszeichen (") ein. Enthält ein Pfad ein oder mehrere Anführungszeichen, schließen Sie den vollständigen Pfad in Hochkommas ein. Die Dateilistenverarbeitung unterstützt keine Pfade, die eine Mischung aus Anführungszeichen und Hochkommas einschließen.

Die folgenden Beispiele zeigen die korrekte und die falsche Verwendung von Anführungszeichen und Hochkommas in Pfaden.

Dieses Beispiel für einen Pfad enthält ein Hochkomma. Der Pfad muss daher in Anführungszeichen eingeschlossen werden:

```
"/home/gatzby/mydir/gatzby's_report.out"
```

Dieses Beispiel für einen Pfad enthält Anführungszeichen. Der Pfad muss daher in Hochkommas eingeschlossen werden:

```
'/home/gatzby/mydir/"top10".out'
```

Dieses Beispiel für einen Pfad enthält ein Leerzeichen. Daher muss der Pfad entweder in Anführungszeichen oder in Hochkommas eingeschlossen werden:

```
"/home/gatzby/mydir/top 10.out"
```

oder

```
'/home/gatzby/mydir/top 10.out'
```

Dieses Beispiel für einen Pfad wird für die Dateilistenverarbeitung nicht unterstützt, da der Pfad Begrenzer ohne Entsprechung (" und ") enthält:

```
/home/gatzby/mydir/andy's_"top 10" report.out
```

Diese Pfade werden für die Dateilistenverarbeitung nicht unterstützt, da sie Platzhalterzeichen enthalten:

```
/home/gatzby*  
/home/*/20??.txt
```

- Alle IBM Spectrum Protect-Dateilisteneinträge, die diesen Regeln nicht entsprechen, werden ignoriert.

Die folgenden Beispiele sind gültige Pfade in einer Dateiliste:

```
/home/dir/file1  
/usr/tivoli/file2  
/usr/avi/dir1  
/fs1/dir2/file3  
"/fs2/Ha Ha Ha/file.txt"  
"/fs3/file.txt"
```

Informationen darüber, wie die Standardverarbeitung von Anführungszeichen und Platzhalterzeichen außer Kraft gesetzt wird, finden Sie in „Quotesareliteral“ auf Seite 544 und in „Wildcardsareliteral“ auf Seite 681.

Sie können die Option `filelist` während einer OFS-Operation (OFS = Open File Support = Unterstützung offener Dateien) verwenden. In diesem Fall verarbeitet der Client die Einträge in der Dateiliste vom virtuellen und nicht vom realen Datenträger.

Wenn ein Eintrag in der Dateiliste ein Verzeichnis angibt, wird nur dieses Verzeichnis und nicht die darin enthaltenen Dateien verarbeitet.

Ist der für die Option `filelist` angegebene Dateiname (Dateilistenspezifikation) nicht vorhanden, schlägt der Befehl fehl. Der Client überspringt alle Einträge in der Dateiliste, die keine gültigen Dateien oder Verzeichnisse sind. Der Client protokolliert Fehler und die Verarbeitung wird mit dem nächsten Eintrag fortgesetzt.

Verwenden Sie Dateispezifikationen im Befehl **restore** und **retrieve**, um das Ziel für die zurückgeschriebenen Dateilisteneinträge anzugeben. Beispiel: In dem folgenden **restore**-Befehl stellt die Dateispezifikation `/usr/record/` den Zurückschreibungszielort für alle Einträge in der Dateiliste dar.

```
restore -filelist=/home/dir/file3 /usr/record/
```

In dem folgenden **selective**-Befehl wird die Dateispezifikation `/usr/record/` jedoch ignoriert.

```
selective -filelist=/home/dir/file3 /usr/record/
```

Wenn Sie für den Befehl **delete archive** oder **delete backup** ein Verzeichnis in einer Dateiliste angeben, wird das Verzeichnis nicht gelöscht. Dateilisten, die Sie im Befehl **delete archive** oder **delete backup** verwenden, dürfen keine Verzeichnisse enthalten.

Die Einträge in der Liste werden in der Reihenfolge der Dateiliste verarbeitet. Um eine optimale Verarbeitungsleistung zu erzielen, sollten Sie die Dateiliste nach Dateibereichsnamen und -pfad vorsortieren.

Anmerkung: Der Client sichert ein Verzeichnis möglicherweise zweimal, wenn folgende Bedingungen auftreten:

- Die Dateiliste enthält einen Eintrag für das Verzeichnis
- Die Dateiliste enthält mindestens einen Eintrag für Dateien in diesem Verzeichnis
- Es ist keine Sicherung des Verzeichnisses vorhanden

Angenommen, Ihre Dateiliste enthält die Einträge `/home/dir/file1` und `/home/dir`. Wenn das Verzeichnis `/dir` auf dem Server nicht vorhanden ist, wird das Verzeichnis `/home/dir` ein zweites Mal an den Server gesendet.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

►—FILEList =— —*Dateilistenspezifikation*————►

Parameter

Dateilistenspezifikation

Gibt die Position und den Namen der Datei an, die die Liste der Dateien enthält, die für den Befehl verarbeitet werden sollen.

Anmerkung: Wenn Sie die Option `filelist` in der Befehlszeile angeben, wird die Option `subdir` ignoriert.

Beispiele

Befehlszeile:

```
sel -filelist=/home/avi/filelist.txt
```

Zugehörige Informationen

„Quotesareliteral“ auf Seite 544

„Wildcardsareliteral“ auf Seite 681

Filename

Verwenden Sie die Option `filename` im Befehl **query systeminfo**, um den Namen einer Datei anzugeben, in der Informationen gespeichert werden sollen.

Sie können Informationen speichern, die von einen oder mehreren der folgenden Elemente zusammengestellt wurden:

- DSMOPTFILE - Der Inhalt der Datei `dsm.opt`
- DSMSYSFILE - Inhalt der Datei `dsm.sys`
- ENV - Umgebungsvariablen
- ERRORLOG - IBM Spectrum Protect-Fehlerprotokolldatei

- FILE - Attribute für den angegebenen Dateinamen.
- INCLEXCL - Stellt eine Liste der Include/Exclude-Anweisungen in der Reihenfolge zusammen, in der sie bei Sicherungs- und Archivierungsoperationen verarbeitet werden.
- OPTIONS - Optionen
- OSINFO - Name und Version des Clientbetriebssystems (umfasst ULIMIT-Informationen für UNIX und Linux).
- POLICY - Speicherauszug der Maßnahmengruppe
- SCHEDLOG - Inhalt des Planungsprotokolls (normalerweise dsmsched.log).
- CLUSTER - AIX-Clusterinformationen

Anmerkung: Der Befehl **query systeminfo** ist in erster Linie als Hilfe für die IBM Unterstützungsfunktion bei der Diagnose von Problemen gedacht. Aber Benutzer, die mit den in diesen Informationen angesprochenen Konzepten vertraut sind, finden ihn möglicherweise auch nützlich. Wenn Sie die Option **console** verwenden, wird keine besondere Formatierung der Ausgabe ausgeführt, um die Anzeighöhe oder -breite anzupassen. Aus diesem Grund ist die Konsolaausgabe wegen der Länge und des Zeilenumbruchs unter Umständen schwierig zu lesen. In diesem Fall verwenden Sie die Option **filename** mit dem Befehl **query systeminfo**, damit die Ausgabe in eine Datei geschrieben wird, die anschließend an die IBM Unterstützungsfunktion übergeben werden kann.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Syntax

►►—FILENAME =— —Ausgabedateiname—►►

Parameter

Ausgabedateiname

Gibt den Namen der Datei an, in der die Informationen gespeichert werden sollen. Wird kein Dateiname angegeben, werden die Informationen standardmäßig in der Datei dsminfo.txt gespeichert.

Beispiele

Befehlszeile:

```
query systeminfo dsmdptfile errorlog -filename=tsminfo.txt
```

Zugehörige Informationen

„Console“ auf Seite 382

Filesonly

Mit der Option **filesonly** wird die Verarbeitung beim Sichern, Zurückschreiben, Abrufen oder Abfragen *nur* auf Dateien beschränkt.

Sie können keine Verzeichnisse vom IBM Spectrum Protect-Server zurückschreiben oder abrufen, wenn Sie die Option **filesonly** in den Befehlen **restore** oder **retrieve** verwenden. Falls erforderlich, werden jedoch Verzeichnisse mit Standardattributen als Platzhalter für Dateien erstellt, die zurückgeschrieben oder abgerufen werden.

Die Option `filesonly` können Sie auch in folgenden Befehlen verwenden:

- `archive`
- `incremental`
- `query archive`
- `query backup`
- `restore`
- `restore backupset`
- `restore group`
- `retrieve`
- `selective`

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

►—FILESOnly—►

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
dsmc incremental -filesonly
```

Followsymbolic

Bei einer Sicherungsoperation gibt die Option `followsymbolic` an, ob Sie eine symbolische Verbindung als virtuellen Mountpunkt verwenden wollen. Bei einer Zurückschreibungs- oder Abrufoperation gibt die Option `followsymbolic` an, wie der Client für Sichern/Archivieren ein Verzeichnis zurückschreibt, dessen Name mit einer symbolischen Verbindung auf dem Zielsystem für die Zurückschreibung übereinstimmt.

Bei Sicherungsoperationen kann die Option `followsymbolic` sich auf die Einstellung der Option `virtualmountpoint` auswirken. Wenn Sie die Option `virtualmountpoint` verwenden, um eine symbolische Verbindung als virtuellen Mountpunkt anzugeben, müssen Sie auch die Option `followsymbolic` definieren.

Bei Zurückschreibungs- und Abrufoperationen kann `followsymbolic` beeinflussen, wie der Client eine symbolische Verbindung im Dateisystem verarbeitet. Definieren Sie `followsymbolic` nur, wenn der Client versucht, ein Verzeichnis zurückzuschreiben, dessen Name mit einer symbolischen Verbindung auf dem Zielsystem für die Zurückschreibung übereinstimmt.

Wenn Sie `followsymbolic=no` (den Standardwert) angeben, schreibt der Client den Inhalt des Verzeichnisses nicht zurück, sondern gibt die folgende Fehlermeldung zurück:

```
ANS4029E Fehler bei der Verarbeitung von 'Dateibereichsname Pfadname Dateiname':  
Verzeichnispfad kann nicht erstellt werden; eine Datei hat denselben Namen  
wie ein Verzeichnis.
```


Befehlszeile:

-fo1=Yes

Zugehörige Informationen

Bei der Archivierung legt die Option „Archsymlinkasfile“ auf Seite 358 fest, wie der Client symbolische Verbindungen verarbeitet.

Für andere Betriebssysteme als Mac OS X finden Sie in „Symbolische Verbindungen sichern“ auf Seite 240 weitere Informationen über die Verarbeitung symbolischer Verbindungen durch den Client für Sichern/Archivieren.

Forcefailover

Mit der Option forcefailover kann eine sofortige Übernahme des Clients auf dem Sekundärserver stattfinden.

Sie können mit der Option forcefailover eine sofortige Verbindung zum Sekundärserver herstellen, auch wenn der Primärserver noch online ist. Sie können mit dieser Option beispielsweise prüfen, ob eine Übernahme des Clients für Sichern/Archivieren auf dem erwarteten Sekundärserver stattfindet.

Bearbeiten Sie diese Option nicht während des Normalbetriebs.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) ein.

Syntax**Parameter**

Yes

Gibt an, dass der Client sofort eine Verbindung zum Sekundärserver herstellt.

No Gibt an, dass eine Übernahme des Clients auf dem Sekundärserver während der nächsten Anmeldung stattfindet, wenn der Primärserver nicht verfügbar ist. Dies ist der Standardwert.

Beispiele**Optionsdatei:**

FORCEFAILOVER yes

Befehlszeile:

-FORCEFAILOVER=yes

Zugehörige Konzepte:

„Konfiguration und Verwendung der automatisierten Clientübernahme“ auf Seite 98

Zugehörige Tasks:

„Client für automatisierte Übernahme konfigurieren“ auf Seite 102

Fromdate

Mit der Option `fromdate` können Sie in Verbindung mit der Option `fromtime` ein Datum mit Uhrzeit angeben, ab dem Sie während einer Zurückschreibungs-, Ab-ruf- oder Abfrageoperation nach Sicherungen oder Archivierungen suchen wollen.

Vor diesem Datum und dieser Zeit gesicherte oder archivierte Dateien werden nicht berücksichtigt; falls erforderlich, werden jedoch ältere Verzeichnisse berück-sichtigt, um die Dateien zurückzuschreiben oder abzurufen.

Die Option `fromdate` ist in den folgenden Befehlen zu verwenden:

- **delete backup**
- **query archive**
- **query backup**
- **restore**
- **restore group**
- **retrieve**

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

►►—FROMDate =— —Datum—————►►

Parameter

Datum

Das Datum, ab dem nach Sicherungsversionen oder Archivierungskopien ge-sucht werden soll. Das Datum muss in dem mit der Option `dateformat` ausge-wählten Format eingegeben werden.

Wenn `dateformat` in einem Befehl angegeben wird, muss diese Option vor den Optionen `fromdate`, `pitdate` und `todate` stehen.

Beispiele

Befehlszeile:

```
dsmc query backup -fromdate=12/11/2003 "/Users/van/Documents/*"
```

Befehlszeile:

```
dsmc query backup -fromdate=12/11/2003 /home/dilbert/*
```

Fromnode

Mit der Option `fromnode` kann ein Knoten Befehle für einen anderen Knoten aus-führen. Ein Benutzer auf einem anderen Knoten muss mit dem Befehl **set access** die Berechtigung zum Abfragen, Zurückschreiben oder Abrufen von Dateien für diesen anderen Knoten erteilen.

Die Option `fromnode` ist in den folgenden Befehlen zu verwenden:

- **query archive**
- **query backup**

- query filesystem
- query image
- query mgmtclass
- restore
- restore group
- restore image
- retrieve

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Syntax

►—FROMNode =— —Knoten—►

Parameter

Knoten

Gibt den Namen des Knotens auf einer Workstation oder auf einem Dateiserver an, auf dessen Sicherungskopien oder archivierte Dateien zugegriffen werden soll.

Beispiele

Befehlszeile:

```
dsmc query archive -fromnode=bob -subdir=yes "/Users/van/Documents/
*"
```

Befehlszeile:

```
dsmc query archive -fromnode=bob -subdir=yes "/home/jones/*"
```

Fromowner

Die Option fromowner gibt einen alternativen Eigner an, von dem Sicherungsversionen oder archivierte Dateien oder Images zurückgeschrieben werden sollen. Der Eigner muss einem anderen Benutzer eine Zugriffsberechtigung für die Dateien oder Images erteilen.

Sollen beispielsweise Dateien aus dem Verzeichnis /home/devel/proja zurückgeschrieben werden, das *usermike* auf dem System *puma* gehört, und sollen die zurückgeschriebenen Dateien in Ihr eigenes Verzeichnis mit dem Namen /home/id/proja gestellt werden, geben Sie den folgenden Befehl ein:

```
dsmc restore -fromowner=usermike -fromnode=puma /home/devel/proja/
/home/id/proja/
```

Anmerkung: Die Archivierung von Imagezurückschreibungen ist nicht für Mac OS X-Betriebssysteme anwendbar.

Benutzer ohne Rootberechtigung können fromowner=*root* angeben, um auf Dateien des Rootbenutzers zuzugreifen, wenn der Rootbenutzer ihnen eine Zugriffsberechtigung erteilt hat.

Anmerkung: Wenn Sie die Option fromowner ohne die Option fromnode angeben, muss der aktive Benutzer sich auf demselben Knoten befinden wie der in fromowner angegebene Benutzer.

Die Option `fromowner` ist in den folgenden Befehlen zu verwenden:

- **query archive**
- **query backup**
- **query group**
- **query image**
- **restore**
- **restore image**
- **restore group**
- **retrieve**

Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients gültig.

Syntax

►► `FROMowner =` `—Eigner—` ►►

Parameter

Eigner

Name eines alternativen Eigners.

Beispiele

Befehlszeile:

`dsmc query archive "/home/id/proja/*" -fromowner=mark`

Fromtime

Mit der Option `fromtime` können Sie in Verbindung mit der Option `fromdate` eine Anfangszeit angeben, ab der Sie während einer Zurückschreibungs-, Abruf- oder Abfrageoperation nach Sicherungen oder Archivierungen suchen wollen.

Der Client für Sichern/Archivieren ignoriert diese Option, wenn Sie nicht die Option `fromdate` angeben.

Die Option `fromtime` ist in den folgenden Befehlen zu verwenden:

- **delete backup**
- **query archive**
- **query backup**
- **restore**
- **restore group**
- **retrieve**

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

►► `FROMTime =` `—Zeit—` ►►

Parameter

Zeit

Gibt eine Anfangszeit an einem bestimmten Datum an, ab der gesicherte oder archivierte Dateien gesucht werden sollen. Wenn keine Zeit angegeben wird, lautet der Standardwert 00:00:00. Die Zeit muss in dem mit der Option `timeformat` ausgewählten Format angegeben werden.

Wenn die Option `timeformat` in einem Befehl angegeben wird, muss sie vor den Optionen `fromtime`, `pittime` und `totime` stehen.

Beispiele

Befehlszeile:

```
dsmc q b -timeformat=4 -fromt=11:59AM -fromd=06/30/2003 -tot=11:59PM  
-tod=06/30/2003 /home/*
```

Groupname

Verwenden Sie die Option `groupname` im Befehl **backup group**, um den Namen für eine Gruppe anzugeben. Operationen können nur mit neuen Gruppen oder der zurzeit aktiven Version einer Gruppe ausgeführt werden.

Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients außer Mac OS X gültig.

Syntax

►►—GROUPName =— —Name—————►►

Parameter

Name

Gibt den Namen der Gruppe an, die die Dateien enthält, die mit der Option `filelist` gesichert wurden. Verzeichnisbegrenzer sind im Gruppennamen nicht zulässig, da der Gruppenname keine Dateispezifikation, sondern ein Namensfeld ist.

Beispiele

Befehlszeile:

```
backup group -filelist=/home/dir1/filelist1 -groupname=group1  
-virtualfsname=virtfs -mode=full
```

Groups (veraltet)

Diese Option ist veraltet.

Host

Die Option `'host'` gibt die Position des ESX-Zielservers an, auf dem die neue virtuelle Maschine während einer VMware-Zurückschreibungsoperation erstellt wird.

Verwenden Sie diese Option in **restore vm**-Befehlen, um den ESX-Host-Server anzugeben, auf den die Daten zurückgeschrieben werden sollen.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Beispiel

Die virtuelle Maschine auf den ESX-Server mit dem Namen vmesxbld1 zurückschreiben.

```
restore vm -host=vmesxbld1.us.acme.com
```

Httpport

Mit der Option httpport wird eine TCP/IP-Anschlussadresse für den Web-Client angegeben.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Web-Client** im Feld **HTTP-Anschluss** des Profileditors definieren.

Syntax

►►—HTTPport— —Anschlussadresse—►►

Parameter

Anschlussadresse

Gibt die TCP/IP-Anschlussadresse für die Datenübertragung mit dem Web-Client an. Der Wertebereich ist 1000 bis 32767; der Standardwert ist 1581.

Beispiele

Optionsdatei:

```
httpport 1502
```

Befehlszeile:

Nicht zutreffend.

Hsmreparsetag

Die Option hsmreparsetag gibt eine eindeutige Analyseerkennung an, die von einem auf Ihrem System installierten HSM-Produkt erstellt wird.

Viele HSM-Produkte verwenden Analysepunkte, um umgelagerte Dateien abzurufen oder zurückzurufen. Nach der Umlagerung einer Datei verbleibt eine kleine Stubdatei mit demselben Namen wie die ursprüngliche Datei in dem Dateisystem. Die Stubdatei ist ein Analysepunkt, der einen Rückruf der ursprünglichen Datei auslöst, wenn ein Benutzer oder eine Anwendung auf die Stubdatei zugreift. Der

Analysepunkt schließt eine eindeutige Kennung mit der Bezeichnung *Analysekennung* ein, um anzugeben, welches HSM-Produkt die Datei umgelagert hat.

Wenn der IBM Spectrum Protect-Client für Sichern/Archivieren die Analysekennung in einer Stubdatei nicht erkennt, weist der Client für Sichern/Archivieren das HSM-Produkt an, die ursprüngliche Datei zurückzurufen. Sie können verhindern, dass Dateien zurückgerufen werden, wenn Sie die Analysekennung mit der Option `hsmreparsetag` angeben.

Der Client für Sichern/Archivieren erkennt die Analysekennung von HSM-Produkten der folgenden Unternehmen:

- International Business Machines Corp.
- Wisdata System Co. Ltd.
- BridgeHead Software Ltd.
- CommVault Systems, Inc.
- Data Storage Group, Inc.
- Enigma Data Solutions, Ltd.
- Enterprise Data Solutions, Inc.
- Global 360
- GRAU DATA AG
- Hermes Software GmbH
- Hewlett Packard Company
- International Communication Products Engineering GmbH
- KOM Networks
- Memory-Tech Corporation
- Moonwalk Universal
- Pointsoft Australia Pty. Ltd.
- Symantec Corporation

Ist das von Ihnen verwendete HSM-Produkt nicht in der vorherigen Liste enthalten, verwenden Sie die Option `hsmreparsetag`, um die Analysekennung anzugeben. Fragen Sie den Lieferanten des HSM-Produkts nach der Analysekennung, die von dem Produkt verwendet wird.

Unterstützte Clients

Diese Option ist für alle Windows-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (`dsm.opt`) ein.

Syntax

►►—HSMREPARSETAG—*Wert_für_Analysekennung*—————►►

Beispiele

Optionsdatei:

```
exclude.dedup /home/*/* ieobjtype=image
```

Befehlszeile:

Nicht zutreffend.

Zugehörige Verweise:

„Exclude-Optionen“ auf Seite 438

„Include-Optionen“ auf Seite 473

Ifnewer

Mit der Option `ifnewer` wird eine vorhandene Datei nur dann durch die letzte Sicherungsversion ersetzt, wenn die Sicherungsversion neuer ist als die vorhandene Datei.

Wenn die Option `inactive` oder `latest` nicht verwendet wird, werden nur aktive Sicherungsversionen berücksichtigt.

Anmerkung: Verzeichniseinträge werden durch die neueste Sicherungsversion ersetzt, unabhängig davon, ob diese älter oder neuer als die vorhandene Version ist.

Verwenden Sie die Option `ifnewer` in den folgenden Befehlen:

- `restore`
- `restore backupset`
- `restore group`
- `retrieve`

Anmerkung: Diese Option wird ignoriert, wenn für die Option `replace` der Wert `No` definiert wird.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

►►—IFNewer—◄◄

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
dsmc restore "/Users/grover/Documents/*" -sub=y -rep=y -ifnewer
```

```
dsmc restore "/home/grover/*" -sub=y -rep=y -ifnewer
```


Imagegapsize

Verwenden Sie die Option `imagegapsize` im Befehl **backup image**, in der Optionsdatei oder mit der Option `include.image`, um die Mindestgröße der leeren Bereiche auf einem Datenträger anzugeben, die Sie während der Imagesicherung überspringen wollen.

Verwenden Sie diese Option für die LAN-gestützte und die LAN-freie Imagesicherung.

Wenn Sie beispielsweise eine Abstandsgröße von 10 angeben, bedeutet dies, dass ein leerer Plattenbereich mit einer Größe von mehr als 10 KB nicht gesichert wird. Abstände, die genau 10 KB groß sind, werden gesichert. Leere Bereiche, die genau 10 KB und kleiner als 10 KB sind, werden jedoch gesichert, auch wenn sie keine Daten enthalten. Ein leerer Bereich, der kleiner als 10 KB ist, wird jedoch gesichert, auch wenn er keine Daten enthält. Eine kleinere Imageabstandsgröße bedeutet, dass weniger Daten übertragen werden müssen, aber möglicherweise auch einen verminderten Durchsatz. Eine größere Imageabstandsgröße führt dazu, dass mehr Daten übertragen werden müssen, aber möglicherweise auch zu einem besseren Durchsatz.

Unterstützte Clients

Diese Option ist nur für AIX-, Linux- und JFS2-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Serverzeilengruppe der Clientsystemoptionsdatei (`dsm.sys`) oder in die Anweisung `include.image` in der Datei `dsm.sys` ein.

Syntax

►►—`IMAGEGapsize`—*Größe*—————►►

Parameter

Größe

Gibt die Mindestgröße leerer Bereiche in einem AIX JFS2-Dateisystem an, die während einer Imagesicherung übersprungen werden sollen. Sie können das Qualifikationsmerkmal `k` (Kilobyte), `m` (Megabyte) oder `g` (Gigabyte) zusammen mit dem Wert angeben. Ohne Angabe eines Qualifikationsmerkmals wird Kilobyte angenommen. Gültige Werte sind 0 bis 4294967295 KB. Wenn Sie den Wert 0 angeben, werden alle Blöcke einschließlich der unbenutzten Blöcke am Ende des Datenträgers gesichert. Wenn Sie einen anderen Wert als 0 angeben, werden unbenutzte Blöcke am Ende des Datenträgers nicht gesichert. Für LAN-gestützte und LAN-freie Imagesicherung beträgt der Standardwert 32 KB. Diese Option ist sowohl für statische Imagesicherungen als auch für Imagesicherungen auf Momentaufnahmebasis gültig.

Anmerkung: Diese Option ist für AIX JFS2-Dateisysteme gültig. Wenn Sie für `imagegapsize` einen Wert größer 0 für ein anderes Dateisystem als AIX JFS2 angeben, empfangen Sie eine Warnung.

Beispiele

Optionsdatei:

Fügen Sie Folgendes der Serverzeilengruppe in der Datei `dsm.sys` hinzu:
`imagegapsize 1m`

Beispiel einer Einschluss-/Ausschlussliste: `include.image /kalafs1`
`imagegapsize=-128k`

Befehlszeile:

`-imagegapsize=64k`

Imagetofile

Verwenden Sie die Option `imagetofile` im Befehl **restore image**, um anzugeben, dass Sie das Quellenimage in eine Datei zurückschreiben wollen.

Es kann erforderlich sein, das Image in eine Datei zurückzuschreiben, wenn der Zieldatenträger defekte Sektoren enthält oder die Imagedaten bearbeitet werden sollen. Später können Sie ein Datenkopierprogramm Ihrer Wahl verwenden, um das Image von der Datei auf einen Plattendatenträger zu übertragen.

Linux unterstützt das Anhängen einer Imagedatei als logischen Datenträger, sodass Sie innerhalb des Image auf Dateidaten zugreifen können. Nachfolgend einige Beispiele:

- Das Dateisystem `/usr` wurde vom Client für Sichern/Archivieren gesichert. Mit dem folgenden Befehl wird das Dateisystemimage in die Datei `/home/usr.img` zurückgeschrieben:

```
# dsmc restore image /usr /home/usr.img -imagetofile
```

- Um die Imagedatei unter dem Verzeichnis `/mnt/usr` anzuhängen, kann der folgende Mountbefehl ausgeführt werden:

```
# mount /home/usr.img /mnt/usr -o loop=/dev/loop0
```

Jetzt ist der Inhalt des Image unter `/mnt/usr` so verfügbar, als wäre ein reguläres Dateisystem an dieses Verzeichnis angehängt.

Unterstützte Clients

Diese Option ist nur für AIX-, Oracle Solaris- und alle Linux-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

►►—IMAGETOfile—◄◄

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
dsmc restore image /usr /home/usr.img -imagetofile
```

Inactive

Verwenden Sie die Option `inactive`, um sowohl aktive als auch inaktive Objekte anzuzeigen.

Die Option `inactive` können Sie in folgenden Befehlen verwenden:

- `delete group`
- `query backup`
- `query group`
- `query image`
- `query nas`
- `restore`
- `restore group`
- `restore image`
- `restore nas`

Wichtig: Wenn Sie die Option `inactive` bei einer Zurückschreibungsoperation verwenden, sollten Sie auch die Option `pick` oder eine andere Filteroption verwenden, da im Gegensatz zur Option `latest` alle Versionen in einer unbestimmten Reihenfolge zurückgeschrieben werden. Diese Option wird implizit unterstellt, wenn `pitdate` verwendet wird.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

►►—INActive—◄◄

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
dsmc restore "/Users/zoe/Documents/*" -inactive -pick
```

Befehlszeile:

```
dsmc restore "/home/zoe/*" -inactive -pick
```

Incl excl

Die Option `incl excl` gibt den Pfad und Dateinamen der Einschluss-/Ausschlussoptionsdatei an.

Mehrere Anweisungen `incl excl` sind zulässig. Sie müssen diese Option jedoch für jede Einschluss-/Ausschlussdatei angeben.

Stellen Sie sicher, dass Sie Ihre Einschluss-/Ausschlussoptionsdatei in einem Verzeichnis speichern, für das alle Benutzer Lesezugriff haben, z. B. `/etc`.

Bei der Verarbeitung werden die Einschluss-/Ausschlussanweisungen innerhalb der Einschluss-/Ausschlussdatei in derselben Reihenfolge in die Listenpositionen gestellt, die durch die Option `incl excl` belegt sind, und entsprechend verarbeitet.

Ist der Client für die hierarchische Speicherverwaltung auf der Workstation installiert, können Dateien mit Hilfe einer Einschluss-/Ausschlussoptionsdatei von der Sicherung und von der Speicherverwaltung, nur von der Sicherung oder nur von der Speicherverwaltung ausgeschlossen werden.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Datei `dsm.sys` *innerhalb* einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Einschluss/Ausschluss** im Profileditor definieren.

Syntax

►—INCLExcl— *—Dateispezifikation—* ►

Parameter

Dateispezifikation

Gibt den Pfad und den Dateinamen *einer* Einschluss-/Ausschlussoptionsdatei an.

Beispiele

Optionsdatei:

```
INCLExcl /Users/user1/Documents/backup.excl
inclExcl /usr/dsm/backup.excl
inclExcl /etc/inclExcl.def
```

Befehlszeile:

Nicht zutreffend.

Zugehörige Informationen

Weitere Informationen über das Erstellen einer Einschluss-/Ausschlussoptionsdatei finden Sie unter „Einschluss-/Ausschlussliste erstellen“ auf Seite 129.

Hinweise für Clients, die für Unicode aktiviert wurden

Eine Einschluss-/Ausschlussdatei kann Unicode-Format oder Nicht-Unicode-Format haben.

Wenn der zum Erstellen einer Einschluss-/Ausschlusslistendatei verwendete codierte Zeichensatz nicht mit dem auf dem Client-Computer verwendeten codierten Zeichensatz übereinstimmt, können Zeichen in der Datei, die vom codierten Zeichensatz des Clients nicht einem anzeigbaren Zeichen zugeordnet werden können, nicht verarbeitet werden, wenn Sicherungen ausgeführt werden.

Die Verwendung der Unicode-Codierung für Dateien, die Einschluss-/Ausschlusslisten enthalten, eliminiert das Problem mit nicht zugeordneten Zeichen. Sie müssen daher nicht mehr Platzhalterzeichen als Ersatz für die unbekannten Zeichen verwenden.

Mac-Benutzer: Erstellen Sie eine Einschluss-/Ausschlussdatei im Unicode-Format, indem Sie die folgenden Schritte ausführen:

1. Öffnen Sie TextEdit. Klicken Sie auf **Format > Make PlainText**.
2. Geben Sie Ihre include- und exclude-Anweisungen ein.
3. Klicken Sie auf **Datei** und anschließend auf **Speichern unter**.
4. Wählen Sie unter **Textdateicodierung** die Option **Unicode (UTF-8)** oder **Unicode (UTF-16)** aus, geben Sie die Datei und das Zielverzeichnis an und sichern Sie dann die Datei. Fügen Sie nicht die Erweiterung `.txt` hinzu.
5. Fügen Sie eine Option `incl excl`, in der die soeben erstellte Einschluss-/Ausschlussdatei angegeben ist, in Ihre Datei `dsm.sys` ein.
6. Starten Sie den Client für Sichern/Archivieren erneut.

Include-Optionen

Die Include-Optionen geben Objekte an, die Sie für Sicherungs- und Archivierungsservices einschließen wollen.

Die Include-Optionen geben Folgendes an:

- Objekte in einer großen Gruppe ausgeschlossener Objekte, die Sie für Sicherungs- und Archivierungsservices einschließen wollen.
- Objekte in einer großen Gruppe ausgeschlossener Objekte, die Sie für Sicherungs-, Archivierungs-, Image- und Speicherverwaltungsservices einschließen wollen.
- Dateien, die für die Sicherungs- oder Archivierungsverarbeitung eingeschlossen sind und die Sie für die Verschlüsselungsverarbeitung einschließen wollen.
- Dateien, die für die Sicherungs- oder Archivierungsverarbeitung eingeschlossen sind und die Sie auch für die Komprimierungsverarbeitung einschließen wollen.
- Objekte, denen Sie eine bestimmte Verwaltungsklasse zuordnen wollen.
- Eine Verwaltungsklasse, die allen Objekten zugeordnet werden soll, denen nicht explizit eine Verwaltungsklasse zugeordnet wird.
- Dateibereiche, denen Sie speichereffiziente Sicherungsverarbeitung zuordnen wollen.
- Dateibereiche, für die Sie die Option `diskcachelocation` verwenden wollen, damit bestimmte Dateisysteme verschiedene, bestimmte Positionen für ihren Plattencache verwenden.

Wenn Sie Objekten keine bestimmte Verwaltungsklasse zuordnen, wird die Standardverwaltungsklasse in der aktiven Maßnahmengruppe Ihrer Maßnahmendomäne verwendet. Verwenden Sie den Befehl **query mgmtclass**, um Informationen zu den Verwaltungsklassen anzuzeigen, die in der aktiven Maßnahmengruppe verfügbar sind.

Hinweis: Der Client für Sichern/Archivieren vergleicht die Dateien, die verarbeitet werden, mit den in den Include/Exclude-Anweisungen angegebenen Mustern, wobei die Optionsdatei von unten nach oben gelesen wird.

Anmerkung:

1. Die Anweisungen `exclude.fs` und `exclude.dir` überschreiben alle Include-Anweisungen, die mit dem Muster übereinstimmen.
2. Auf dem Server können diese Optionen auch mit der Option `incl excl` definiert werden.

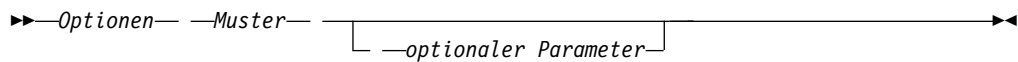
Unterstützte Clients

Diese Option ist für alle Clients gültig. Die Option `include.fs.nas` kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein. Sie können diese Optionen auf der Registerkarte **Einschluss/Ausschluss** im Profileditor definieren.

Syntax



include, include.backup, include.file

Mit diesen Optionen können Sie Dateien einschließen oder Verwaltungsklassen für die Sicherungsverarbeitung zuordnen.

Die Option `include` hat Auswirkungen auf die Archivierungs- und Sicherungsverarbeitung. Wenn Sie unterschiedliche Verwaltungsklassen für die Archivierungs- und Sicherungsverarbeitung zuordnen wollen, müssen Sie `include.archive` und `include.backup` immer mit ihren eigenen Verwaltungsklassen angeben. In diesem Beispiel wird die Verwaltungsklasse `archmc` zugeordnet, wenn eine Archivierungsoperation ausgeführt wird. Die Verwaltungsklasse wird zugeordnet, wenn eine Archivierungsoperation ausgeführt wird, da `include.backup` nur für die Sicherungsverarbeitung und nicht für die Archivierungsverarbeitung verwendet wird.

```
include.archive /home/test/* archmc
include.backup /home/test/*
```

include.archive

Schließt Dateien für die Archivierungsverarbeitung ein oder ordnet Verwaltungsklassen zu.

include.attribute.symlink

Schließt eine Datei oder Dateigruppe, bei denen es sich um symbolische Verbindungen oder Aliasnamen handelt, innerhalb einer größeren Gruppe von ausgeschlossenen Dateien nur bei der Sicherungsverarbeitung ein.

Anmerkung: Für Mac OS X werden Aliasnamen eingeschlossen.

include.compression

Schließt Dateien für die Komprimierungsverarbeitung ein, wenn Sie die Option `compression` auf `yes` setzen. Diese Option gilt für Sicherungen und Archivierungen.

include.dedup

Schließt Dateien bei der clientseitigen Deduplizierung von Daten ein. Zum Steuern einer clientseitigen Operation für die Deduplizierung von Daten können Sie `ieobjtype` als Wert der Option `include.dedup` angeben. Standardmäßig werden alle Objekte, die für die clientseitige Deduplizierung von Daten in Frage kommen, bei der clientseitigen Deduplizierung von Daten eingeschlossen.

Gültige Parameter für `ieobjtype` sind:

- File
- Image

Der Standardwert ist File.

include.encrypt

Schließt die angegebenen Dateien in die Verschlüsselungsverarbeitung ein. Standardmäßig führt der Client keine Verschlüsselungsverarbeitung durch.

Anmerkungen:

1. Die Option `include.encrypt` ist die einzige Möglichkeit, die Verschlüsselung auf dem Client für Sichern/Archivieren zu aktivieren. Werden keine Anweisungen `include.encrypt` verwendet, findet keine Verschlüsselung statt.
2. Die Verschlüsselung ist nicht mit der clientseitigen Deduplizierung kompatibel. Bei der Verschlüsselung eingeschlossene Dateien werden bei der clientseitigen Deduplizierung nicht dedupliziert.
3. Die Verschlüsselung ist nicht mit Sicherungen virtueller VMware-Maschinen kompatibel, bei denen die immer inkrementellen Sicherungsmodi (`MODE=IFIncremental` und `MODE=IFFull`) verwendet werden. Ist der Client für die Verschlüsselung konfiguriert, können Sie nicht die immer inkrementelle Sicherung verwenden.
4. Die Verschlüsselung ist nicht mit IBM Spectrum Protect for Virtual Environments Data Protection for VMware Recovery Agent kompatibel. Ist der Client für die Verschlüsselung konfiguriert, können Sie mit dem Client Sicherungen zurückschreiben, die mit dem Gesamt- oder Teilsicherungsmodus (`MODE=Full` und `MODE=Incremental`) des Clients der Version 7.1 erstellt wurden. Sie können jedoch nicht den Recovery Agent für die Zurückschreibung der verschlüsselten Sicherungen verwenden.

include.fs

Für AIX JFS2-Dateisysteme: Verwenden Sie die Option `snapshotcachesize` in der Datei `dsm.sys` oder mit der Option `include.fs`, um eine geeignete Momentaufnahmengröße anzugeben, sodass während der Dateisicherung oder -archivierung auf Momentaufnahmebasis alle alten Datenblöcke gespeichert werden können.

Für die Steuerung der Verarbeitung Ihres Dateibereichs durch den Client für die Teilsicherung können Sie die folgenden zusätzlichen Optionen in Ihrer Datei `dsm.sys` als Werte der Option `include.fs` angeben: `diskcachelocation` und `memoryefficientbackup`.

Jede der Optionen `include.fs`, `memoryefficientbackup` und `diskcachelocation` muss in der Optionsdatei in derselben Zeile stehen.

```
include.fs /home
memoryefficientbackup=diskcachemethod
diskcachelocation=/usr
include.fs /usr
memoryefficientbackup=diskcachemethod
diskcachelocation=/home
include.fs /Volumes/hfs3
memoryefficientbackup=diskcachemethod
diskcachelocation=/Volumes/hfs2
Nur für AIX JFS2-Dateisysteme: include.fs
/kalafs1 snapshotproviderfs=JFS2
```

Werden diese Optionen sowohl in der Optionsdatei als auch in der Option `include.fs` angegeben, werden die Werte von `include.fs` statt der Werte in einer Optionsdatei oder in der Befehlszeile für den angegebenen Dateibereich verwendet.

include.fs.nas

Verwenden Sie die Option `include.fs.nas`, um eine Verwaltungsklasse an NAS-Dateisysteme zu binden. Sie können auch angeben, ob der Client während einer Imagesicherung des NAS-Dateisystems Inhaltsverzeichnisinformationen (TOC-Informationen) speichert. Verwenden Sie dazu die Option `toc` mit der Option `include.fs.nas` in Ihrer Datei `dsm.sys`. Diese Option ist nur für AIX- und Solaris-Clients gültig.

include.image

Schließt einen Dateibereich oder einen logischen Datenträger ein oder ordnet eine Verwaltungsklasse zu (bei Verwendung im Befehl **backup image**). Der Befehl **backup image** ignoriert alle anderen Einschlussoptionen.

Für Linux x86_64-Clients: Verwenden Sie die Option `snapshotcachesize` in den folgenden Situationen:

- Mit dem Befehl **backup image**
- In der Datei `dsm.sys`
- Mit der Option `include.image`

Wenn Sie die Option `snapshotcachesize` in diesen Situationen verwenden, können Sie eine geeignete Momentaufnahmengröße angeben, sodass während der Imagesicherung alle alten Datenblöcke gespeichert werden können.

Eine Momentaufnahmengröße von 100 Prozent gewährleistet eine gültige Momentaufnahme.

Für AIX JFS2-Dateisysteme: Verwenden Sie die Option `snapshotcachesize` in den folgenden Situationen:

- Mit dem Befehl **backup image**
- In der Datei `dsm.sys`
- Mit der Option `include.image`

Wenn Sie die Option `snapshotcachesize` in diesen Situationen verwenden, können Sie eine geeignete Momentaufnahmengröße angeben, sodass während der Imagesicherung alle alten Datenblöcke gespeichert werden können.

Diese Option ist für AIX-, Linux- und Oracle Solaris-Clients gültig.

Parameter

Muster

Gibt die Objekte an, die für die Sicherungs- oder Archivierungsverarbeitung berücksichtigt werden sollen oder denen eine bestimmte Verwaltungsklasse zugeordnet werden soll.

Anmerkung: Für NAS-Dateisysteme: Sie müssen den NAS-Knotennamen als Präfix vor die Dateispezifikation setzen, um den Dateiserver anzugeben, für den die Einschlussanweisung gilt. Wenn Sie keinen NAS-Knotennamen angeben, bezieht sich das identifizierte Dateisystem auf den NAS-Knotennamen, der in der Clientsystemoptionsdatei (`dsm.sys`) oder in der Befehlszeile angegeben ist.

Wenn das Muster mit einem einfachen oder doppelten Anführungszeichen beginnt oder eingebettete Leerzeichen oder Gleichheitszeichen enthält, muss der Wert in einfache (') oder doppelte (") Anführungszeichen eingeschlossen werden. Die Anführungszeichen am Anfang und am Ende müssen identisch sein.

Für die Option `include.image` ist das Muster der Name eines angehängten Dateisystems oder eines unformatierten logischen Datenträgers.

Optionaler Parameter

Name der Verwaltungsklasse

Gibt den Namen der Verwaltungsklasse an, die den Objekten zugeordnet werden soll. Wenn keine Verwaltungsklasse angegeben wird, wird die Standardverwaltungsklasse verwendet. Verwenden Sie folgende Syntax, um eine Verwaltungsklasse einer Sicherungsgruppe in einer Einschlussanweisung zuzuordnen:

```
include Name_des_virtuellen_Dateibereichs\Gruppenname Verwaltungsklassenname
```

Hierbei gilt Folgendes:

Name_des_virtuellen_Dateibereichs

Gibt den Namen des virtuellen Dateibereichs des IBM Spectrum Protect-Servers, den Sie im Befehl **Backup Group** der Gruppe zugeordnet haben.

Gruppenname

Der Name der Gruppe, die Sie bei Ausführung des Befehls **Backup Group** erstellt haben.

Verwaltungsklassenname

Der Name der Verwaltungsklasse, die den Dateien in der Gruppe zugeordnet werden soll.

Beispiel: Eine Gruppe mit dem Namen 'MyGroup' ist in einem virtuellen Dateibereich mit dem Namen 'MyVirtualFileSpace' gespeichert. Verwenden Sie folgende Syntax, um der Gruppe eine Verwaltungsklasse mit dem Namen TEST zuzuordnen:

```
include MyVirtualFileSpace/MyGroup TEST
```

Tabelle 75. Weitere optionale Parameter

Optionaler Parameter	Verwendung mit der Option
ieobjtype „Ieobjtype“ auf Seite 467	include.dedup
memoryefficientbackup „Memoryefficientbackup“ auf Seite 507	include.fs
diskcachelocation „Diskcachelocation“ auf Seite 405	include.fs
dynamicimage „Dynamicimage“ auf Seite 423	include.image
postsnapshotcmd „Postsnapshotcmd“ auf Seite 533	include.image
presnapshotcmd „Presnapshotcmd“ auf Seite 540	include.image
snapshotcachesize „Snapshotcachesize“ auf Seite 590	include.image
snapshotproviderfs „Snapshotproviderfs“ auf Seite 591	include.image
snapshotproviderimage „Snapshotproviderimage“ auf Seite 592	include.image

Beispiele

Optionsdatei:

```
include /home/proj/text/devel.*
include /home/proj/text/* textfiles
include * managall
include /WAS_ND_NDNODE mgmtclass
include /WAS_APPNODE mgmtclass
include.image /home
include.archive /home/proj/text/
    * myarchiveclass
include.backup /home/proj/text/
    * mybackupclass
include.compression /home/proj/text/
    devel.*
include.encrypt /home/proj/gordon/*
include.fs.nas netappsj/vol/vol0
    homemgmtclass

include.dedup /Users/Administrator/Documents/Important/.../*
```

Nur für AIX:

```
include.image /home
    MGMTCLASSNAME
    snapshotproviderimage=JFS2
    snapshotcachesize=40
include.image /home
    snapshotproviderimage=NONE
include.fs /kalafs1
    snapshotproviderfs=JFS2
```

Nur für LINUX:

```
include.image /home
    snapshotproviderimage=LINUX_LVM
include.image /myfs1 dynamicimage=yes
include.image /home MGMTCLASSNAME
    snapshotproviderimage=NONE
include.image /myfs1 dynamicimage=yes
include.attribute.symlink /home/spike/.../*
include.fs /usr
    memoryefficientbackup=diskcachemethod
```

Befehlszeile:

Nicht zutreffend.

Zugehörige Verweise:


„Snapshotcachesize“ auf Seite 590

„Toc“ auf Seite 619

Zugehörige Informationen:

 Befehl 'mmbackup': IBM Spectrum Protect-Voraussetzungen

 Anleitung für die Integration von IBM Spectrum Scale AFM mit IBM Spectrum Protect

 Hinweise zur Verwendung der Einschluss- und Ausschlussoptionen von IBM Spectrum Protect in Verbindung mit dem IBM Spectrum Scale-Befehl 'mmbackup'

Die Verarbeitung symbolischer Verbindungen und Aliasnamen steuern

IBM Spectrum Protect behandelt symbolische Verbindungen und Aliasnamen (Aliasnamen gelten nur für Mac OS X) als tatsächliche Dateien und sichert sie. Die Datei, auf die durch die symbolische Verbindung verwiesen wird, wird jedoch nicht gesichert.

In einigen Fällen können symbolische Verbindungen und Aliasnamen problemlos reproduziert werden und müssen nicht gesichert werden. Darüber hinaus kann

durch das Sichern dieser symbolischen Verbindungen oder Aliasnamen die Sicherungsverarbeitungszeit zunehmen und ein wesentlicher Bereich des Speichers auf dem IBM Spectrum Protect-Server eingenommen werden.

Sie können die Option `exclude.attribute.symlink` verwenden, um eine Datei oder Dateigruppe, bei denen es sich um symbolische Verbindungen oder Aliasnamen handelt, von der Sicherungsverarbeitung ausschließen. Falls notwendig, können Sie mit Hilfe der Option `include.attribute.symlink` symbolische Verbindungen oder Aliasnamen innerhalb einer breiten Gruppe ausgeschlossener Dateien für die Sicherungsverarbeitung einschließen. Sollen beispielsweise alle symbolischen Verbindungen oder Aliasnamen von der Sicherungsverarbeitung ausgeschlossen werden, mit Ausnahme derjenigen, die sich unter dem Verzeichnis `/home/spike` befinden, geben Sie die folgenden Anweisungen in Ihre Datei `dsm.sys` ein:

```
exclude.attribute.symlink  /.../*
include.attribute.symlink  /home/spike/.../*
```

Zugehörige Verweise:

„Exclude-Optionen“ auf Seite 438

Komprimierungs- und Verschlüsselungsverarbeitung bei der Sicherung

In diesem Abschnitt sind einige Hinweise aufgeführt, die Sie beachten sollten, wenn Sie bestimmte Dateien oder Dateigruppen während einer Sicherungs- oder Archivierungsoperation bei der Komprimierungs- und Verschlüsselungsverarbeitung einschließen wollen.

- Sie müssen die Option `compression` auf *yes* setzen, um die Komprimierungsverarbeitung zu aktivieren. Wenn Sie die Option `compression` nicht angeben oder die Option `compression` auf *no* setzen, führt der Client für Sichern/Archivieren keine Komprimierungsverarbeitung aus.
- Der Client verarbeitet `exclude.fs`, `exclude.dir` und andere Einschluss-/Ausschlussanweisungen zuerst. Danach berücksichtigt der Client alle Anweisungen `include.compression` und `include.encrypt`. Wenn beispielsweise folgende Einschluss-/Ausschlussliste eingegeben wird:

```
exclude /home/jones/proj1/file.txt
include.compression /home/jones/proj1/file.txt
include.encrypt /home/jones/proj1/file.txt
```

Der Client prüft die Anweisung `exclude /home/jones/proj1/file.txt` zuerst und stellt fest, dass `/home/jones/proj1/file.txt` von der Sicherungsverarbeitung ausgeschlossen und daher kein Kandidat für die Komprimierungs- und Verschlüsselungsverarbeitung ist.

- Die Komprimierungs- und Verschlüsselungsverarbeitung von Einschluss-/Ausschlussdateien ist *nur* für die Sicherungs- und Archivierungsverarbeitung gültig.

Zugehörige Verweise:

„Compression“ auf Seite 380

Verarbeitung von NAS-Dateisystemen

Verwenden Sie die Option `include.fs.nas`, um eine Verwaltungsklasse an NAS-Dateisysteme zu binden und zu steuern, ob Inhaltsverzeichnisangaben (TOC-Angaben) für die Dateisystemsicherung gespeichert werden.

Für eine NAS-Dateisystemspezifikation werden folgende Konventionen verwendet:

- NAS-Knoten stellen eine neue Knotenart dar. Der Name des NAS-Knotens identifiziert einen NAS-Dateiserver und seine Daten eindeutig für den Client für Sichern/Archivieren. Sie können den NAS-Knotennamen als Präfix vor die

Dateispezifikation setzen, um den Dateiserver anzugeben, für den die Einschlussanweisung gilt. Wenn Sie keinen NAS-Knotennamen angeben, gilt das angegebene Dateisystem für alle NAS-Dateiserver.

- Unabhängig vom Clientbetriebssystem wird in NAS-Dateisystemspezifikationen der Schrägstrich (/) als Trennzeichen verwendet, wie in diesem Beispiel: /vol/vol0.

Verwenden Sie die folgende Syntax:

►—*Muster*— *Verwaltungsklassenname*— *toc=Wert*—►

Dabei gilt:

Muster

Gibt die Objekte an, die für die Sicherungsservices berücksichtigt werden sollen, denen eine bestimmte Verwaltungsklasse zugeordnet werden soll oder für die die TOC-Erstellung gesteuert werden soll. Sie können Platzhalterzeichen im Muster verwenden.

Verwaltungsklassenname

Gibt den Namen der Verwaltungsklasse an, die den Objekten zugeordnet werden soll. Wird keine Verwaltungsklasse angegeben, wird die Standardverwaltungsklasse verwendet.

toc=Wert

Weitere Informationen enthält der Abschnitt „Toc“ auf Seite 619.

Beispiel 1: Soll dem Dateisystem /vol/vol1 eines NAS-Knotens mit dem Namen netappsj eine Verwaltungsklasse zugeordnet werden, geben Sie die folgende Einschlussanweisung an:

```
include.fs.nas netappsj/vol/vol1 nasMgmtClass toc=yes
```

Beispiel 2: Soll dieselbe Verwaltungsklasse allen Pfaden zugeordnet werden, die dem Dateisystem /vol/ auf einem NAS-Knoten mit dem Namen netappsj untergeordnet sind (beispielsweise /vol/vol1, /vol/vol2 und /vol/vol3), geben Sie die folgende Einschlussanweisung an:

```
include.fs.nas netappsj/vol/* nasMgmtClass toc=yes
```

Include-Optionen für virtuelle Maschinen

Einschluss- und Ausschlussoptionen für virtuelle Maschinen wirken sich auf das Verhalten von Sicherungs- und Zurückschreibungsoperationen für virtuelle Maschinen aus. Diese Optionen werden vor allen Befehlszeilenoptionen verarbeitet. Daher können Optionen in der Befehlszeile Optionen überschreiben, die in den Einschluss- oder Ausschlussoptionen für virtuelle Maschinen angegebenen sind. Informationen zu den Optionen finden Sie in der jeweiligen Optionsbeschreibung.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Zugehörige Verweise:


„Include.vmdisk“ auf Seite 482

„INCLUDE.VMTSMVSS“ auf Seite 488

„INCLUDE.VMSNAPSHOTATTEMPTS“ auf Seite 485

Include.vm:

Bei VM-Operationen überschreibt diese Option die Verwaltungsklasse, die in der Option `vmmc` angegeben ist.

 Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Die in der Option `vmmc` angegebene Verwaltungsklasse gilt für alle VMware-Sicherungen.

Sie können die Option `include.vm` verwenden, um diese Verwaltungsklasse für eine oder mehrere virtuelle Maschinen zu überschreiben. Die durch die Option `vmctlmc` angegebene Verwaltungsklasse wird durch die Option `include.vm` weder überschrieben noch beeinflusst. Die Option `vmctlmc` bindet Steuerdateien für gesicherte virtuelle Maschinen an eine bestimmte Verwaltungsklasse.

Unterstützte Clients

Diese Option kann für unterstützte Linux-Clients verwendet werden, die für die Sicherung virtueller VMware-Maschinen konfiguriert sind.

Optionsdatei

Definieren Sie diese Option in der Clientoptionsdatei.

Syntax

►► INCLUDE.VM — VM-Name — Name_der_Verwaltungsklasse —►

Parameter

VM-Name

Erforderlicher Parameter. Gibt den Namen einer virtuellen Maschine an, die Sie an die angegebene Verwaltungsklasse binden wollen. Der Name ist der Anzeigename der virtuellen Maschine. In jeder Anweisung `include.vm` kann nur eine einzige virtuelle Maschine angegeben werden. Sie können jedoch so viele `include.vm`-Anweisungen angeben wie für das Binden jeder virtuellen Maschine an eine bestimmte Verwaltungsklasse benötigt werden.

Sie können Platzhalterzeichen im Namen der virtuellen Maschine verwenden. Ein Stern (*) entspricht einer beliebigen Zeichenfolge. Ein Fragezeichen (?) entspricht einem einzelnen Zeichen. Wenn der Name der virtuellen Maschine ein Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen (") ein.

Tipp: Wenn der Name der virtuellen Maschine Sonderzeichen enthält, ersetzen Sie die Sonderzeichen durch das Platzhalterzeichen ? (Fragezeichen), wenn Sie den Namen der virtuellen Maschine angeben.

Verwaltungsklassenname

Optionaler Parameter. Gibt die Verwaltungsklasse an, die bei der Sicherung der angegebenen virtuellen Maschine verwendet werden soll. Wird dieser Parameter nicht angegeben, wird standardmäßig die globale Verwaltungsklasse für virtuelle Maschinen verwendet, die durch die Option `vmmc` angegeben ist.

Beispiele

Für diese Beispiele wird vorausgesetzt, dass die folgenden Verwaltungsklassen vorhanden und auf dem IBM Spectrum Protect-Server aktiv sind:

- MCFORTESTVMS
- MCFORPRODVMS
- MCUNIQUEVM

Beispiel 1

Mit der folgenden Anweisung `include.vm` in der Clientoptionsdatei werden alle virtuellen Maschinen, deren Namen mit VMTEST beginnen, an die Verwaltungsklasse MCFORTESTVMS gebunden:

```
include.vm vmtest* MCFORTESTVMS
```

Beispiel 2

Mit der folgenden Anweisung `include.vm` in der Clientoptionsdatei wird die virtuelle Maschine mit dem Namen WHOPPER VM1 [PRODUCTION] an die Verwaltungsklasse MCFORPRODVMS gebunden:

```
include.vm "WHOPPER VM1 ?PRODUCTION?" MCFORPRODVMS
```

Der Name der virtuellen Maschine muss in Anführungszeichen eingeschlossen werden, weil er Leerzeichen enthält. Außerdem wird das Fragezeichen als Platzhalterzeichen für die Sonderzeichen im Namen der virtuellen Maschine verwendet.

Beispiel 3

Mit der folgenden Anweisung `include.vm` in der Clientoptionsdatei wird die virtuelle Maschine VM1 an die Verwaltungsklasse MCUNIQUEVM gebunden:

```
include.vm VM1 MCUNIQUEVM
```

Include.vmdisk:

Mit der Option `INCLUDE.VMDISK` wird eine Platte einer virtuellen Maschine (VM) in Sicherungsoperationen eingeschlossen. Wenn Sie nicht mindestens einen Plattenkennsatz angeben, werden alle Platten in der VM gesichert.

Diese Option ist nur verfügbar, wenn Sie das lizenzierte Produkt 'IBM Spectrum Protect for Virtual Environments' verwenden. Weitere Informationen zu dieser Option finden Sie in der Produktdokumentation zu IBM Spectrum Protect for Virtual Environments im IBM Knowledge Center unter <http://www.ibm.com/support/knowledgecenter/SSERB6/welcome>.

Die Option `INCLUDE.VMDISK` gibt den Kennsatz einer VM-Platte an, die in eine Operation **backup vm** eingeschlossen werden soll. Wenn Sie im Befehl **backup vm** eine Platte einschließen, überschreiben die Befehlszeilenparameter alle Anweisungen `INCLUDE.VMDISK` in der Optionsdatei.

INCLUDE.VMDISK für virtuelle VMware-Maschinen

Verwenden Sie die Option `INCLUDE.VMDISK`, um eine virtuelle VMware-Maschine in Sicherungsoperationen einzuschließen.

Unterstützte Clients

Diese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Optionsdatei

Definieren Sie diese Option in der Clientoptionsdatei. Befehlszeilenparameter überschreiben Anweisungen in der Optionsdatei.

Syntax für virtuelle VMware-Maschinen

►—INCLUDE.VMDISK—*VM-Name*—*VM-Plattenkennsatz*—►

Parameter

VM-Name

Gibt den Namen der virtuellen Maschine an, die eine Platte enthält, die in eine Operation **Backup VM** eingeschlossen werden soll. Der Name ist der Anzeigename der virtuellen Maschine. In jeder Anweisung INCLUDE.VMDISK können Sie nur den Namen einer einzigen virtuellen Maschine angeben. Geben Sie zusätzliche INCLUDE.VMDISK-Anweisungen für jede Platte einer virtuellen Maschine, die Sie einschließen wollen, an.

Der Name der virtuellen Maschine kann einen Stern (*) enthalten, der einer beliebigen Zeichenfolge entspricht, und ein Fragezeichen (?), das einem beliebigen einzelnen Zeichen entspricht. Schließen Sie den VM-Namen in Anführungszeichen („ ") ein, wenn der VM-Name Leerzeichen enthält.

Tipp: Wenn der Name der virtuellen Maschine Sonderzeichen enthält, wie z. B. eckige Klammern ([oder]), wird der Name der virtuellen Maschine möglicherweise nicht korrekt abgeglichen. Enthält der Name der virtuellen Maschine Sonderzeichen, müssen Sie möglicherweise ein Fragezeichen (?) verwenden, um die Sonderzeichen im VM-Namen abzugleichen.

Soll z. B. Hard Disk 1 bei der Sicherung der virtuellen Maschine "Windows VM3 [2012R2]" berücksichtigt werden, verwenden Sie diese Syntax in der Optionsdatei: INCLUDE.VMDISK "Windows VM3 ?2012R2?" "Hard Disk 1"

VM-Plattenkennsatz

Gibt den Plattenkennsatz der Platte an, die eingeschlossen werden soll. Platzhalterzeichen sind nicht zulässig. Verwenden Sie den Befehl **Backup VM** mit der Option -preview, um die Plattenkennsätze der Platten in einer bestimmten virtuellen Maschine zu bestimmen. Informationen zur Syntax finden Sie in der Beschreibung des Befehls "**Backup VM**".

Beispiele

Optionsdatei

Beispiel: Eine virtuelle Maschine mit dem Namen vm1 enthält vier Platten mit den Kennsätzen "Festplatte 1", "Festplatte 2", "Festplatte 3" und "Festplatte 4". Um nur Festplatte 2 in Operationen **Backup VM** einzuschließen, geben Sie in der Optionsdatei Folgendes an:

```
INCLUDE.VMDISK "vm1" "Festplatte 2"
```

Festplatte 2 und Festplatte 3 in Operationen **Backup VM** einschließen:

```
INCLUDE.VMDISK "vm1" "Festplatte 2"  
INCLUDE.VMDISK "vm1" "Festplatte 3"
```

Befehlszeile:

Eine einzelne Platte bei der Sicherung von vm1 einschließen:

```
dsmc backup vm "vm1:vmdk=Festplatte 1"
```

Festplatte 2 und Festplatte 3 bei der Sicherung von vm1 einschließen:

```
dsmc backup vm "vm1:vmdk=Festplatte 2:vmdk=Festplatte 3"
```

Zugehörige Verweise:

„Backup VM“ auf Seite 710

„Restore VM“ auf Seite 791

„Domain.vmfull“ auf Seite 414

„Exclude.vmdisk“ auf Seite 443

Include.vmlocalsnapshot:

Diese Option gibt die Verwaltungsklasse an, die auf lokale Sicherungen von virtuellen VMware-Maschinen angewendet wird. Die Verwaltungsklasse definiert die Aufbewahrungsmaßnahmen für die lokalen Sicherungen.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Sie können diese Option nur für virtuelle Maschinen verwenden, die in einem Datenspeicher für virtuelle Datenträger (VVOL) gespeichert werden.

Unterstützte Clients

Diese Option kann für unterstützte Linux-Clients verwendet werden, die für die Sicherung von virtuellen VMware-Maschinen konfiguriert sind.

Optionsdatei

Definieren Sie diese Option in der Clientoptionsdatei.

Syntax

```
▶▶ INCLUDE.VMLOCALSNAPSHOT — VM-Name — Verwaltungsklassenname ▶▶
```

Parameter

VM-Name

Gibt den Namen einer virtuellen Maschine an, die Sie für lokale Sicherungsoperationen an die angegebene Verwaltungsklasse binden wollen. Der Name ist der Anzeigename der virtuellen Maschine.

In einer Anweisung INCLUDE.VMLOCALSNAPSHOT kann nur jeweils eine virtuelle Maschine angegeben werden. Sie können jedoch so viele INCLUDE.VMLOCALSNAPSHOT-Anweisungen angeben wie für das Binden jeder virtuellen Maschine an eine bestimmte Verwaltungsklasse benötigt werden.

Sie können Platzhalterzeichen im Namen der virtuellen Maschine verwenden. Ein Stern (*) entspricht einer beliebigen Zeichenfolge. Ein Fragezeichen (?) entspricht einem einzelnen Zeichen. Wenn der Name der virtuellen Maschine ein Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen (") ein.

Tipp: Wenn der Name der virtuellen Maschine Sonderzeichen enthält, ersetzen Sie die Sonderzeichen durch das Platzhalterzeichen ? (Fragezeichen), wenn Sie den Namen der virtuellen Maschine angeben.

Verwaltungsklassenname

Gibt die Verwaltungsklasse an, die für lokale Sicherungen der virtuellen Maschine verwendet werden soll. Wird dieser Parameter nicht angegeben, wird standardmäßig die globale Verwaltungsklasse für virtuelle Maschinen verwendet, die durch die Option `vmmc` angegeben ist.

Beispiele

Für diese Beispiele wird vorausgesetzt, dass die folgenden Verwaltungsklassen vorhanden und auf dem IBM Spectrum Protect-Server aktiv sind:

- MCFORTESTVMS
- MCFORPRODVMS
- MCUNIQUEVM

Beispiel 1

Mit der folgenden Anweisung `INCLUDE.VMLOCALSNAPSHOT` in der Clientoptionsdatei werden alle virtuellen Maschinen, deren Namen mit `VMTEST` beginnen, an die Verwaltungsklasse `MCFORTESTVMS` gebunden:

```
include.vmlocalsnapshot vmtest* MCFORTESTVMS
```

Beispiel 2

Mit der folgenden Anweisung `INCLUDE.VMLOCALSNAPSHOT` in der Clientoptionsdatei wird die virtuelle Maschine mit dem Namen `WHOPPER VM1 [PRODUCTION]` an die Verwaltungsklasse `MCFORPRODVMS` gebunden:

```
include.vmlocalsnapshot "WHOPPER VM1 ?PRODUCTION?" MCFORPRODVMS
```

Der Name der virtuellen Maschine muss in Anführungszeichen eingeschlossen werden, weil er Leerzeichen enthält. Außerdem wird das Fragezeichen als Platzhalterzeichen für die Sonderzeichen im Namen der virtuellen Maschine verwendet.

Beispiel 3

Mit der folgenden Anweisung `INCLUDE.VMLOCALSNAPSHOT` in der Clientoptionsdatei wird die virtuelle Maschine `VM1` an die Verwaltungsklasse `MCUNIQUEVM` gebunden:

```
include.vmlocalsnapshot VM1 MCUNIQUEVM
```

Zugehörige Verweise:

„Backup VM“ auf Seite 710

„Vmmc“ auf Seite 659

INCLUDE.VMSNAPSHOTATTEMPTS:

Bestimmen Sie mithilfe der Option `INCLUDE.VMSNAPSHOTATTEMPTS` die Gesamtzahl Versuche, eine Momentaufnahme für eine Sicherungsoperation für eine virtuelle Maschine (VM) zu erstellen, die aufgrund eines Momentaufnahmefehlers fehlschlägt.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Unterstützte Clients

Diese Option kann für unterstützte Linux-Clients verwendet werden, die für die Sicherung virtueller VMware-Maschinen konfiguriert sind.

Optionsdatei

Diese Option ist in der Clientoptionsdatei (dsm.opt) gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. In der Befehlszeile ist sie nicht gültig.

Syntax

```
►—INCLUDE.VMSNAPSHOTATTEMPTS—VM-Name—Anzahl_mit_Stillegung—————►  
►—Anzahl_ohne_Stillegung—————►◀
```

Parameter

VM-Name

Ein erforderlicher positionsgebundener Parameter, der den Namen der virtuellen Maschine angibt, für die die Gesamtzahl Versuche zur Erstellung einer Momentaufnahme ausgeführt werden soll, wenn ein Sicherungsversuch aufgrund eines Momentaufnahmefehlers fehlschlägt. Der Name ist der Anzeigenname der virtuellen Maschine.

In einer Anweisung INCLUDE.VMSNAPSHOTATTEMPTS kann nur jeweils eine virtuelle Maschine angegeben werden. Sie können jedoch mit den folgenden Methoden die Gesamtzahl der Momentaufnahmeversuche für andere virtuelle Maschinen konfigurieren:

- Geben Sie für jede virtuelle Maschine, für die diese Option gelten soll, so viele Anweisungen INCLUDE.VMSNAPSHOTATTEMPTS an, wie Wiederholungsversuche zur Erstellung von Momentaufnahmen, die fehlgeschlagen sind, erforderlich sind.
- Verwenden Sie Platzhalterzeichen für den Parameterwert *VM-Name*, um Namen virtueller Maschinen anzugeben, die mit dem Platzhalterzeichenmuster übereinstimmen. Ein Stern (*) entspricht einer beliebigen Zeichenfolge. Ein Fragezeichen (?) entspricht einem einzelnen Zeichen. Wenn der Name der virtuellen Maschine ein Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen (") ein.

Tipp: Wenn der Name der virtuellen Maschine Sonderzeichen enthält, ersetzen Sie die Sonderzeichen durch das Platzhalterzeichen ? (Fragezeichen), wenn Sie den Namen der virtuellen Maschine angeben.

Anzahl_mit_Stillegung

Ein positionsgebundener Parameter, der die folgende Aktion angibt:

Für VMware-Sicherungsoperation:

- Für virtuelle Windows-Maschinen mit aktiviertem IBM Spectrum Protect-Anwendungsschutz gibt *Anzahl_mit_Stillegung* die Anzahl auszuführender Versuche zur Erstellung der Momentaufnahme mit IBM Spectrum Protect-VSS-Stillegung und Microsoft Windows-System-Provider-VSS-Stillegung an. VSS-Stillegung ist nur für virtuelle Windows-Maschinen gültig.

Abhängig von der von Ihnen angegebenen Anzahl, erfolgt der erste Versuch zur Erstellung einer Momentaufnahme immer mit IBM Spectrum Protect-VSS-Stillegung. Nachfolgende Versuche zur Erstellung einer Momentaufnahme erfolgen mit Windows-System-Provider-VSS-Stillegung.

- Für virtuelle Windows-Maschinen ohne aktivierten IBM Spectrum Protect-Anwendungsschutz und für virtuelle Linux-Maschinen gibt *Anzahl_mit_Stilllegung* die Anzahl Versuche zur Erstellung einer Momentaufnahme mit VMware Tools-Dateisystemstilllegung an.

Der Maximalwert, den Sie angeben können, ist zehn (10). Der Standardwert ist zwei (2). Der Mindestwert, den Sie angeben können, ist null (0).

Anzahl_ohne_Stilllegung

Für VMware-Sicherungsoperation:

Ein positionsgebundener Parameter, der die Anzahl Versuche zur Erstellung einer Momentaufnahme mit inaktiverter VMware Tools-Dateisystemstilllegung und Anwendungsstilllegung (VSS-Stilllegung) angibt, nachdem die angegebene Anzahl Versuche mit VSS-Stilllegung (*Anzahl_mit_Stilllegung*) ausgeführt wurde. Sie können diesen Parameter beispielsweise für eine virtuelle Maschine angeben, die bereits durch einen in einer virtuellen Gastmaschine installierten IBM Data Protection-Agenten geschützt wird.

Der Maximalwert, den Sie angeben können, ist zehn (10). Der Mindestwert, den Sie angeben können und der gleichzeitig der Standardwert ist, ist null (0).

Wichtig: Wenn dieser Parameter auf die Sicherung einer virtuellen Maschine angewendet wird, wird die Sicherung als absturzkonsistent betrachtet. Demzufolge sind Betriebssystem-, Dateisystem- und Anwendungskonsistenz nicht garantiert. Ein Eintrag `include.vmsnapshotattempts 0 0` ist nicht gültig. Für Sicherungsoperationen ist mindestens eine Momentaufnahme erforderlich.

Beispiele

Beispiele für VMware:

Beispiel 1

Mit der folgenden Anweisung `INCLUDE.VMSNAPSHOTATTEMPTS` in der Client-optionsdatei werden insgesamt zwei Momentaufnahmeversuche (mit VSS-Stilllegung) für die virtuelle Maschine 'VM_a' unternommen:

```
INCLUDE.VMSNAPSHOTATTEMPTS VM_a 2 0
```

Beispiel 2

Mit der folgenden Anweisung `INCLUDE.VMSNAPSHOTATTEMPTS` in der Client-optionsdatei werden insgesamt drei Versuche zur Erstellung einer Momentaufnahme für virtuelle Windows-Maschinen ausgeführt, deren Namen mit der Zeichenfolge "vmServer_Dept*" übereinstimmen:

- Der erste Versuch erfolgt mit IBM Spectrum Protect-VSS-Stilllegung.
- Der zweite Versuch erfolgt mit Windows-System-Provider-VSS-Stilllegung.
- Der dritte Versuch zur Erstellung einer Momentaufnahme erfolgt ohne VSS-Stilllegung.

```
INCLUDE.VMSNAPSHOTATTEMPTS vmServer_Dept* 2 1
```

Beispiel 3

Mit der folgenden Anweisung `INCLUDE.VMSNAPSHOTATTEMPTS` in der Client-optionsdatei wird insgesamt ein Momentaufnahmeversuch (mit VSS-Stilllegung)

gung) für virtuelle Maschinen unternommen, deren Namen mit der Zeichenfolge 'vmDB_Dept*' übereinstimmen:

```
INCLUDE.VMSNAPSHOTATTEMPTS vmDB_Dept* 1 0
```

Beispiel 4

Mit der folgenden Anweisung INCLUDE.VMSNAPSHOTATTEMPTS in der Clientoptionsdatei werden insgesamt zwei Versuche zur Erstellung einer Momentaufnahme (mit VSS-Stillegung) für alle virtuelle Maschinen ausgeführt:

- Der erste Versuch erfolgt mit IBM Spectrum Protect-VSS-Stillegung.
- Der zweite Versuch erfolgt mit Windows-System-Provider-VSS-Stillegung.

```
INCLUDE.VMSNAPSHOTATTEMPTS * 2 0
```

Beispiel 5

In diesem Beispiel verfügt die virtuelle Maschine DB15 über einen in einer virtuellen Gastmaschine installierten IBM Data Protection-Agenten und benötigt keine anwendungskonsistente Momentaufnahme. Mit der folgenden Anweisung INCLUDE.VMSNAPSHOTATTEMPTS in der Clientoptionsdatei wird insgesamt ein Versuch zur Erstellung einer Momentaufnahme (ohne VSS-Stillegung) für die virtuelle Maschine DB15 ausgeführt:

```
INCLUDE.VMSNAPSHOTATTEMPTS DB15 0 1
```

Zugehörige Verweise:

„INCLUDE.VMTSMVSS“

INCLUDE.VMTSMVSS:

Mit der Option INCLUDE.VMTSMVSS werden Anwendungen einer virtuellen Maschine benachrichtigt, dass eine Sicherung bevorsteht. Durch diese Option ist es möglich, dass die Anwendung Transaktionsprotokolle abschneidet und Transaktionen festschreibt, so dass sie nach Beendigung der Sicherung in einem konsistenten Zustand fortfahren kann. Ein optionaler Parameter kann angegeben werden, der das Abschneiden der Transaktionsprotokolle unterdrückt.

Wenn eine virtuelle Maschine durch diese Option eingeschlossen wird, stellt IBM Spectrum Protect Anwendungsschutz bereit. Das heißt, der Client blockiert (freeze) die VSS-Ausgabeprogramme, gibt sie frei (thaw) und schneidet optional die Anwendungsprotokolle ab.

Wenn eine virtuelle VMware-Maschine nicht durch diese Option geschützt ist, wird Anwendungsschutz von VMware bereitgestellt. VMware blockiert (freeze) die VSS-Ausgabeprogramme und gibt sie frei (thaw), aber Anwendungsprotokolle werden nicht abgeschnitten.

Wenn eine virtuelle Hyper-V-Maschine nicht durch diese Option geschützt ist, wird Anwendungsschutz von Hyper-V bereitgestellt. Hyper-V blockiert (freeze) die VSS-Ausgabeprogramme und gibt sie frei (thaw), aber Anwendungsprotokolle werden nicht abgeschnitten.

Wichtig: Vor der Ausführung von Sicherungen mit Anwendungsschutz müssen Sie sicherstellen, dass sich die Anwendungsdatenbank (z. B. die Microsoft SQL Server-Datenbank oder die Microsoft Exchange Server-Datenbank) auf einem nicht bootenden Laufwerk (beliebiges Laufwerk außer dem Bootlaufwerk) befindet, falls eine **diskshadow revert**-Operation während der Zurückschreibung erforderlich ist.

Unterstützte Clients

Diese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Optionsdatei

Definieren Sie diese Option in der Clientoptionsdatei. Diese Option kann nicht vom Profileditor und nicht in der Befehlszeile angegeben werden.

Syntax

►►—INCLUDE.VMTSMVSS—*VM-Name*— —OPTions=KEEPSqllog—◄◄

Parameter

VM-Name

Gibt den Namen der virtuellen Maschine an, die die Anwendungen enthält, die in den Wartemodus versetzt werden sollen. Der Name ist der Anzeigename der virtuellen Maschine. Geben Sie eine einzige virtuelle Maschine pro Anweisung INCLUDE.VMTSMVSS an. Um beispielsweise eine virtuelle Maschine mit dem Namen 'Windows VM3 [2012R2]' einzuschließen, verwenden Sie diese Syntax in der Optionsdatei: INCLUDE.VMTSMVSS "Windows VM3 [2012R2]".

Verwenden Sie einen Stern als Platzhalterzeichen, um alle virtuellen Maschinen mit dieser Option zu schützen (INCLUDE.VMTSMVSS *). Sie können auch Fragezeichen als Platzhalterzeichen für beliebige einzelne Zeichen verwenden. Mit der Angabe INCLUDE.VMTSMVSS vm?? werden z. B. alle virtuellen Maschinen geschützt, deren Namen mit 'vm' und zwei beliebigen weiteren Zeichen beginnen (vm10, vm11, vm17 usw.).

Tipp: Wenn der Name der virtuellen Maschine Sonderzeichen enthält, wie z. B. eckige Klammern ([oder]), wird der Name der virtuellen Maschine möglicherweise nicht korrekt abgeglichen. Enthält der Name einer virtuellen Maschine Sonderzeichen, können Sie mit dem Fragezeichen (?) die Sonderzeichen im VM-Namen abgleichen.

Für diesen Parameter gibt es keinen Standardwert. Sie müssen virtuelle Maschinen, die geschützt werden sollen, in mindestens einer Anweisung INCLUDE.VMTSMVSS angeben, um den Anwendungsschutz zu aktivieren. Stellen Sie sicher, dass keine Platte in einer virtuellen Maschine ausgeschlossen wird (mit der Option EXCLUDE.VMDISK), wenn die Platte Anwendungsdaten enthält, die geschützt werden sollen.

OPTions=KEEPSqllog

Wenn der Parameter OPTions KEEPSqllog in einer Anweisung INCLUDE.VMTSMVSS angegeben wird, verhindert er, dass SQL Server-Protokolle abgeschnitten werden, wenn ein Client für Sichern/Archivieren, der auf einem Knoten der Einheit zum Versetzen von Daten installiert ist, eine virtuelle Maschine sichert, auf der ein SQL Server ausgeführt wird. Die Angabe dieses Parameters ermöglicht es dem SQL Server-Administrator, die SQL Server-Protokolle manuell zu verwalten (sichern und ggf. abschneiden), sodass sie beibehalten und für die Zurückschreibung von SQL-Transaktionen an einen bestimmten Prüfpunkt verwendet werden können, nachdem die virtuelle Maschine zurückgeschrieben wurde.

Wenn diese Option angegeben wird, wird das SQL-Protokoll nicht abgeschnitten und die folgende Nachricht wird angezeigt und auf dem Server protokolliert:

ANS4179I Der IBM Spectrum Protect-Anwendungsschutz hat die Microsoft SQL Server-Protokolle auf der virtuellen Maschine 'VM' nicht abgeschnitten.

Sie können die Option `OPTIONS=KEEPSQLLOG` entfernen, um das Abschneiden der SQL-Protokolle bei Beendigung einer Sicherung zu ermöglichen.

Anmerkung: Der Client sichert nicht die SQL-Protokolldateien. Der SQL-Administrator muss die Protokolldateien sichern, damit sie nach dem Zurückschreiben der Datenbank angewendet werden können.

Beispiele

Optionsdatei



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird. Anwendungsschutz für eine virtuelle Maschine mit dem Namen 'vm_example' konfigurieren:

```
INCLUDE.VMTSMVSS vm_example
```

Anwendungsschutz für vm11, vm12 und vm15 konfigurieren:

```
INCLUDE.VMTSMVSS vm11  
INCLUDE.VMTSMVSS vm12  
INCLUDE.VMTSMVSS vm15 options=keepsqlllog
```

Befehlszeile:

Nicht gültig. Diese Option kann nicht in der Befehlszeile angegeben werden.

Zugehörige Verweise:

Exclude.vmdisk

Include.vmdisk

„INCLUDE.VMSNAPSHOTATTEMPTS“ auf Seite 485

Zugehörige Informationen:

Vmtimeout

Incrbydate

Verwenden Sie die Option `incrbydate` im Befehl **incremental**, um neue und geänderte Dateien zu sichern, deren Änderungsdatum nach dem Datum der letzten auf dem Server gespeicherten Teilsicherung liegt (sofern die Dateien nicht von der Sicherung ausgeschlossen sind).

Wichtig: Dateien, die nach der Verarbeitung des jeweiligen Verzeichnisses durch den Client für Sichern/Archivieren, aber vor Vollendung der Teilsicherung nach Datum geändert oder erstellt werden, werden nicht gesichert und werden auch in zukünftigen Teilsicherungen nach Datum nicht gesichert; es sei denn, die Dateien werden erneut geändert. Führen Sie aus diesem Grund eine regelmäßige reguläre Teilsicherung ohne Angabe der Option `incrbydate` aus.

Eine Teilsicherung nach Datum aktualisiert das Datum und die Uhrzeit der letzten Teilsicherung auf dem Server. Wenn Sie eine Teilsicherung nach Datum nur für ei-

nen Teil eines Dateisystems ausführen, wird das Datum der letzten vollständigen Teilsicherung nicht aktualisiert und bei der nächsten Teilsicherung nach Datum werden die Dateien erneut gesichert.

Wichtig:

Der Zeitpunkt der letzten Teilsicherung bezieht sich auf die Serverzeit und der Zeitpunkt der letzten Dateiänderung auf die Clientzeit. Sind die Clientzeit und die Serverzeit nicht synchronisiert oder befinden der Client und der Server sich in verschiedenen Zeitzonen, wirkt sich dies auf die Teilsicherung nach Datum mit `mode=incremental` aus.

Der Zeitpunkt der letzten Teilsicherung bezieht sich auf die Serverzeit und der Zeitpunkt der letzten Dateiänderung auf die Clientzeit. Sind die Clientzeit und die Serverzeit nicht synchronisiert oder befinden der Client und der Server sich in verschiedenen Zeitzonen, wirkt sich dies auf die Teilsicherung nach Datum und die Imagesicherung mit `mode=incremental` aus.

Sowohl bei vollständigen Teilsicherungen als auch bei Teilsicherungen nach Datum werden neue und geänderte Dateien gesichert. Eine Teilsicherung nach Datum hat eine kürzere Verarbeitungszeit als eine vollständige Teilsicherung und benötigt weniger Speicherbereich. Anders als eine vollständige Teilsicherung hält eine Teilsicherung nach Datum den Serverspeicher jedoch nicht auf dem aktuellen Stand aller Workstationdateien, weil:

- Sicherungsversionen von Dateien, die aus der Workstation gelöscht wurden, hierbei nicht verfallen.
- Sicherungsversionen nicht erneut an eine neue Verwaltungsklasse gebunden werden, wenn sich die Verwaltungsklasse geändert hat.
- Dateien mit geänderten Attributen, wie z. B. ACL-Daten (ACL = Access Control List, Zugriffssteuerungsliste) nur dann gesichert werden, wenn sich auch das Änderungsdatum und die Änderungszeit geändert haben.
- Das Attribut 'Häufigkeit' der Kopiengruppe in den Verwaltungsklassen ignoriert wird.

Tipp: Wenn während der Woche zu wenig Zeit für Sicherungen zur Verfügung steht, aber freie Zeit am Wochenende vorhanden ist, können Sie den Serverspeicher Ihrer Workstationdateien durch eine Teilsicherung mit der Option `incrbydate` an den Wochentagen und eine vollständige Teilsicherung am Wochenende auf dem aktuellen Stand halten.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

►►—INCRbydate—►►

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
dsmc incremental -incrbydate
```

Incremental

Verwenden Sie die Option **incremental** im Befehl **restore image**, um sicherzustellen, dass am Basisimage vorgenommene Änderungen auch auf das zurückgeschriebene Image angewendet werden.

Wird außerdem die Option **deletefiles** verwendet, beinhalten die Änderungen das Löschen von Dateien und Verzeichnissen, die in dem ursprünglichen Image waren, später aber aus der Workstation gelöscht wurden.

Anmerkung: Die Verwendung der Option **incremental** im Befehl **restore image** zur Ausführung einer dynamischen Imagesicherung wird nicht unterstützt.

Unterstützte Clients

Diese Option ist nur für AIX, Linux x86_64, Linux on POWER und Solaris gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

►—INCRemental—►

Beispiele

Befehlszeile:

```
res i "/home/devel/projecta/*" -incremental
```

Instrlogmax

Die Option **instrlogmax** gibt die maximale Größe des Instrumentierungsprotokolls (**dsminstr.log**) in MB an. Während der Sicherungs- oder Zurückschreibungsverarbeitung werden Leistungsdaten für den Client in der Datei **dsminstr.log** erfasst, wenn die Option **enableinstrumentation** auf *yes* gesetzt ist.

Wenn Sie den Wert der Option **instrlogmax** ändern, wird das vorhandene Protokoll erweitert oder gekürzt, um der neuen Größe zu entsprechen. Wird der Wert verkleinert, werden die ältesten Einträge gelöscht, um die Datei auf die neue Größe zu verkleinern.

Unterstützte Clients

Diese Option ist für alle Clients und die IBM Spectrum Protect-API gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (**dsm.sys**) innerhalb einer Serverzeilengruppe ein.

Syntax

Parameter

Größe

Gibt die maximale Größe für die Instrumentierungsprotokolldatei in MB an. Der Wertebereich ist 0 bis 2047. Der Standardwert ist 25.

Wenn die Größe der Datei `dsminstr.log` die maximale Größe überschreitet, wird die Protokolldatei in `dsminstr.log.bak` umbenannt. Nachfolgende Instrumentierungsdaten werden weiterhin in der Datei `dsminstr.log` gesichert.

Wenn Sie 0 angeben, wächst die Protokolldatei unbegrenzt an.

Beispiele

Optionsdatei:

```
instrlogmax 100
```

Befehlszeile:

```
dsmc sel /home/mydir/* -subdir=yes -enableinstrumentation=yes  
-instrlogmax=100
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Zugehörige Verweise:

„Enableinstrumentation“ auf Seite 427

„Instrlogname“

Instrlogname

Die Option `instrlogname` gibt den Pfad und den Namen der Datei an, in der Leistungsdaten gespeichert werden sollen, die der Client für Sichern/Archivieren erfasst.

Wenn Sie die Option `enableinstrumentation yes` verwenden, um Leistungsdaten während der Ausführung von Sicherungs- und Zurückschreibungsoperationen zu erfassen, speichert der Client die Informationen automatisch in einer Protokolldatei.

Standardmäßig werden die Leistungsdaten in der Instrumentierungsprotokolldatei (`dsminstr.log`) in dem Verzeichnis gespeichert, das mit der Umgebungsvariablen `DSM_LOG` (oder der Umgebungsvariablen `DSMI_LOG` für die API-abhängigen Produkte IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server und IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server) angegeben wird. Wenn Sie die Umgebungsvariable `DSM_LOG` nicht definiert haben, wird die Instrumentierungsprotokolldatei im aktuellen Verzeichnis gespeichert (das Verzeichnis, in dem der Befehl **dsmc** ausgegeben wurde).

Verwenden Sie diese Option nur, wenn der Dateiname und die Position des Instrumentierungsprotokolls geändert werden sollen.

Soll die Größe der Protokolldatei gesteuert werden, verwenden Sie die Option `instrlogmax`.

Unterstützte Clients

Diese Option ist für alle Clients und die IBM Spectrum Protect-API gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Wichtig: Geben Sie für die Umgebungsvariable DSM_LOG ein Verzeichnis an, in das das Protokoll gestellt werden soll. Das angegebene Verzeichnis muss Berechtigungen aufweisen, die einen Schreibzugriff von dem Konto zulassen, unter dem der Client ausgeführt wird. Das Stammverzeichnis ist kein gültiger Wert für DSM_LOG.

Syntax

►►—INSTRLOGNAME— —*Dateispezifikation*—►►

Parameter

Dateispezifikation

Gibt den Pfad und den Namen der Datei an, in der Leistungsdaten während der Sicherungs- und Zurückschreibungsverarbeitung gespeichert werden sollen. Wenn ein Teil des von Ihnen angegebenen Pfads nicht vorhanden ist, versucht der Client, ihn zu erstellen.

Wird nur ein Dateiname angegeben, wird die Datei in dem Verzeichnis gespeichert, das mit der Umgebungsvariablen DSM_LOG angegeben wird. Wenn Sie die Umgebungsvariable DSM_LOG nicht definiert haben, wird die Instrumentierungsprotokolldatei im aktuellen Verzeichnis gespeichert (das Verzeichnis, in dem der Befehl **dsmc** ausgegeben wurde). Die Instrumentierungsprotokolldatei kann keine symbolische Verbindung sein.

Für Mac OS X: Wenn Sie nur einen Dateinamen angeben, wird die Datei in Ihrem Standardordner gespeichert. Die Standardverzeichnisse sind:

```
~/Library/Logs/tivoli/tsm  
/Library/Logs/tivoli/tsm
```

Dieser Instrumentierungsprotokolldateiname ersetzt den vorherigen Instrumentierungsprotokolldateinamen dsminstr.report.pXXX, der von der Option TESTFLAG=instrument:detail oder instrument:API erstellt wurde.

Beispiele

Optionsdatei:

Für AIX-, Linux- und Oracle Solaris-Clients:

```
instrlogname /home/user1/mydir/mydsminstr.log
```

Für Mac OS X-Clients:

```
instrlogname /Users/user1/Library/Logs/mydsminstr.log
```

Befehlszeile:

Für AIX-, Linux- und Oracle Solaris-Clients:

```
dsmc sel /home/user1/mydir/* -subdir=yes -instrlogname=/usr/log/mydsminstr.log
```

Für Mac OS X-Clients:

```
dsmc sel /Users/user1/mydir/* -subdir=yes -instrlogname=/Users/user1/Library/Logs/mydsminstr.log
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Zugehörige Verweise:

„Enableinstrumentation“ auf Seite 427

„Instrlogmax“ auf Seite 492

Lanfreecommmethod

Die Option `lanfreecommmethod` gibt das Übertragungsprotokoll zwischen dem IBM Spectrum Protect-Client und dem Speicheragenten an. Dadurch wird die Verarbeitung zwischen dem Client und der an SAN angeschlossenen Speichereinheit aktiviert.

Bei Verwendung der LAN-Übernahme müssen Sie `lanfreecommmethod` in der Datei `dsm.sys` innerhalb einer Serverzeilengruppe angegeben haben.

Für AIX, Linux und Solaris: Verwenden Sie die Option `lanfreeshmport`, um die Shared-Memory-Anschlussnummer anzugeben, an der der Speicheragent empfangsbereit ist.

Unterstützte Clients

Diese Option ist für AIX-, Linux- und Oracle Solaris-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Datei `dsm.sys` innerhalb einer Serverzeilengruppe ein.

Syntax

►—LANFREECommmethod— *Übertragungsmethode* —►

Parameter

Übertragungsmethode

Gibt das unterstützte Protokoll für den Client für Sichern/Archivieren an:

TCPip

Die Übertragungsmethode Transmission Control Protocol/Internet Protocol (TCP/IP).

Verwenden Sie die Option `lanfreetcpport`, um die Nummer des TCP/IP-Anschlusses anzugeben, an dem der Speicheragent empfangsbereit ist. Die Übertragungsmethode TCP/IP ist die Standardeinstellung für Benutzer ohne Rootberechtigung auf allen unterstützten Plattformen.

V6Tcpip

Gibt an, dass abhängig von der Systemkonfiguration und den Ergebnissen einer DNS-Suche (Domain Name Service - Domänennamensservice) entweder TCP/IP v4 oder v6 verwendet werden soll. Das einzige Mal, wenn dies nicht zutrifft, ist bei Verwendung von **dsmc schedule** und `schedmode=prompt`. Es muss eine gültige DNS-Umgebung verfügbar sein.

SHAREdmem

Verwenden Sie die Shared-Memory-Übertragungsmethode, wenn der Client und der Speicheragent auf demselben System ausgeführt werden.

Shared Memory ermöglicht eine bessere Leistung als das TCP/IP-Protokoll. Dies ist die Standardübertragungsmethode für AIX-, Linux- und Solaris-Rootbenutzer. Wenn Sie diese Übertragungsmethode unter AIX angeben, kann der Benutzer des Clients für Sichern/Archivieren als Root oder Nicht-Root angemeldet sein, solange der Speicheragent als Root ausgeführt wird. Wird der Speicheragent nicht als Root ausgeführt, muss die Benutzer-ID, die den Client für Sichern/Archivieren ausführt, mit der Benutzer-ID, die den Speicheragenten ausführt, übereinstimmen.

Beispiele

Optionsdatei:

```
lanfreecommmethod tcp
```

Nur TCP/IP v4 verwenden

```
lanfreecommmethod V6Tcpip
```

Sowohl TCP/IP v4 als auch v6 verwenden, abhängig von der Systemkonfiguration und den Ergebnissen einer DNS-Suche.

Befehlszeile:

```
-lanfreec=tcp
```

```
-lanfreec=V6Tcpip
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Zugehörige Informationen

„Lanfreeshmport“

„Lanfreetcppport“ auf Seite 497

Lanfreeshmport

Verwenden Sie die Option `lanfreeshmport`, wenn `lanfreecommmethod=SHAREdmem` für die Übertragung zwischen dem Client für Sichern/Archivieren und dem Speicheragenten angegeben wird. Dadurch wird die Verarbeitung zwischen dem Client und der an SAN angeschlossenen Speichereinheit aktiviert.

Unterstützte Clients

Diese Option ist für AIX-, Linux- und Oracle Solaris-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein.

Syntax

►►—LANFREEShmport— —Anschlussadresse—◄◄

Parameter

Anschlussadresse

Gibt die Nummer an, mit der die Verbindung zum Speicheragenten hergestellt wird. Der Wertebereich ist 1 bis 32767.

Für Windows-Clients lautet der Standardwert 1.

Mit Ausnahme von Windows-Clients lautet der Standardwert für alle Clients 1510.

Beispiele

Optionsdatei:

lanfrees 1520

Befehlszeile:

-lanfrees=1520

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Zugehörige Informationen

„Lanfreecommmethod“ auf Seite 495

Lanfreetcport

Die Option lanfreetcport gibt die Nummer des TCP/IP-Anschlusses an, an dem der IBM Spectrum Protect-Speicheragent empfangsbereit ist.

Verwenden Sie diese Option, wenn Sie lanfreecommmethod=TCPIP für die Übertragung zwischen dem Client für Sichern/Archivieren und dem Speicheragenten angeben. Geben Sie die Option lanfreetcport nicht an, wenn Sie die Übertragungsmethode NAMEDpipes für LAN-freie Übertragung verwenden wollen.

Unterstützte Clients

Diese Option ist nur für AIX-, Linux x86_64-, Linux on POWER- und Oracle Solaris-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe ein.

Syntax

►►—LANFREETCHPORT— —Anschlussadresse—►►

Parameter

Anschlussadresse

Gibt die Nummer des TCP/IP-Anschlusses an, an dem der Speicheragent empfangsbereit ist. Der Wertebereich ist 1 bis 32767; der Standardwert ist 1500.

Anmerkung: Für die Kommunikation mit dem Speicheragenten (virtuellen Server) muss der lanfreetcport-Wert des Clients mit dem tcport-Wert des

Speicheragenten übereinstimmen. Für die Kommunikation mit dem tatsächlichen Server muss der tcpport-Wert des Clients dem tcpport-Wert des Servers entsprechen.

Beispiele

Optionsdatei:

```
lanfreecpp 1520
```

Befehlszeile:

```
-lanfreecpp=1520
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Zugehörige Informationen

„Lanfreecommethode“ auf Seite 495

Lanfreessl

Verwenden Sie die Option `lanfreessl`, um Secure Sockets Layer (SSL) für eine sichere Client- und Speicheragentenkommunikation zu aktivieren. Diese Option wird nicht mehr unterstützt, wenn Sie die Verbindung zu einem IBM Spectrum Protect-Server der Version 8.1.2 und höheren Stufen sowie der Version 7.1.8 und höheren Stufen der Version 7 herstellen.

Unterstützte Clients

Mit Ausnahme von Mac OS X-Clients wird diese Option auf allen Clients unterstützt.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei ein. Sie können diese Option nicht in der grafischen Benutzeroberfläche oder in der Befehlszeile definieren.

Syntax



Parameter

No Gibt an, dass der Client für Sichern/Archivieren bei der Kommunikation mit dem Speicheragenten nicht SSL verwendet. No ist der Standardwert.

Yes

Gibt an, dass der Client für Sichern/Archivieren bei der Kommunikation mit dem Speicheragenten SSL aktiviert. Zum Aktivieren von SSL geben Sie `lanfreessl=yes` an und ändern Sie den Wert der Option `lanfreecppport`. Die Änderung des Werts der Option `lanfreecppport` ist erforderlich, da der IBM Spectrum Protect-Speicheragent in der Regel so konfiguriert ist, dass er an einem anderen Anschluss für SSL-Verbindungen empfangsbereit ist.

Beispiele

Optionsdatei:

```
lanfreessl yes  
lanfreessl no
```

Befehlszeile:

Nicht gültig. Sie können diese Option nicht in der Befehlszeile definieren.

Lanfreetcpserveraddress

Die Option `lanfreetcpserveraddress` gibt die TCP/IP-Adresse für den IBM Spectrum Protect-Speicheragenten an.

Verwenden Sie diese Option, wenn Sie `lanfreecommmethod=TCPip` oder `V6Tcpip` für die Übertragung zwischen dem Client für Sichern/Archivieren und dem Speicheragenten angeben.

Das Überschreiben des Standardwerts für diese Option ist nützlich, wenn Sie LAN-frei in einer Umgebung konfigurieren, in der der Client und der Speicheragent auf unterschiedlichen Systemen ausgeführt werden. Sie können diese Speicheragentenadresse von Ihrem Administrator erfahren.

Unterstützte Clients

Diese Option ist nur für AIX-, Linux x86_64-, Linux on POWER- und Oracle Solaris-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei ein.

Syntax

►►—LANFREETCPServeraddress— —*Speicheragentenadresse*—————►►

Parameter

Speicheragentenadresse

Gibt eine 1- bis 64-stellige TCP/IP-Adresse für einen Server an. Geben Sie einen TCP/IP-Domännennamen oder eine numerische IP-Adresse an. Die numerische IP-Adresse kann entweder eine TCP/IP-V4- oder eine TCP/IP-V6-Adresse sein. Der Standardwert ist 127.0.0.1 (localhost).

Beispiele

Optionsdatei:

```
LANFREETCPServeraddress stagent.example.com
```

```
LANFREETCPServeraddress 192.0.2.1
```

Befehlszeile:

Nicht zutreffend.

Latest

Verwenden Sie die Option `latest`, um die neueste Sicherungsversion einer Datei zurückzuschreiben, auch wenn die Sicherung inaktiv ist.

Die Option `latest` können Sie in folgenden Befehlen verwenden:

- **restore**
- **restore group**

Wenn Sie eine zeitpunktgesteuerte Zurückschreibung (mit der Option `pitdate`) ausführen, ist es nicht notwendig, `latest` anzugeben, da diese Option bei Verwendung von `pitdate` implizit verwendet wird.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

▶—LATest—▶

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
dsmc restore "/Users/devel/projecta/*" -latest
```

Befehlszeile:

```
dsmc restore "/home/devel/projecta/*" -latest
```

Localbackupset

Die Option `localbackupset` gibt an, ob die GUI des Clients für Sichern/Archivieren die anfängliche Anmeldung beim IBM Spectrum Protect-Server umgeht, um einen lokalen Sicherungssatz auf einer eigenständigen Workstation zurückzuschreiben.

Wenn Sie die Option `localbackupset` auf `yes` setzen, versucht die GUI keine anfängliche Anmeldung beim Server. In diesem Fall aktiviert die GUI nur die Funktionalität für Zurückschreiben.

Wenn Sie die Option `localbackupset` auf `no` (Standardwert) setzen, versucht die GUI die anfängliche Anmeldung beim Server und aktiviert alle GUI-Funktionen.

Anmerkung: Der Befehl **restore backupset** unterstützt die Zurückschreibung lokaler Sicherungssätze auf einer eigenständigen Workstation ohne Verwendung der Option `localbackupset`.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein.

Syntax



Parameter

No Gibt an, dass die GUI eine anfängliche Anmeldung am Server versucht, und aktiviert alle Funktionen. Dies ist der Standardwert.

Yes

Gibt an, dass die GUI keine anfängliche Anmeldung am Server versucht, und aktiviert nur die Funktionalität für Zurückschreiben.

Beispiele

Optionsdatei:

```
localbackupset yes
```

Diese Option ist mit dem Befehlszeilenclient **dsmc** nicht gültig.

Zugehörige Informationen

„Restore Backupset“ auf Seite 777

Makesparsefile

Verwenden Sie die Option **makesparsefile** im Befehl **restore** oder **retrieve**, um anzugeben, wie Dateien mit freien Bereichen erneut erstellt werden.

Dateien mit freien Bereichen haben keinen Plattenspeicherplatz für jeden Block im gesamten Adressraum zugeordnet, was zu freien Datenbereichen innerhalb der Datei führt. Der Client für Sichern/Archivieren erkennt Dateien mit freien Bereichen während einer Sicherungsoperation und markiert sie als solche auf dem IBM Spectrum Protect-Server. Freie Datenbereiche werden durch ihren Inhalt erkannt, der immer null ist.

Wenn Sie die Option **makesparsefile** auf **yes** (Standardwert) setzen, werden die freien Datenbereiche innerhalb der Datei nicht auf Platte geschrieben, sodass während einer Zurückschreibung kein zusätzlicher Plattenspeicherplatz zugeordnet wird.

Wenn Sie die Option **makesparsefile** auf **no** setzen, werden die freien Datenbereiche nicht erneut erstellt, was dazu führt, dass für den gesamten Adressraum Plattenblöcke zugeordnet werden. Dies kann unter Umständen einen größeren belegten Plattenspeicherplatz zum Ergebnis haben. Stellen Sie sicher, dass Sie über ausreichend Plattenspeicherplatz verfügen, um alle Daten zurückzuschreiben.

Auf einigen UNIX- und Linux-Systemen ist es möglicherweise erforderlich, system-spezifische Dateien nicht als Dateien mit freien Bereichen zu sichern. Verwenden Sie die Option **makesparsefile** für Dateien, bei denen die Existenz physischer Plattenblöcke erforderlich ist, wie z. B. bei der Datei **ufsboot** in Solaris, die beim Booten ausgeführt wird. Das Bootdateiladeprogramm des Betriebssystems greift direkt auf die physischen Plattenblöcke zu und unterstützt keine Dateien mit freien Bereichen.

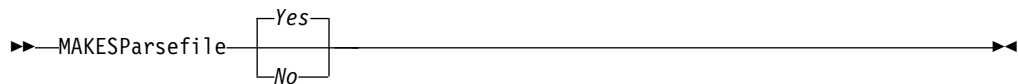
Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients außer Mac OS X gültig.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein.

Syntax



Parameter

Yes

Gibt an, dass freie Datenbereiche innerhalb der Datei nicht geschrieben werden, sodass während einer Zurückschreibung kein zusätzlicher Plattenspeicherplatz zugeordnet wird. Dies ist der Standardwert.

No

Gibt an, dass freie Datenbereiche nicht erneut erstellt werden, was dazu führt, dass für den gesamten Adressraum Plattenblöcke zugeordnet werden.

Beispiele

Optionsdatei:

```
makesparsefile no
```

Befehlszeile:

```
-makesparsefile=no
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Managedservices

Die Option `managedservices` gibt an, ob der IBM Spectrum Protect-Clientakzeptor-service den Scheduler oder den Web-Client oder beides verwaltet.

Einschränkung: Sie können den `dsmcad` nicht für die Planung verwenden, wenn Sie die Option `sessioninitiation` auf `serveronly` setzen.

Der Clientakzeptordämon dient als externer Zeitgeber für den Scheduler. Wenn der Scheduler gestartet wird, fragt er den Server nach dem nächsten geplanten Ereignis. Das Ereignis wird entweder sofort ausgeführt oder der Scheduler wird beendet. Der Clientakzeptordämon startet den Scheduler erneut, wenn der Zeitpunkt für die Ausführung des geplanten Ereignisses gekommen ist.

Anmerkung:

1. Wenn Sie die Option `schedmode` auf `prompt` setzen, fordert der Server über Systemanfrage den Clientakzeptordämon zur Aktion auf, wenn es Zeit ist, den Zeitplan auszuführen. Der Scheduler stellt die Verbindung zum Server her und unterbricht diese, wenn der Clientakzeptordämon zum ersten Mal gestartet wird.

Der Befehl `'dsmc schedule'` kann nicht verwendet werden, wenn sowohl `schedmode prompt` als auch `commmethod V6Tcpi` angegeben werden.

2. Wenn Sie unter Mac OS X die Option `managedservices` nicht angeben, verwaltet der Clientakzeptordämon standardmäßig sowohl das Schedulerprogramm als auch den Web-Client.
3. Setzen Sie die Option `passwordaccess` in Ihrer Datei `dsm.sys` auf `generate` und generieren Sie ein Kennwort, damit IBM Spectrum Protect Ihr Kennwort automatisch verwalten kann.

Die Verwendung des Clientakzeptordämons zum Verwalten des Scheduler-Service kann folgende Vorteile bieten:

- Probleme mit der Speicheraufbewahrungsdauer, die bei den traditionellen Ausführungsmethoden des Schedulers auftreten können, werden beseitigt. Die Verwendung des Clientakzeptordämons zum Verwalten des Schedulers erfordert zwischen den geplanten Operationen sehr wenig Speicher.
- Der Clientakzeptordämon kann sowohl das Schedulerprogramm als auch den Web-Client verwalten, wodurch die Anzahl der Hintergrundprozesse auf Ihrer Workstation reduziert wird.
- Damit der Web-Client verwendet werden kann, müssen Sie diese Option in der `Clientsystemoptionsdatei` angeben.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die `Clientsystemoptionsdatei` (`dsm.sys`) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Web-Client** im Profileditor definieren.

Syntax

►—MANAGEDServices—Modus—►

Parameter

Modus

Gibt an, ob der Clientakzeptordämon den Scheduler, den Web-Client oder beides verwaltet.

webclient

Gibt an, dass der Clientakzeptordämon den Web-Client verwaltet. Dies ist der Standardwert für UNIX und Linux. Beide Werte, `webclient` und `schedule`, sind der Standardwert für Mac OS X.

schedule

Gibt an, dass der Clientakzeptordämon den Scheduler verwaltet. Beide Werte, `webclient` und `schedule`, sind der Standardwert für Mac OS X.

none

Für Mac OS X: Gibt an, dass der Clientakzeptordämon weder den Web-Client noch Zeitpläne verwaltet. Setzen Sie `managedservices` auf `none`, um den Befehl **dsmt schedule** zu aktivieren.

Beispiele

Optionsdatei:

Es folgen Beispiele für die Angabe der Option `managedservices` in Ihrer Clientsystemoptionsdatei (`dsm.sys`).

Task Angeben, dass der Clientakzeptordämon nur den Web-Client verwaltet.

```
managedservices webclient
```

Task Angeben, dass der Clientakzeptordämon nur den Scheduler verwaltet.

```
managedservices schedule
```

Task Angeben, dass der Clientakzeptordämon sowohl den Web-Client als auch den Scheduler verwaltet.

```
managedservices schedule webclient
```

Anmerkung: Die Reihenfolge, in der diese Werte angegeben werden, ist unwichtig.

Task Zur Verwendung des Befehls **`dsmc schedule`** unter Mac OS X Folgendes angeben:

```
managedservices none
```

Befehlszeile:

Nicht zutreffend.

Zugehörige Informationen

„Passwordaccess“ auf Seite 525

Unter „Scheduler konfigurieren“ auf Seite 69 finden Sie Anweisungen zum Konfigurieren des Clientakzeptordämons für die Verwaltung des Schedulers.

„Sessioninitiation“ auf Seite 576

„Cadlistenonport“ auf Seite 372

Maxcmdretries

Mit der Option `maxcmdretries` kann angegeben werden, wie oft der Client-Scheduler auf Ihrer Workstation einen geplanten Befehl, der bei der Ausführung fehlgeschlagen ist, maximal wiederholt.

Die Befehlswiederholung startet nur, wenn der Client-Scheduler noch keine Datei gesichert hat, noch nie eine Verbindung zum Server hergestellt hat oder vor dem Sichern einer Datei fehlgeschlagen ist. Diese Option wird nur verwendet, wenn der Scheduler aktiv ist.

Diese Option kann auch der IBM Spectrum Protect-Administrator definieren. Gibt Ihr Administrator einen Wert für diese Option an, überschreibt dieser Ihre Angabe in der Clientoptionsdatei, nachdem Ihr Clientknoten erfolgreich den Kontakt zum Server hergestellt hat.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Scheduler** im Feld **Max. Anz. Befehlswiederholungen** im Profileditor definieren.

Syntax

►—MAXCMDRetries— *Maximale Anzahl Befehlswiederholungen* —►

Parameter

Maximale Anzahl Befehlswiederholungen

Gibt an, wie oft der Client-Scheduler einen geplanten Befehl, der bei der Ausführung fehlgeschlagen ist, maximal wiederholen kann. Der Wertebereich ist Null bis 9999; Standardwert ist 2.

Beispiele

Optionsdatei:

maxcmdr 4

Befehlszeile:

-maxcmdretries=4

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Mbobjrefreshthresh

Die Option mbobjrefreshthresh (Aktualisierungsschwellenwert für Megablockobjekte) gibt eine Zahl an, die einen Schwellenwert definiert. Wenn die Anzahl der IBM Spectrum Protect-Objekte, die zum Beschreiben eines 128-MB-Megablocks benötigt werden, diesen Wert überschreitet, wird der gesamte Megablock aktualisiert und die Objekte, mit denen dieser Bereich in vorherigen Sicherungen dargestellt wurde, verfallen.

Beim Sichern einer virtuellen Maschine werden die Daten in 128-MB-Einheiten, den sogenannten *Megablöcken*, auf dem IBM Spectrum Protect-Server gespeichert. Wenn sich ein Bereich auf der Produktionsplatte ändert und eine neue Teilsicherung ausgeführt wird, wird ein neuer Megablock erstellt, um die Änderungen an den zuvor gesicherten Daten darzustellen. Da bei jeder Teilsicherung ein neuer Megablock erstellt werden kann, können die Megablocke schließlich die Leistung der IBM Spectrum Protect-Datenbank und folglich die Leistung der meisten IBM Spectrum Protect-Operationen beeinträchtigen.

Verwenden Sie diese Option bei der Schätzung von IBM Spectrum Protect-Objekten, die Produktionsdaten darstellen, für jede Sicherung virtueller Maschinen. Wenn beispielsweise die Anzahl der IBM Spectrum Protect-Objekte diesen Wert überschreitet, wird der Megablock aktualisiert. Bei dieser Aktion wird der gesamte 128-MB-Block auf den Server kopiert und als ein einziges IBM Spectrum Protect-Objekt dargestellt. Der Mindestwert ist 2 und der Maximalwert 8192. Der Standardwert ist 50.

Unterstützte Clients

Diese Option ist für Einheiten zum Versetzen von Daten gültig, die virtuelle VMware-Maschinen schützen. Für diese Option benötigen Sie eine Lizenzvereinbarung für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Optionsdatei

Diese Option ist in der Clientoptionsdatei (dsm.opt) gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. In der Befehlszeile ist sie nicht gültig.

Syntax



Parameter

Der zulässige Mindestwert ist 2 Megablocke, der größte Wert ist 8192 Megablocke. Der Standardwert ist 50 Megablocke.

Beispiele

Definieren Sie die folgende Option, um eine Megablockaktualisierung auszulösen, wenn die Anzahl der Objekte, die zur Darstellung eines aktualisierten Megablocks benötigt werden, 20 Objekte überschreitet:

```
MBOBJREFRESHTHRESH 20
```

Mbpctrefreshthresh

Die Option `mbpctrefreshthresh` (Aktualisierungsschwellenwert für Megablockprozentsatz) gibt eine Zahl an, die einen Schwellenwert definiert. Wenn der Prozentsatz der IBM Spectrum Protect-Objekte, die zum Beschreiben eines 128-MB-Megablocks benötigt werden, diesen Wert überschreitet, wird der gesamte Megablock aktualisiert und die Objekte, mit denen dieser Bereich in vorherigen Sicherungen dargestellt wurde, verfallen.

Beim Sichern einer virtuellen Maschine werden die Daten in 128-MB-Einheiten, den sogenannten *Megablöcken*, auf dem IBM Spectrum Protect-Server gespeichert. Wenn sich ein Bereich auf der Produktionsplatte ändert und eine neue Teilsicherung ausgeführt wird, wird ein neuer Megablock erstellt, um die Änderungen an den zuvor gesicherten Daten darzustellen. Da bei jeder Teilsicherung ein neuer Megablock erstellt werden kann, können die Megablocke schließlich die Leistung der IBM Spectrum Protect-Datenbank und folglich die Leistung der meisten IBM Spectrum Protect-Operationen beeinträchtigen.

Verwenden Sie diese Option für die Schätzung des zusätzlichen Datenvolumens, das für jede virtuelle Maschine gesichert wird. Wenn sich beispielsweise ein 128-MB-Block einer Produktionsplatte um mehr als den angegebenen Prozentsatz ändert, wird der gesamte 128-MB-Block auf den Server kopiert. Der Block wird als ein einziges IBM Spectrum Protect-Objekt dargestellt.

Unterstützte Clients

Diese Option ist für Clients gültig, die als Knoten der Einheit zum Versetzen von Daten agieren und virtuelle VMware-Maschinen schützen. Für diese Option benötigen Sie eine Lizenzvereinbarung für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Optionsdatei

Diese Option ist in der Clientoptionsdatei (dsm.opt) gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. In der Befehlszeile ist sie nicht gültig.

Syntax



Parameter

Der zulässige Mindestwert ist 1 Prozent, der größte Wert ist 99 Prozent. Der Standardwert ist 50 Prozent.

Beispiele

Definieren Sie die folgende Option, um eine Megablockaktualisierung auszulösen, wenn sich mindestens 50 Prozent der Objekte in einem Megablock auf einer Produktionsplatte geändert haben:

```
MBPCTREFRESHTHRESHOLD 50
```

Memoryefficientbackup

Mit der Option `memoryefficientbackup` wird der Speichersparalgorithmus für die Verwendung bei der Verarbeitung von Gesamtsicherungen für Dateibereiche angegeben.

Eine Methode sichert jeweils nur ein einziges Verzeichnis, wodurch weniger Speicher benötigt wird. Die andere Methode verwendet viel weniger Speicher, erfordert aber mehr Plattenspeicherplatz.

Verwenden Sie die Option `memoryefficientbackup` im Befehl **incremental**, wenn Ihre Workstation über wenig Speicher verfügt. Sie können diese Option auch als Parameter für die Option `include.fs` verwenden, um den vom Client für Sichern/Archivieren verwendeten Algorithmus auf Dateibereichsbasis auszuwählen.

Verwenden Sie `memoryefficientbackup=diskcachemethod` für Dateibereiche, die so viele Dateien enthalten, dass der Client die Teilsicherung weder mit der Standardeinstellung, `memoryefficientbackup=no`, noch mit der Einstellung `memoryefficientbackup=yes` ausführen kann.

Der tatsächlich erforderliche Plattenspeicherplatz für die Plattencachedatei, die bei Teilsicherungen des Plattencaches erstellt wird, ist von der Anzahl der Dateien und Verzeichnisse abhängig, die in die Sicherung eingeschlossen werden, sowie von der durchschnittlichen Pfadlänge der zu sichernden Dateien und Verzeichnisse. Für

UNIX und Linux beträgt der Schätzwert 1 Byte pro Zeichen im Pfadnamen. Für Mac OS X beträgt der Schätzwert 4 Byte pro Zeichen im Pfadnamen. Beispiel: Es müssen 1 000 000 Dateien und Verzeichnisse gesichert werden und die durchschnittliche Pfadlänge beträgt 200 Zeichen. In diesem Fall belegt die Datenbank etwa 200 MB für UNIX- und Linux-Clients und 800 MB für Mac OS X-Clients. Ein anderes Schätzverfahren für Planungszwecke besteht darin, die Anzahl der Dateien und Verzeichnisse mit der Länge des längsten Pfads zu multiplizieren, um eine maximale Datenbankgröße zu ermitteln.

Beim Sichern eines über HSM verwalteten Dateisystems wird eine zweite Plattencachedatei für die Liste der umgelagerten Dateien erstellt. Für beide Plattencachedateien zusammen - die bei Teilsicherungen des Plattencaches erstellte Plattencachedatei und die bei Sicherungen von über HSM verwalteten Dateisystemen erstellte Plattencachedatei - können mehr als 400 MB Plattenspeicherplatz pro Million zu sichernder Dateien erforderlich sein. Die Plattencachedatei kann sehr groß werden. Auf dem Dateisystem, das für die Plattencachedatei verwendet wird, muss Unterstützung für große Dateien aktiviert sein.

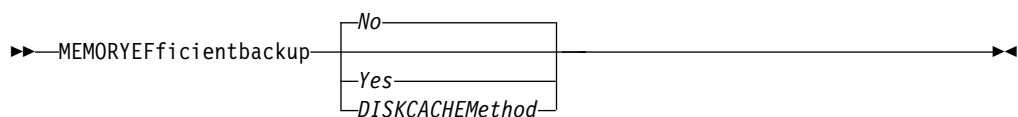
Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Diese Option ist sowohl in dsm.opt als auch innerhalb einer Serverzeilengruppe in dsm.sys zulässig; der Wert in dsm.opt wird jedoch ignoriert, wenn die Option auch in dsm.sys vorhanden ist. Sie können diese Option auch in die Anfangsbefehlszeile einfügen. Im interaktiven Modus kann diese Option mit dem Befehl **incremental** verwendet werden. Sie können diese Option auch auf der Registerkarte **Leistungs-optimierung** im Profileditor und durch Auswahl des Kontrollkästchens **Speichersparalgorithmus verwenden** definieren.

Syntax



Parameter

No Der Clientknoten verwendet die schnellere, speicherintensivere Methode für die Verarbeitung von Teilsicherungen. Dies ist der Standardwert.

Yes

Der Clientknoten verwendet die Methode, bei der weniger Speicher für die Verarbeitung von Teilsicherungen benötigt wird.

Diskcachemethod

Der Clientknoten verwendet die Methode, bei der viel weniger Speicher, aber mehr Plattenspeicherplatz für die Verarbeitung von Teilsicherungen für komplette Dateisysteme benötigt wird.

Beispiele

Optionsdatei:


```
memoryefficientbackup yes
memoryefficientbackup diskcachem
```

Befehlszeile:

```
-memoryef=no
```

Zugehörige Informationen

„Include-Optionen“ auf Seite 473

Mode

Mit der Option 'mode' können Sie den Sicherungsmodus angeben, der bei bestimmten Sicherungsoperationen verwendet werden soll.

Die Option mode bleibt bei Sicherungen unformatierter logischer Einheiten ohne Wirkung.

Die Option mode können Sie in folgenden Sicherungsbefehlen verwenden:

backup image

Angeben, ob eine selektive Imagesicherung oder eine Imageteilsicherung von Clientdateisystemen ausgeführt werden soll.

backup nas

Angeben, ob eine vollständige oder eine differenzielle Imagesicherung von NAS-Dateisystemen ausgeführt werden soll.

backup group

Angeben, ob eine vollständige oder differenzielle Gruppensicherung einer Liste von Dateien ausgeführt werden soll, die sich in einem oder mehreren Dateibereichen befinden.

backup vm

Für virtuelle VMware-Maschinen gibt dieser Parameter an, ob eine immer inkrementelle Gesamtsicherung oder eine immer inkrementelle Teilsicherung virtueller VMware-Maschinen ausgeführt werden soll.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Unterstützte Clients

Mit Ausnahme von Mac OS ist diese Option auf allen unterstützten Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Diese Option ist für Einheiten zum Versetzen von Daten gültig, die virtuelle VMware-Maschinen schützen. Für diese Option benötigen Sie eine Lizenzvereinbarung für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Syntax

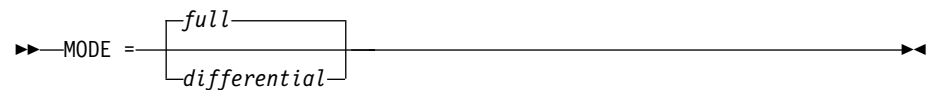
Für Imagesicherungen von Clientdateisystemen



Für Imagesicherungen von NAS-Dateisystemen



Für Gruppensicherungen



Für die Sicherung virtueller VMware-Maschinen



Parameter

Imagesicherungsparameter

selective

Gibt an, dass Sie eine vollständige (selektive) Imagesicherung ausführen wollen. Dies ist der Standardmodus für Imagesicherungen von Clientdateisystemen.

incremental

Gibt an, dass Sie nur die Daten sichern wollen, die sich seit der letzten Imagesicherung geändert haben. Wenn noch keine Imagesicherung erstellt wurde, ist die erste Sicherung eine vollständige Imagesicherung (mode=selective); die Angabe für die Option 'mode' hat dabei keinen Einfluss.

NAS-Sicherungsparameter

differential

Dies ist der Standardwert für NAS-Objekte. Gibt an, dass Sie eine NAS-Sicherung von Dateien ausführen wollen, die sich seit der letzten vollständigen Sicherung geändert haben. Ist keine Kopie eines Gesamtimage auf dem IBM Spectrum Protect-Server vorhanden, wird eine vollständige Sicherung ausgeführt. Ist ein Gesamtimage vorhanden, wird bei Angabe von MODE=differential eine differenzielle Imagesicherung gesendet, unabhängig davon, ob das Image zurückgeschrieben werden kann oder verfallen ist und nur wegen abhängiger differenzieller Images aufbewahrt wird. Wird ein Gesamtimage während einer differenziellen Sicherung gesendet, wird dieses bei Ausführung des Serverbefehls QUERY NASBACKUP als Gesamtimage angezeigt.

Ein Gesamtimage kann auf Basis der Versionsverarbeitung oder der Aufbewahrung (verexists retextra) für den Verfall ausgewählt sein, aber dennoch weiter auf dem Server verwaltet werden, damit abhängige differenzielle Images zurückgeschrieben werden können. Ein Gesamtimage, das für den Verfall ausgewählt ist, kann nicht zum Zurückschreiben ausgewählt werden. Daher wird es nicht angezeigt, wenn der Serverbefehl QUERY NASBACKUP verwendet wird. Die differenziellen Imagesicherungen, die von einem "verfallenen" Gesamtimage abhängig sind, können zurückgeschrieben werden.

full

Gibt an, dass Sie eine vollständige Sicherung von NAS-Dateisystemen ausführen wollen.

Gruppensicherungsparameter

full

Gibt an, dass Sie eine vollständige Sicherung von Gruppenobjekten ausführen wollen. Dies ist der Standardwert für Gruppensicherungen.

differential

Gibt an, dass Sie eine Gruppensicherung von Dateien ausführen wollen, die sich seit der letzten vollständigen Sicherung geändert haben. Ist keine Kopie eines Gesamtimage auf dem IBM Spectrum Protect-Server vorhanden, wird eine vollständige Sicherung ausgeführt. Ist ein Gesamtimage vorhanden, wird bei Angabe von MODE=differential eine differenzielle Imagesicherung gesendet, unabhängig davon, ob das Image zurückgeschrieben werden kann oder verfallen ist und nur wegen abhängiger differenzieller Images aufbewahrt wird. Wird ein Gesamtimage während einer differenziellen Sicherung gesendet, wird dieses bei Ausführung des Serverbefehls QUERY GROUP als Gesamtimage angezeigt.

Ein Gesamtimage kann auf Basis der Versionsverarbeitung oder der Aufbewahrung (verexists retextra) für den Verfall ausgewählt sein, aber dennoch weiter auf dem Server verwaltet werden, damit abhängige differenzielle Images zurückgeschrieben werden können. Ein Gesamtimage, das für den Verfall ausgewählt ist, kann nicht zum Zurückschreiben ausgewählt werden. Daher wird es nicht angezeigt, wenn der Serverbefehl QUERY GROUP verwendet wird. Die differenziellen Imagesicherungen, die von einem "verfallenen" Gesamtimage abhängig sind, können zurückgeschrieben werden.

Parameter für virtuelle VMware-Maschinen

IFFull

Gibt an, dass eine immer inkrementelle Gesamtsicherung einer virtuellen Maschine ausgeführt werden soll. Bei einer immer inkrementellen Gesamtsicherung werden alle verwendeten Blöcke auf den Platten einer virtuellen VMware-Maschine gesichert.

Standardmäßig ist die erste Sicherung einer virtuellen VMware-Maschine selbst dann eine immer inkrementelle Gesamtsicherung (mode=iffull), wenn Sie mode=ifincremental angeben (oder den Standardwert der Option mode verwenden). Bei nachfolgenden Sicherungen wird standardmäßig mode=ifincremental verwendet.

Diesen Sicherungsmodus können Sie nicht für die Sicherung einer virtuellen Maschine verwenden, wenn der Client für die Verschlüsselung der Sicherungsdaten konfiguriert ist.

Eine Beschreibung der Sicherungsstrategie "Immer inkrementell" finden Sie in Sicherungs- und Wiederherstellungstypen.

IFIncremental

Gibt an, dass Sie eine immer inkrementelle Teilsicherung einer virtuellen Maschine ausführen möchten. Bei einer immer inkrementellen Teilsicherung werden nur die Plattenblöcke gesichert, die sich seit der letzten Sicherung geändert haben.

Dieser Modus ist der Standardsicherungsmodus für Sicherungen virtueller VMware-Maschinen.

Diesen Sicherungsmodus können Sie nicht für die Sicherung einer virtuellen Maschine verwenden, wenn der Client für die Verschlüsselung der Sicherungsdaten konfiguriert ist.

Beispiele

Task Eine Sicherung der virtuellen VMware-Maschine `vm1` mit dem Modus `ifincremental` (immer inkrementell, inkrementell) ausführen, damit nur die Daten gesichert werden, die sich seit der letzten Sicherung geändert haben.

```
dsmc backup vm vm1 -mode=ifincremental  
-vmbackuptype=full
```

Task Die NAS-Imagesicherung des gesamten Dateisystems ausführen.

```
dsmc backup nas -mode=full -nasnodename=nas1  
/vol/vol0 /vol/vol1
```

Task Den Dateibereich `/home/test` mithilfe einer Imageteilsicherung sichern, bei der nur Dateien gesichert werden, die seit der letzten vollständigen Imagesicherung neu sind oder sich geändert haben.

```
dsmc backup image /home/test -mode=incremental -snapshotproviderimage=none
```

Task Eine vollständige Sicherung aller in der Dateiliste `/home/dir1/filelist1` angegebenen Dateien auf den virtuellen Dateibereich mit dem Namen `/virtfs` und mit der Hauptmemberdatei `/home/group1` ausführen.

```
dsmc backup group -filelist=/home/dir1/filelist1  
-groupname=group1 -virtualfsname=/virtfs -mode=full
```

Zugehörige Verweise:

„Backup VM“ auf Seite 710

„Backup Group“ auf Seite 699

„Backup Image“ auf Seite 702

„Backup NAS“ auf Seite 708

Monitor

Die Option `monitor` gibt an, ob eine Imagesicherung oder -zurückschreibung von Dateisystemen, die zu einem NAS-Dateiserver gehören, überwacht werden soll (NAS = Network Attached Storage, Netzspeicher).

Wenn Sie `monitor=yes` angeben, überwacht der Client für Sichern/Archivieren die aktuelle NAS-Imagesicherungs- oder -zurückschreibungsoperation und zeigt Verarbeitungsinformationen am Bildschirm an. Dies ist der Standardwert.

Wenn Sie `monitor=no` angeben, überwacht der Client die aktuelle NAS-Imagesicherungs- oder -zurückschreibungsoperation nicht und ist für die Verarbeitung des nächsten Befehls verfügbar.

Verwenden Sie diese Option im Befehl **backup nas** oder **restore nas**.

Unterstützte Clients

Diese Option ist *nur* für AIX-, Linux- und Solaris-Clients gültig.

Syntax



Parameter

Yes

Gibt an, dass Sie die aktuelle NAS-Imagesicherungs- oder -zurückschreibungsoperation überwachen und Verarbeitungsinformationen am Bildschirm anzeigen wollen. Dies ist der Standardwert.

No

Gibt an, dass Sie die aktuelle NAS-Imagesicherungs- oder -zurückschreibungsoperation nicht überwachen wollen.

Beispiele

Befehlszeile:

```
backup nas -mode=full -nasnodename=nas1 -monitor=yes
/vol/vol0 /vol/vol1
```

Myreplicationserver

Die Option myreplicationserver gibt an, welche Zeilengruppe des Sekundärserver der Client im Fall einer Übernahme verwendet.

Die Zeilengruppe des Sekundärserver wird durch die Option replservername angegeben und enthält Verbindungsdaten zum Sekundärserver.

Diese Option wird vom Administrator des IBM Spectrum Protect-Servers für den Clientknoten definiert. Während des normalen Anmeldeprozesses (ohne Übernahme) wird die Option an den Client gesendet und in der Clientoptionsdatei gespeichert.

Bearbeiten Sie diese Option nicht während des Normalbetriebs.

Bearbeiten Sie diese Option nur in Situationen wie den folgenden:

- Der Primärserver ist offline und die Informationen für den Sekundärserver befinden sich nicht in der Optionsdatei.
- Die Informationen des Sekundärserver sind nicht auf dem neuesten Stand oder falsch.

Alle von Ihnen bearbeiteten Werte werden bei Ihrer nächsten Anmeldung am Primärserver entfernt oder aktualisiert.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Diese Option wird in eine Serverzeilengruppe in der Datei dsm.sys eingefügt.

Syntax

►—MYREPLICATIONServer—*Replikationsservername*—►

Parameter

Replikationsservername

Gibt den Namen der Zeilengruppe für den Sekundärserver an, die im Fall einer Übernahme verwendet werden soll. Dieser Wert ist in der Regel der Name des Sekundärservers, nicht der Hostname des Servers. Außerdem muss bei dem Wert des Parameters *Replikationsservername* nicht die Groß-/Kleinschreibung beachtet werden, aber der Wert muss dem für die Option `REPLSERVERName` angegebenen Wert entsprechen.

Beispiele

Optionsdatei:

```
MYREPLICATIONServer TargetReplicationServer1
```

Befehlszeile:

Nicht zutreffend.

Optionsdatei:

Das folgende Beispiel zeigt, wie Optionen für drei unterschiedliche Server in der Datei `dsm.sys` angegeben werden und wie ein Verweis auf den Sekundärserver aussieht.

Verbindungsdaten für mehrere Sekundärserver liegen in Zeilengruppen vor. Jede Zeilengruppe wird durch die Option **replservername** und den Namen des Sekundärservers angegeben.

Die Zeilengruppe **servername** muss die Option **myrePLICATIONserver** enthalten, die auf den Sekundärserver verweist, der durch die Zeilengruppe **replservername** angegeben wird.

Nur ein Sekundärserver kann für jeweils eine Zeilengruppe **servername** angegeben werden.

```
REPLSERVERNAME TargetReplicationServer1
REPLTCPSERVERADDRESS TargetReplicationServer1
REPLTCPSPORT 1505
REPLSSLPORT 1506
REPLSERVERGUID 91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00
```

```
REPLSERVERNAME TargetReplicationServer2
REPLTCPSERVERADDRESS TargetReplicationServer2
REPLTCPSPORT 1505
REPLSSLPORT 1506
REPLSERVERGUID 91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02
```

```
SErvername server_a
  COMMMethod TCPip
  TCPPort 1500
  TCPServeraddress server_hostname1.example.com
  PASSWORDAccess prompt
  MYREPLICATIONServer TargetReplicationServer1
```

```
SErvername server_b
  COMMMethod TCPip
  TCPPort 1500
  TCPServeraddress server_hostname2.example.com
  PASSWORDAccess generate
  INCLExcl /adm/tsm/archive.excl
```

MYREPLICATIONServer	TargetReplicationServer2
SErvername	server_c
COMMMethod	TCPip
TCPPort	1500
TCPServeraddress	server_hostname3.example.com
PASSWORDAccess	generate
MYREPLICATIONServer	TargetReplicationServer1

Zugehörige Konzepte:

„Konfiguration und Verwendung der automatisierten Clientübernahme“ auf Seite 98

Zugehörige Tasks:

„Client für automatisierte Übernahme konfigurieren“ auf Seite 102

Nasnodename

Die Option **nasnodename** gibt den Knotennamen des NAS-Dateiservers bei der Verarbeitung von NAS-Dateisystemen an. Der Client fordert Sie zur Eingabe einer Administrator-ID auf.

Der Knotenname identifiziert den NAS-Dateiserver für den IBM Spectrum Protect-Server. Der Server muss den NAS-Dateiserver registrieren.

Sie können diese Option in der Befehlszeile oder in der Clientsystemoptionsdatei (dsm.sys) angeben.

Sie können den Standardwert in der Datei dsm.sys überschreiben, indem Sie einen anderen Wert in die Befehlszeile eingeben. Wenn Sie die Option **nasnodename** nicht in der Datei dsm.sys angeben, müssen Sie diese Option bei der Verarbeitung von NAS-Dateisystemen in der Befehlszeile angeben.

Die Option **nasnodename** können Sie in folgenden Befehlen verwenden:

- **backup nas**
- **delete filespace**
- **query backup**
- **query filespace**
- **restore nas**

Mit dem Befehl **delete filespace** können Sie NAS-Dateibereiche interaktiv aus dem Serverspeicher löschen.

Verwenden Sie die Option **nasnodename**, um den NAS-Dateiserver zu identifizieren. Fügen Sie die Option **nasnodename** in Ihre Clientsystemoptionsdatei (dsm.sys) ein. Der Wert in der Clientsystemoptionsdatei ist der Standardwert, dieser Wert kann jedoch in der Befehlszeile überschrieben werden. Ist die Option **nasnodename** nicht in der Clientsystemoptionsdatei angegeben, müssen Sie diese Option bei der Verarbeitung von NAS-Dateisystemen in der Befehlszeile angeben.

Mit der Option **class** können Sie die Klasse des zu löschenden Dateibereichs angeben. Verwenden Sie die Option **-class=nas**, um eine Liste der zu einem NAS-Knoten gehörenden Dateibereiche anzuzeigen, in der Sie einen Dateibereich zum Löschen auswählen können.

Informationen zum Löschen von NAS-Dateibereichen mit dem Web-Client finden Sie im Abschnitt zum Sichern Ihrer Daten.

Unterstützte Clients

Diese Option ist nur für die AIX-, Linux- und Solaris-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Allgemein** des Profileditors definieren.

Syntax

►—NASNodename— —Knotenname—►

Parameter

Knotenname

Gibt den Knotennamen für den NAS-Dateiserver an.

Beispiele

Optionsdatei:

nasnodename nas2

Befehlszeile:

-nasnodename=nas2

Nfstimeout

Die Option `nfstimeout` gibt die Wartezeit des Clients auf einen Statussystemaufruf für ein NFS-Dateisystem in Sekunden an, bevor eine Zeitlimitüberschreitung auftritt.

Mit dieser Option können Sie das Standardverhalten von Statusaufrufen für Dateisysteme abmildern. Wenn ein NFS-Dateisystem beispielsweise nicht aktuell ist, wird ein Statussystemaufruf durch NFS wegen Zeitlimitüberschreitung beendet (bedingter Mount) oder er blockiert den Prozess (absoluter Mount).

Wird der Wert dieser Option in einen anderen Wert außer Null geändert, wird vom aufrufenden Modul ein neuer Thread erstellt, um den Statussystemaufruf auszugeben. Der neue Prozess wird vom aufrufenden Thread wegen Zeitlimitüberschreitung beendet, und die Operation kann fortgesetzt werden.

Anmerkung: Unter Solaris kann die Option `nfstimeout` fehlschlagen, wenn der NFS-Mount ein absoluter Mount ist. Bleibt das System hängen, müssen Sie die Option `nfstimeout` inaktivieren und das NFS-Dateisystem wie folgt mit einem bedingten Mount anhängen:

```
mount -o soft,timeo=5,retry=5 machine:/filesystem /mountpoint
```

Die Parameter sind wie folgt definiert:

soft Generiert einen bedingten Mount des NFS-Dateisystems. Tritt ein Fehler auf, gibt die Funktion `stat()` einen Fehler zurück. Wird die Option `hard` verwendet, gibt `stat()` erst dann einen Rückkehrcode aus, wenn das Dateisystem verfügbar ist.

timeo=*n*

Setzt das Zeitlimit für den Fehler eines bedingten Mounts auf *n* Zehntel einer Sekunde.

retry=*n*

Setzt die internen Wiederholungen und die Mountwiederholungen auf *n*, Standardwert ist 10000.

Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Datei `dsm.sys` innerhalb einer Serverzeilengruppe oder in die Clientoptionsdatei (`dsm.opt`) ein.

Syntax

►► —NFSTIMEout— —*Zahl*— ◀◀

Parameter*Zahl*

Gibt die Wartezeit des Clients auf einen Statussystemaufruf für ein Dateisystem in Sekunden an, bevor eine Zeitlimitüberschreitung auftritt. Der Wertebereich ist 0 bis 120; Standardwert ist 0 Sekunden.

Beispiele**Optionsdatei:**

```
nfstimeout 10
```

Befehlszeile:

```
-nfstimeout=10
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Zugehörige Informationen

Unter „Absolute und bedingte NFS-Mounts“ auf Seite 243 finden Sie Informationen zur Handhabung von absoluten und bedingten NFS-Mounts.

Nodename

Verwenden Sie die Option `nodename` in Ihrer Clientoptionsdatei, um Ihre Workstation beim Server zu identifizieren. Für mehrere Betriebssysteme auf der Workstation können verschiedene Knotennamen verwendet werden.

Wenn Sie die Option `nodename` verwenden, werden Sie zur Eingabe des Kennworts aufgefordert, das dem angegebenen Knoten zugeordnet ist, falls ein Kennwort erforderlich ist.

Wenn Sie Dateien vom Server zurückschreiben oder abrufen wollen, während Sie an einer anderen Workstation arbeiten, müssen Sie die Option `virtualnodename` verwenden. Sie können auch die Option `asnodename` verwenden, wenn sie vom Administrator definiert ist.

Wenn eine Verbindung zu einem Server hergestellt wird, muss sich der Client beim Server identifizieren. Diese Anmeldeidentifikation wird wie folgt bestimmt:

- Ist weder ein Eintrag `nodename` in der Datei `dsm.sys` noch ein Eintrag `virtualnodename` in der Clientbenutzeroptionsdatei (`dsm.opt`) vorhanden und wird kein virtueller Knotenname in einer Befehlszeile angegeben, ist die Standardmelde-ID der Name, den der Befehl **hostname** zurückgibt.
- Ist ein Eintrag `nodename` in der Datei `dsm.sys` vorhanden, überschreibt der Eintrag `nodename` den Namen, den der Befehl **hostname** zurückgibt.
- Ist ein Eintrag `virtualnodename` in der Clientsystemoptionsdatei (`dsm.sys`) vorhanden oder wird ein virtueller Knotenname in einer Befehlszeile angegeben, darf dieser Name nicht dem Namen entsprechen, den der Befehl **hostname** zurückgibt. Wenn der Server den virtuellen Knotennamen akzeptiert, ist ein Kennwort erforderlich (wenn die Authentifizierung aktiv ist), auch wenn für die Option `passwordaccess` der Wert `generate` gilt. Sobald eine Verbindung zum Server besteht, ist der Zugriff auf alle Dateien zulässig, die unter Verwendung dieser Anmelde-ID gesichert werden.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Datei `dsm.sys` innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Allgemein** im Feld **Knotenname** im Profileditor definieren.

Syntax

►►—NODename— —Knotenname—————◄◄

Parameter

Knotenname

Gibt einen aus 1 bis 64 Zeichen bestehenden Knotennamen an, für den IBM Spectrum Protect-Services angefordert werden sollen. Der Standardwert ist der Wert, der mit dem Befehl **hostname** zurückgegeben wird.

Wird kein Knotenname angegeben, kann der Knotenname standardmäßig den Hostnamen der Workstation annehmen.

Beispiele

Optionsdatei:

`nodename cougar`

„Virtualnodename“ auf Seite 632

Nojournal

Verwenden Sie die Option **nojournal** im Befehl **incremental**, um anzugeben, dass statt der standardmäßigen journalgestützten Sicherung eine traditionelle vollständige Teilsicherung ausgeführt werden soll.

Die journalgestützte Teilsicherung unterscheidet sich von der traditionellen vollständigen Teilsicherung auf folgende Weise:

- Nicht standardmäßige Kopienhäufigkeiten (außer 0) werden auf dem IBM Spectrum Protect-Server nicht erzwungen.
- Änderungen an speziellen UNIX-Dateien werden vom Journaldämon nicht festgestellt und folglich auch nicht gesichert.

Aus diesen Gründen empfiehlt es sich möglicherweise, regelmäßig die Option **nojournal** zu verwenden, um eine traditionelle vollständige Teilsicherung auszuführen.

Unterstützte Clients

Diese Option ist für den AIX- und Linux-Client für Sichern/Archivieren gültig.

Syntax

►—NOJournal—►

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
dsmc incr /home -nojournal
```

Zugehörige Konzepte:

„Journalgestützte Sicherung“ auf Seite 737

Noprompt

Die Option **noprompt** unterdrückt die Bestätigungsaufforderung, die von den Befehlen **delete group**, **delete archive**, **expire**, **restore image** und **set event** angezeigt wird.

- **delete archive**
- **delete backup**
- **delete group**
- **expire**
- **restore image**

Anmerkung: Der Befehl **restore image** ist nicht für Mac OS X-Betriebssysteme anwendbar.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

►►—NOPrompt—►►

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
dsmc delete archive -noprompt "/Users/van/Documents/*"
```

Befehlszeile:

```
dsmc delete archive -noprompt "/home/project/*"
```

Nrtablepath

Die Option `nrtablepath` gibt die Position der Knotenreplikationstabelle auf dem Client an. Der Client für Sichern/Archivieren verwendet diese Tabelle für die Speicherung von Informationen zu jeder Sicherungs- oder Archivierungsoperation auf dem IBM Spectrum Protect-Server.

Der Server, auf dem Sie Ihre Daten sichern, muss mindestens die Version 7.1 aufweisen und muss Clientknotendaten auf dem Sekundärserver replizieren.

Wenn eine Übernahme stattfindet, könnten die Informationen auf dem Sekundärserver nicht die neueste Version aufweisen, falls vor der Übernahme keine Replikation stattfand. Der Client kann die Informationen in der Knotenreplikationstabelle mit den Informationen vergleichen, die sich auf dem Sekundärserver befinden, um festzustellen, ob die Sicherung auf dem Server die neueste Sicherungsversion ist.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (`dsm.sys`) ein.

Diese Option kann auch in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server konfiguriert werden.

Syntax

►►—NRTABLEPath—*Pfad*—►►

Parameter

Pfad

Gibt die Position an, an der die Datenbank der Knotenreplikationstabelle erstellt wird. Die Standardposition ist das Installationsverzeichnis des Clients für Sichern/Archivieren.

Für Benutzer ohne Rootberechtigung müssen Sie einen Pfad angeben, für den Ihre Benutzer-ID Schreibzugriff hat, z. B. ein temporäres Verzeichnis. Die meisten Benutzer ohne Rootberechtigung haben keinen Zugriff auf das Clientinstallationsverzeichnis.

Einschränkung: Die Knotenreplikationstabelle kann nicht im Stammverzeichnis (/) erstellt werden. Wenn Sie eine Position für die Knotenreplikationstabelle angeben wollen, verwenden Sie nicht das Stammverzeichnis.

Beispiel

Optionsdatei:

```
nrtablepath /Volumes/nrtbl
```

Befehlszeile:

Nicht zutreffend.

Zugehörige Tasks:

„Status replizierter Clientdaten bestimmen“ auf Seite 104

„Client für automatisierte Übernahme konfigurieren“ auf Seite 102

Numberformat

Mit der Option `numberformat` wird das Format angegeben, das zum Anzeigen von Zahlen verwendet werden soll.

Die AIX- und Solaris-Clients unterstützen andere Ländereinstellungen als Englisch, die jede Benutzerschnittstelle beschreiben, deren Position oder Sprache abweicht.

Der Client für Sichern/Archivieren und der Verwaltungsclient erhalten standardmäßig Formatinformationen aus der Ländereinstellungsdefinition, die beim Aufruf des Clients aktiv ist. Ausführliche Informationen zur Definition der länderspezifischen Angaben können der Dokumentation auf dem lokalen System entnommen werden.

Anmerkung: Die Option `numberformat` wirkt sich nicht auf den Web-Client aus. Der Web-Client verwendet das Zahlenformat der Ländereinstellung, die im Browser aktiv ist. Ist im Browser eine nicht unterstützte Ländereinstellung aktiv, verwendet der Web-Client das Zahlenformat für amerikanisches Englisch.

Die Option `numberformat` können Sie in folgenden Befehlen verwenden:

- **delete archive**
- **delete backup**
- **expire**
- **query archive**
- **query backup**
- **query image**
- **query nas**
- **restore**
- **restore image**
- **restore nas**
- **retrieve**
- **set event**

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte **Regionale Einstellungen** im Feld **Zahlenformat** im Profileditor definieren.

Syntax

►—NUMBERformat— —*Nummer*—►

Parameter

Zahl

Zeigt Zahlen in einem der folgenden Formate an. Die Nummer (0–6) für das Zahlenformat angeben, das verwendet werden soll.

0 Das in den länderspezifischen Angaben definierte Datumsformat verwenden. Dies ist der Standardwert (gilt nicht für Mac OS X).

1 1,000.00

Dies ist der Standardwert für die folgenden verfügbaren Übersetzungen:

- Amerikanisches Englisch
- Japanisch
- Traditionelles Chinesisch
- Vereinfachtes Chinesisch
- Koreanisch

2 1,000,00

3 1 000,00

Dies ist der Standardwert für die folgenden verfügbaren Übersetzungen:

- Französisch
- Tschechisch
- Ungarisch
- Polnisch
- Russisch

4 1 000.00

5 1.000,00

Dies ist der Standardwert für die folgenden verfügbaren Übersetzungen:

- Brasilianisches Portugiesisch
- Deutsch
- Italienisch
- Spanisch

6 1'000,00

Für AIX und Solaris: Um Zahlenformate zu definieren, ändern Sie die folgenden Zeilen in der Quellendatei für Ihre Ländereinstellung. Das ausgewählte Format gilt sowohl für die Ausgabe als auch für die Eingabe.

decimal_point

Dezimalzeichen. Das Zeichen, das die ganze Zahl von ihrem Bruchteil trennt.

thousands_sep

Tausendertrennzeichen. Das Zeichen, das die Hunderter, Tausender und Millionen trennt.

grouping

Gruppierung. Die Anzahl Stellen in jeder Gruppe, die durch das Tausendertrennzeichen getrennt werden.

Beispiele

Optionsdatei:

num 4

Befehlszeile:

-numberformat=4

Diese Option ist in der Anfangsbefehlszeile und im interaktiven Modus gültig. Wird die Option im interaktiven Modus eingegeben, ist nur der Befehl betroffen, mit dem sie eingegeben wird. Wenn dieser Befehl beendet ist, wird der Wert auf den Wert zu Beginn der interaktiven Sitzung zurückgesetzt. Dies ist der Wert aus der Datei dsm.opt, sofern er nicht durch die Anfangsbefehlszeile oder eine vom Server erzwungene Option überschrieben wurde.

Optfile

Die Option optfile gibt die Clientoptionsdatei an, die verwendet werden soll, wenn Sie eine Sitzung des Clients für Sichern/Archivieren starten.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Syntax

►►—OPTFILE =— —*Dateiname*—————►►

Parameter

Dateiname

Gibt eine alternative Clientoptionsdatei an, wenn Sie den vollständig qualifizierten Pfadnamen verwenden. Wenn Sie nur den Dateinamen angeben, nimmt der Client an, dass die angegebene Datei sich im aktuellen Arbeitsverzeichnis befindet. Der Standardwert ist dsm.opt.

Einschränkung: Geben Sie den vollständigen Pfad an, wenn Sie diese Option mit dem Clientakzeptordämon (dsmcad) verwenden, da der Clientakzeptordämon sein Arbeitsverzeichnis nach der Initialisierung in das Stammverzeichnis ("/") ändert.

Beispiele

Befehlszeile:

dsmc query session -optfile=myopts.opt

Clientakzeptordämon:

dsmcad -optfile=/usr/tivoli/tsm/client/ba/bin/myopts.opt

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Password

Die Option password gibt ein Kennwort für IBM Spectrum Protect an.

Wenn Sie diese Option nicht angeben und Ihr Administrator die Authentifizierung auf 0n gesetzt hat, werden Sie zur Eingabe eines Kennworts aufgefordert, wenn Sie eine Sitzung des Clients für Sichern/Archivieren starten.

Anmerkung:

1. Wenn der Server die Kennworteingabe anfordert, wird das Kennwort während der Eingabe nicht angezeigt. Wenn Sie die Option password in der Befehlszeile verwenden, wird Ihr Kennwort jedoch bei der Eingabe angezeigt.
2. Wenn sich der Name des IBM Spectrum Protect-Servers ändert oder die Clients für Sichern/Archivieren zu einem anderen Server geleitet werden, müssen alle Clients sich erneut beim Server authentifizieren, da das gespeicherte verschlüsselte Kennwort neu generiert werden muss.

Die Option password wird ignoriert, wenn für die Option passwordaccess der Wert generate definiert wird.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein.

Syntax

►►—PASsword— —Kennwort—►►

Parameter

Kennwort

Gibt das Kennwort an, mit dem Sie sich beim IBM Spectrum Protect-Server anmelden.

Die maximale Kennwortlänge beträgt 63 Zeichen. Die Vorgaben für Kennwörter sind davon abhängig, wo die Kennwörter gespeichert und verwaltet werden und von der Version des Servers, zu dem Ihr Client eine Verbindung herstellt.

Wenn Ihr IBM Spectrum Protect-Server die Version 6.3.3 oder höher aufweist und Sie einen LDAP-Verzeichnisserver zum Authentifizieren von Kennwörtern verwenden

Verwenden Sie die folgenden Zeichen, um ein Kennwort zu erstellen:

```
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 . ! @ # $ % ^ & * _ - + = ` ( )  
| { } [ ] : ; < > , ? / ~
```

Bei den Kennwörtern muss die Groß-/Kleinschreibung beachtet werden. Außerdem können die Kennwörter weiteren Einschränkungen aufgrund von LDAP-Richtlinien unterliegen.

Wenn Ihr IBM Spectrum Protect-Server die Version 6.3.3 oder höher aufweist und Sie keinen LDAP-Verzeichnisserver zum Authentifizieren von Kennwörtern verwenden

Verwenden Sie die folgenden Zeichen, um ein Kennwort zu erstellen:

```
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 werden in der IBM Spectrum Protect-Serverdatenbank gespeichert. Bei diesen Kennwörtern muss die Groß-/Kleinschreibung nicht beachtet werden.

Wenn Ihr IBM Spectrum Protect-Server eine Version vor Version 6.3.3 aufweist Verwenden Sie die folgenden Zeichen, um ein Kennwort zu erstellen:

```
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 werden in der IBM Spectrum Protect-Serverdatenbank gespeichert. Bei diesen Kennwörtern muss die Groß-/Kleinschreibung nicht beachtet werden.

Hinweis:

Schließen Sie in der Befehlszeile alle Parameter, die mindestens ein Sonderzeichen enthalten, in Anführungszeichen ein. Ohne Anführungszeichen können die Sonderzeichen als Shell-Escapezeichen, als Dateiumleitungszeichen oder als andere Zeichen, die eine Bedeutung für das Betriebssystem haben, interpretiert werden.

Auf AIX-, Linux- und Solaris-Systemen:

Schließen Sie die Befehlsparameter in Hochkommas (') ein.

Beispiel für die Befehlszeile:

```
dsmc set password -type=vmguest 'Win 2012 SQL'
'tsql2dag\administrator' '7@#$$^&7'
```

Anführungszeichen sind nicht erforderlich, wenn Sie ein Kennwort mit Sonderzeichen in einer Optionsdatei eingeben.

Beispiele

Optionsdatei:

```
password secretword
```

Befehlszeile:

```
-password=secretword
```

```
-password='my>pas$word'
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Passwordaccess

Mit der Option passwordaccess kann angegeben werden, ob Ihr Kennwort automatisch generiert oder als Benutzereingabeaufforderung definiert werden soll.

Ihr Administrator kann ein Kennwort für Ihren Clientknoten erforderlich machen, indem die Authentifizierungsfunktion aktiviert wird. Fragen Sie Ihren Administrator, ob für Ihren Clientknoten ein Kennwort erforderlich ist.

Wenn ein Kennwort erforderlich ist, können Sie eine der folgenden Methoden auswählen:

- Das Kennwort für den Clientknoten selbst definieren und den Client bei jeder Serviceanforderung zur Eingabe des Kennworts auffordern lassen.
- Den Client automatisch ein neues Kennwort für den Clientknoten generieren lassen, sobald ein Kennwort abläuft, das Kennwort verschlüsseln und in einer Datei speichern und bei einer Serviceanforderung aus dieser Datei abrufen. Sie werden nicht zur Eingabe des Kennworts aufgefordert.
- Ist in der Serverkonfiguration nicht festgelegt, dass ein Kennwort für die Anmeldung erforderlich ist, können Sie dennoch zur Eingabe Ihres Knotenkennworts aufgefordert werden, wenn der Client für Sichern/Archivieren eine Verbindung zu dem Server herstellt. Dieses Verhalten tritt auf, wenn für diese Option, passwordaccess, der Standardwert verwendet wird oder wenn Sie sie auf passwordaccess prompt setzen. Das Kennwort, das Sie bei der Eingabeaufforderung angeben, wird nur zur Verschlüsselung Ihrer Anmeldeinformationen verwendet und nicht für die Anmeldung beim Server. In dieser Konfiguration können Sie die Kennworteingabe vermeiden, indem Sie diese Option auf passwordaccess generate setzen. Die Festlegung von passwordaccess generate bewirkt, dass der Client das Kennwort für Sie erstellt, speichert und übergibt. Ist passwordaccess generate festgelegt, wird die Option password ignoriert.

Das Setzen der Option passwordaccess auf generate ist in folgenden Situationen erforderlich:

- Bei Verwendung des HSM-Clients.
- Bei Verwendung des Web-Clients.
- Bei der Ausführung von NAS-Operationen.
- Bei Verwendung von IBM Spectrum Protect for Workstations.

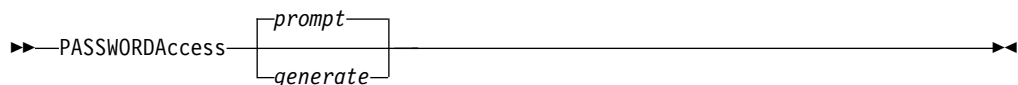
Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Berechtigung** im Abschnitt **Kennwortzugriff** des Profileditors definieren.

Syntax



Parameter

prompt

Sie werden jedes Mal, wenn ein Client eine Verbindung zum Server herstellt, zur Eingabe des Kennworts für Ihren Clientknoten aufgefordert. Dies ist der Standardwert.

Zur Geheimhaltung des Kennworts des Clientknotens sollten Befehle ohne das Kennwort eingegeben und stattdessen auf die Kennworteingabeaufforderung durch den Client gewartet werden.

Jeder Benutzer muss das IBM Spectrum Protect-Kennwort für Ihren Clientknoten kennen. Alle Benutzer, die das Kennwort für Ihren Clientknoten kennen, können auf alle Sicherungen und Archivierungen zugreifen, die auf Ihrem Clientknoten vorgenommen wurden. Wenn der Benutzer beispielsweise den Knotennamen und das Kennwort für Ihren Clientknoten von einem anderen Clientknoten aus eingibt, wird der Benutzer zu einem virtuellen Root.

API-Anwendungen müssen das Kennwort zur Verfügung stellen, wenn eine Sitzung eingeleitet wird. Die Anwendung ist verantwortlich für das Abrufen des Kennworts.

generate

Das Kennwort des Benutzers wird verschlüsselt und lokal gespeichert; wenn das alte Kennwort verfällt, wird ein neues Kennwort generiert. Das neue Kennwort wird vom Client zufällig generiert. Die Vorgaben für Kennwörter sind davon abhängig, wo die Kennwörter gespeichert und verwaltet werden und von der Version des Servers, zu dem Ihr Client eine Verbindung herstellt. Generierte Kennwörter haben eine Länge von 63 Zeichen und enthalten mindestens zwei der folgenden Zeichen:

- Großbuchstaben
- Kleinbuchstaben
- Numerische Zeichen
- Sonderzeichen

Außerdem ist das erste und das letzte Zeichen eines generierten Kennworts ein alphabetisches Zeichen in Groß- oder Kleinschreibung. Generierte Kennwörter enthalten keine wiederholten Zeichen.

Eine Aufforderung zur Kennworteingabe erfolgt bei der offenen Registrierung einer Workstation in einem Server oder wenn Ihr Administrator Ihr Kennwort manuell ändert.

Bei einer lokalen Anmeldung müssen die Benutzer das Kennwort für den Clientknoten nicht kennen. Mit Hilfe der Option `nodename` auf einem fernen Knoten können Benutzer jedoch auf eigene Dateien zugreifen und auf Dateien, für die ihnen ein anderer Benutzer Zugriffsberechtigung erteilt hat.

Beispiele

Optionsdatei:

`passwordaccess generate`

Befehlszeile:

Nicht zutreffend.

Zugehörige Informationen

Informationen darüber, wo das Kennwort gespeichert wird, enthält „`Passworddir`“.

Passworddir

Die Option `passworddir` gibt die Verzeichnisposition an, in der eine verschlüsselte Kennwortdatei gespeichert werden soll.

Das Standardverzeichnis für AIX ist /etc/security/adsm. Für andere UNIX- und Linux-Plattformen ist das Standardverzeichnis /etc/adsm. Das Standardverzeichnis für Mac ist /Library/Preferences/Tivoli Storage Manager. Unabhängig von ihrer Speicherposition wird der vom Client erstellten Kennwortdatei immer der Name TSM.sth zugeordnet. Eine Kennwortdatei wird aus drei Dateien gebildet. In TSM.KDB werden die verschlüsselten Kennwörter gespeichert. In TSM.sth wird der Verschlüsselungszufallsschlüssel gespeichert, mit dem Kennwörter in der Datei TSM.KDB verschlüsselt werden. Diese Datei wird durch das Dateisystem geschützt. TSM.IDX ist eine indexierte Datei zur Protokollierung der Kennwörter in der Datei TSM.KDB.

Unterstützte Clients

Diese Option ist für alle UNIX-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Syntax

►—PASSWORDDIR— —*Verzeichnisname*—►

Parameter

Verzeichnisname

Gibt den Pfad an, in dem die verschlüsselte Kennwortdatei gespeichert werden soll. Die Kennwortdatei hat den Namen TSM.sth. Ist ein Bestandteil des angegebenen Pfads nicht vorhanden, versucht IBM Spectrum Protect, ihn zu erstellen.

Beispiele

Optionsdatei:

```
passworddir "/Users/user1/Library/Preferences/Tivoli Storage Manager/"  
passworddir /etc/security/tsm
```

Befehlszeile:

Nicht zutreffend.

Pick

Die Option pick erstellt eine Liste der Sicherungsversionen oder Archivierungskopien, die mit der von Ihnen eingegebenen Dateispezifikation übereinstimmen.

Aus der Liste können die zu verarbeitenden Versionen ausgewählt werden. Fügen Sie die Option inactive ein, um sowohl aktive als auch inaktive Objekte anzuzeigen.

Werden bei Images kein Quellendateibereich und kein Zieldateibereich angegeben, enthält die Auswahlliste alle gesicherten Images. In diesem Fall werden die aus der Liste ausgewählten Images an ihre ursprüngliche Position zurückgeschrieben. Werden der Quellendateibereich und der Zieldateibereich angegeben, darf nur ein einziger Eintrag aus der Liste ausgewählt werden.

Die Option pick ist in den folgenden Befehlen zu verwenden:

- delete archive
- delete backup
- delete group
- expire
- restore
- restore group
- restore image
- restore nas
- retrieve

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

►—Pick—►

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
dsmc restore "/Users/van/Documents/*" -pick -inactive
```

Befehlszeile:

```
dsmc restore "/home/project/*" -pick -inactive
```

Pitdate

Verwenden Sie die Option `pitdate` mit der Option `pittime`, um einen Zeitpunkt zu definieren, für den die letzte Version Ihrer Sicherungen angezeigt oder zurückgeschrieben werden soll.

Dateien, deren Sicherung *zu oder vor* dem von Ihnen angegebenen Zeitpunkt (Datum und Uhrzeit) erfolgte und die nicht *vor* diesem Zeitpunkt gelöscht wurden, werden verarbeitet. Nach diesem Datum und dieser Uhrzeit erstellte Sicherungsversionen werden ignoriert.

Die Option `pitdate` ist in den folgenden Befehlen zu verwenden:

- delete backup
- query backup
- query group
- query image
- restore
- restore group
- restore image
- restore nas

Wird `pitdate` verwendet, werden die Optionen `inactive` und `latest` implizit verwendet.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

►► `—PITDate = — —Datum—` ◄◄

Parameter

Datum

Gibt das entsprechende Datum an. Das Datum muss in dem mit der Option `dateformat` ausgewählten Format eingegeben werden.

Wenn `dateformat` in einem Befehl angegeben wird, muss diese Option vor den Optionen `fromdate`, `pitdate` und `todate` stehen.

Beispiele

Befehlszeile:

```
dsmc restore "/Volumes/proj4/myproj/*" -sub=y -pitdate=08/01/2003  
-pittime=06:00:00
```

Befehlszeile:

```
dsmc restore "/fs1/*" -sub=y -pitdate=08/01/2003 -pittime=06:00:00
```

Pittime

Verwenden Sie die Option `pittime` mit der Option `pitdate`, um einen Zeitpunkt zu definieren, für den die letzte Version Ihrer Sicherungen angezeigt oder zurückgeschrieben werden soll.

Dateien, deren Sicherung *zu oder vor* dem von Ihnen angegebenen Zeitpunkt (Datum und Uhrzeit) erfolgte und die nicht *vor* diesem Zeitpunkt gelöscht wurden, werden verarbeitet. Nach diesem Datum und dieser Uhrzeit erstellte Sicherungsversionen werden ignoriert. Diese Option wird ignoriert, wenn Sie die Option `pitdate` nicht angeben.

Die Option `pittime` ist in den folgenden Befehlen zu verwenden:

- **delete backup**
- **query backup**
- **query image**
- **restore**
- **restore image**
- **restore nas**

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

►—PITTime =— —Zeit—►

Parameter

Zeit

Gibt eine Uhrzeit an einem bestimmten Datum an. Wenn keine Zeit angegeben wird, lautet der Standardwert 23:59:59. Die Zeit muss in dem mit der Option `timeformat` ausgewählten Format angegeben werden.

Wenn die Option `timeformat` in einem Befehl angegeben wird, muss sie vor den Optionen `fromtime`, `pittime` und `totttime` stehen.

Beispiele

Befehlszeile:

```
dsmc query backup -pitt=06:00:00 -pitt=08/01/2003  
"/Volumes/proj5/myproj/*"
```

Befehlszeile:

```
dsmc q b "/fs1/*" -pitt=06:00:00 -pitt=08/01/2003
```

Postschedulecmd/Postnschedulecmd

Die Option `postschedulecmd/postnschedulecmd` gibt einen Befehl an, den das Clientprogramm verarbeitet, nachdem ein Zeitplan ausgeführt wurde.

Wenn das Clientprogramm auf die Beendigung des Befehls warten soll, bevor es andere Verarbeitungsschritte fortsetzt, verwenden Sie die Option `postschedulecmd`. Wenn nicht auf die Beendigung des Befehls gewartet werden soll, bevor der Client andere Verarbeitungsschritte fortsetzt, geben Sie die Option `postnschedulecmd` an.

Die Handhabung von Rückkehrcodes und das Verhalten bei geplanten Aktionen ist einerseits von der angegebenen Option und andererseits vom Typ der geplanten Operation abhängig:

- Geplante Operationen, bei denen die geplante Aktion nicht `COMMAND` ist:
Wenn der Befehl `postschedulecmd` nicht mit dem Rückkehrcode 0 (null) beendet wird, ist der Rückkehrcode für das geplante Ereignis entweder 8 oder der Rückkehrcode der geplanten Operation (der höhere der beiden Codes). Wenn Sie nicht wollen, dass diese Regel auf den Befehl `postschedulecmd` angewendet wird, können Sie eine Script- oder Stapeldatei erstellen, die den Befehl aufruft und mit dem Rückkehrcode 0 beendet wird. Dann müssen Sie `postschedulecmd` so konfigurieren, dass die Script- oder Stapeldatei gestartet wird.
- Geplante Operationen, bei denen die geplante Aktion `COMMAND` ist:
Der Rückkehrcode des mit der Option `postschedulecmd` angegebenen Befehls hat keinen Einfluss auf den Rückkehrcode, der dem Server nach Beendigung des geplanten Ereignisses gemeldet wird. Wenn die Ergebnisse der `postschedulecmd`-Operationen Einfluss auf den Rückkehrcode des geplanten Ereignisses nehmen sollen, fügen Sie die `postschedulecmd`-Operationen in das Befehlsscript der geplanten Aktion ein und verwenden Sie nicht die Option `postschedulecmd`.
- Wenn die Scheduleraktion nicht gestartet werden kann und der mit der Option `preschedulecmd` angegebene Befehl mit dem Rückkehrcode 0 (null) beendet wird, wird der mit der Option `postschedulecmd` angegebene Befehl ausgeführt.

- ## Unterstützte Clients

Optionsdatei

Syntax



```
postschedulecmd osascript "/Volumes/La Pomme/Scripting/
Database Script"
```

Beispiele

```
postschedulecmd "restart database"
```


Die Befehlszeichenfolge ist ein gültiger Befehl zum Neustart der Datenbank.

Befehlszeile:

```
-postschedulecmd="/Volumes/La Pomme/Scripting/postsched.sh"
```

Befehlszeile:

```
-postschedulecmd="'restart database'"
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Zugehörige Konzepte:

Kapitel 8, „Clientrückkehrcodes“, auf Seite 307

Zugehörige Verweise:

 Befehl DEFINE SCHEDULE

Postsnapshotcmd

Mit der Option `postsnapshotcmd` können Sie Shellbefehle oder Scripts des Betriebssystems ausführen, nachdem der Client für Sichern/Archivieren während einer Sicherungsoperation auf Momentaufnahmebasis eine Momentaufnahme gestartet hat.

Nur für AIX: Diese Option ist nur für JFS2-Dateisicherung oder -archivierung auf Momentaufnahmebasis und für Imagesicherung auf Momentaufnahmebasis gültig. Verwenden Sie diese Option bei Dateisicherungen oder -archivierungen auf Momentaufnahmebasis im Befehl **backup**, mit der Option `include.fs` oder in der Datei `dsm.sys`.

Nur für Linux: Diese Option ist nur gültig, wenn der LVM auf Ihrem System installiert und so konfiguriert ist, dass Sie eine Imagesicherungsoperation auf Momentaufnahmebasis ausführen können.

Nur für AIX und Linux: Verwenden Sie diese Option für eine Imagesicherung auf Momentaufnahmebasis im Befehl **backup image**, mit der Option `include.image` oder in der Datei `dsm.sys`.

Wenn `postsnapshotcmd` fehlschlägt, wird die Operation fortgesetzt. Es werden jedoch entsprechende Warnungen protokolliert.

Unterstützte Clients

Diese Option ist nur für AIX-Clients und Linux x86_64-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientssystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auch auf der Registerkarte **Momentaufnahmeimage** des Profileeditors definieren.

Syntax

►►—POSTSNAPshotcmd— —"*Befehlszeichenfolge*"——►►

Parameter

"Befehlszeichenfolge"

Gibt einen Befehl an, der verarbeitet werden soll.

Verwenden Sie die Option `srvprepostsnapdisabled`, um zu verhindern, dass der IBM Spectrum Protect-Serveradministrator Betriebssystembefehle auf dem Clientsystem ausführt.

Wenn die Befehlszeichenfolge Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden:

```
"resume database myDb"
```

Haben Sie innerhalb der Befehlszeichenfolge Anführungszeichen verwendet, müssen Sie die gesamte Befehlszeichenfolge in Hochkommas einschließen:

```
'resume database "myDb"'
```

Beispiele

Optionsdatei:

```
postsnapshotcmd "beliebiger Befehl"
```

Die Befehlszeichenfolge ist ein gültiger Befehl zum Neustart der Anwendung.

Befehlszeile:

```
backup image -postsnapshotcmd="beliebiger Befehl"
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Zugehörige Informationen

„Include-Optionen“ auf Seite 473

„Srvprepostscheddisabled“ auf Seite 596

Preschedulecmd/Prenschedulecmd

Mit der Option `preschedulecmd` wird ein Befehl angegeben, den das Clientprogramm vor der Ausführung eines Zeitplans verarbeitet.

Das Clientprogramm wartet auf die Beendigung des Befehls, bevor der Zeitplan gestartet wird. Soll nicht gewartet werden, muss `prenschedulecmd` angegeben werden.

Anmerkung:

1. Die erfolgreiche Beendigung des Befehls `preschedulecmd` wird als Voraussetzung für das Ausführen der geplanten Operation angesehen. Wenn der Befehl `preschedulecmd` nicht mit dem Rückkehrcode 0 beendet wird, werden die geplante Operation und die Befehle `postschedulecmd` und `postschedulecmd` nicht ausgeführt. Der Client meldet, dass das geplante Ereignis fehlgeschlagen ist und der Rückkehrcode 12 lautet. Wenn Sie nicht wollen, dass der Befehl `preschedulecmd` von dieser Regel gesteuert wird, können Sie eine Script- oder Stapeldatei erstellen, die den Befehl aufruft und mit dem Rückkehrcode 0 beendet wird. Dann müssen Sie `preschedulecmd` so konfigurieren, dass die Script- oder Stapeldatei aufgerufen wird. Der Rückkehrcode für den Befehl `prenschedulecmd` wird nicht protokolliert und hat keinen Einfluss auf den Rückkehrcode des geplanten Ereignisses.

2. Die Option `preschedulecmd` kann (wie die Option `prenschedulecmd`) auch auf dem Server definiert werden.

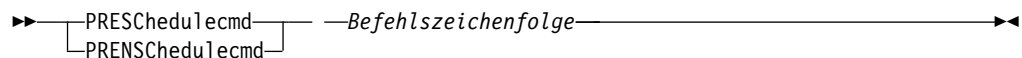
Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Scheduler** im Dialogfeld **Befehl für Zeitplan** im Profileditor definieren.

Syntax



Parameter

Befehlszeichenfolge

Gibt den zu verarbeitenden Befehl an. Nur eine Option `preschedulecmd` verwenden. Mit dieser Option kann ein Befehl eingegeben werden, der vor einem Zeitplan ausgeführt werden soll.

Wenn die Befehlszeichenfolge Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden. Haben Sie innerhalb der Befehlszeichenfolge Anführungszeichen verwendet, müssen Sie die gesamte Befehlszeichenfolge in Hochkommas einschließen.

Geben Sie eine Leer- oder Nullzeichenfolge für *Befehlszeichenfolge* an, wenn die Ausführung aller Befehle verhindert werden soll, die der IBM Spectrum Protect-Serveradministrator für `postschedulecmd` und `preschedulecmd` verwendet. Wird eine Leer- oder Nullzeichenfolge in einer der beiden Optionen angegeben, kann der Administrator in beiden Optionen keinen Befehl verwenden.

Gibt der Administrator eine Leer- oder Nullzeichenfolge in der Option `preschedulecmd` an, kann der Benutzer keinen Befehl vor einem Zeitplan ausführen.

Für Mac OS X: Wenn der Zeitplanbefehl `preschedulecmd` ein AppleScript ist, müssen Sie den Befehl **osascript** zum Ausführen des Scripts verwenden. Beispiel: Ist „Database Script“ ein AppleScript, geben Sie den folgenden Befehl ein:

```
preschedulecmd osascript "/Volumes/La Pomme/Scripting/
Database Script"
```

Beispiele

Optionsdatei:

```
preschedulecmd "<Befehl zum Versetzen Ihres Datenbankprodukts in den Wartemodus>
Datenbank"
```

Die Befehlszeichenfolge ist ein gültiger Befehl zum Versetzen der Datenbank in den Wartemodus.

Befehlszeile:

```
-preschedulecmd="'quiesce database'"
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Zugehörige Konzepte:

Kapitel 8, „Clientrückkehrcodes“, auf Seite 307

PreserveLastAccessDate

Mit der Option `preserveLastAccessDate` können Sie angeben, ob eine Sicherungs- oder Archivierungsoperation die letzte Zugriffszeit ändert.

Eine Sicherungs- oder Archivierungsoperation kann die letzte Zugriffszeit einer Datei ändern. Nach einer Operation kann der Client für Sichern/Archivieren die letzte Zugriffszeit auf den Wert vor der Operation zurücksetzen. Die letzte Zugriffszeit wird vom Client für Sichern/Archivieren nicht geändert, sondern kann beibehalten werden. Das Zurücksetzen der letzten Zugriffszeit erfordert zusätzliche Verarbeitung für jede gesicherte oder archivierte Datei.

Wenn Sie die Unterstützung offener Dateien aktivieren, wird das Datum des letzten Zugriffs auf Dateien immer beibehalten, unabhängig von der Einstellung für `preserveLastAccessDate`. Wenn die Unterstützung offener Dateien aktiviert ist, verwenden Sie die Option `preserveLastAccessDate` nicht.

Verwenden Sie diese Option in den Befehlen **incremental**, **selective** oder **archive**.

Anmerkung:

1. Diese Option gilt nur für Dateien, nicht für Verzeichnisse.
2. Das Zurücksetzen des Datums des letzten Zugriffs wirkt sich auf die Sicherungs- und Archivierungsleistung aus.
3. Das Zurücksetzen des Datums des letzten Zugriffs kann sich auf Anwendungen auswirken, die sich auf ein präzises Datum des letzten Zugriffs stützen, z. B. eine SRM-Anwendung (SRM = Storage Resource Management).
4. Auf Dateisystemen, die nicht vom IBM Spectrum Protect for Space Management-Client verwaltet werden, oder wenn Benutzer ohne Rootberechtigung sichern oder archivieren, wird das Attribut `ctime` zurückgesetzt. Das Attribut für die Uhrzeit und das Datum der letzten Änderung (`ctime`) wird auf das Datum und die Uhrzeit der Sicherungs- oder Archivierungsoperation zurückgesetzt.
5. Die Option `updateTime` hat Vorrang vor der Option `preserveLastAccessDate`. Wenn beide Optionen auf `yes` gesetzt sind, wird die Option `preserveLastAccessDate` ignoriert.
6. Verwenden Sie auf Dateisystemen, die nicht vom IBM Spectrum Protect for Space Management-Client verwaltet werden, nicht `preserveLastAccessDate yes` und den GPFS-Befehl `mmbackup`. Mit dem Befehl **mmbackup** und mit `preserveLastAccessDate yes` werden alle Dateien für jede Sicherungsoperation ausgewählt.
7. Sie können das Datum des letzten Zugriffs von schreibgeschützten Dateien nicht zurücksetzen. Die Option `preserveLastAccessDate` ignoriert schreibgeschützte Dateien und ändert deren Datum nicht.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte 'Sichern' des Profileditors definieren.

Syntax



Parameter

No Eine Sicherungs- oder Archivierungsoperation kann das Datum des letzten Zugriffs ändern. Dies ist der Standardwert.

Yes

Eine Sicherungs- oder Archivierungsoperation ändert das Datum des letzten Zugriffs nicht.

Beispiele

Optionsdatei:

```
preservelastaccessdate yes
```

Befehlszeile:

```
Incremental /proj/test/test_file -preservelastaccessdate=yes
```

Zugehörige Informationen:

- ➡ Befehl 'mmbackup': IBM Spectrum Protect-Voraussetzungen
- ➡ Anleitung für die Integration von IBM Spectrum Scale AFM mit IBM Spectrum Protect
- ➡ Hinweise zur Verwendung der Einschluss- und Ausschlussoptionen von IBM Spectrum Protect in Verbindung mit dem IBM Spectrum Scale-Befehl 'mmbackup'

Preservepath

Mit der Option `preservepath` wird angegeben, wie viel vom Quellenpfad als Teil des Zielverzeichnispfades wiederherzustellen ist, wenn Dateien an einen neuen Standort zurückgeschrieben oder abgerufen werden.

Verwenden Sie die Option `-subdir=yes`, um die vollständige Unterverzeichnisstruktur des Quellenverzeichnisses (Verzeichnisse und Dateien unter dem Quellenverzeichnis der untersten Ebene) als zurückzuschreibende Quelle festzulegen. Ist ein erforderliches Zielverzeichnis nicht vorhanden, wird es erstellt. Hat eine Zieldatei denselben Namen wie eine Quelldatei, wird sie überschrieben. Verwenden Sie die Option `-replace=prompt`, damit der Client eine Bestätigung anfordert, bevor Dateien überschrieben werden.

Verwenden Sie die Option `preservepath` in den folgenden Befehlen:

- **restore**
- **restore backupset**
- **restore group**
- **retrieve**

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Syntax



Parameter

Subtree

Das Quellenverzeichnis der untersten Ebene wird als ein Unterverzeichnis des Zielverzeichnisses erstellt. Dateien aus dem Quellenverzeichnis werden in dem neuen Unterverzeichnis gespeichert. Dies ist der Standardwert.

Complete

Der gesamte Pfad wird ab dem Stammverzeichnis in das angegebene Verzeichnis zurückgeschrieben. Der vollständige Pfad umfasst alle Verzeichnisse mit Ausnahme des Dateibereichsnamens.

NOBase

Der Inhalt des Quellenverzeichnisses wird ohne das Verzeichnis der untersten Ebene (Basisverzeichnis) in das angegebene Zielverzeichnis zurückgeschrieben.

NONE

Alle ausgewählten Quellendateien werden in das Zielverzeichnis zurückgeschrieben. Im Ziel werden keine Teile des Quellenpfades im oder oberhalb des Quellenverzeichnisses wiederhergestellt.

Wenn Sie SUBDIR=yes angeben, schreibt der Client alle Dateien in den Quellenverzeichnissen in das einzelne Zielverzeichnis zurück.

Beispiele

Befehlszeile:

Voraussetzung ist, dass der Serverdateibereich folgende Sicherungskopien enthält:

```
/fs/h1/m1/file.a  
/fs/h1/m1/file.b  
/fs/h1/m1/l1/file.x  
/fs/h1/m1/l1/file.y
```

Dieser Befehl:

```
dsmc res /fs/h1/m1/ /u/ann/ -preser=complete
```

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
/u/ann/h1/m1/file.a  
/u/ann/h1/m1/file.b
```

Dieser Befehl:

```
dsmc res /fs/h1/m1/ /u/ann/ -preser=nobase
```

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
/u/ann/file.a  
/u/ann/file.b
```

Dieser Befehl:

```
dsmc res backupset /fs/h1/m1/ /u/ann/ -su=yes  
-preser=nobase -loc=file
```

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
/u/ann/file.a  
/u/ann/file.b  
/u/ann/file.x  
/u/ann/file.y
```

Dieser Befehl:

```
dsmc res /fs/h1/m1/ /u/ann/ -preser=subtree
```

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
/u/ann/m1/file.a  
/u/ann/m1/file.b
```

Dieser Befehl:

```
dsmc res /fs/h1/m1/ /u/ann/ -preser=none
```

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
/u/ann/file.a  
/u/ann/file.b
```

Dieser Befehl:

```
dsmc res /fs/h1/m1/ /u/ann/ -su=yes -preser=complete
```

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
/u/ann/h1/m1/file.a  
/u/ann/h1/m1/file.b  
/u/ann/h1/m1/l1/file.x  
/u/ann/h1/m1/l1/file.y
```

Dieser Befehl:

```
dsmc res /fs/h1/m1/ /u/ann/ -su=yes -preser=nobase
```

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
/u/ann/file.a  
/u/ann/file.b  
/u/ann/l1/file.x  
/u/ann/l1/file.y
```

Dieser Befehl:

```
dsmc res /fs/h1/m1/ /u/ann/ -su=yes -preser=subtree
```

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
/u/ann/m1/file.a  
/u/ann/m1/file.b  
/u/ann/m1/l1/file.x  
/u/ann/m1/l1/file.y
```

Dieser Befehl:

```
dsmc res /fs/h1/m1/ /u/ann/ -su=yes -preser=none
```

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
/u/ann/file.a  
/u/ann/file.b  
/u/ann/file.x  
/u/ann/file.y
```

Presnapshotcmd

Mit der Option `presnapshotcmd` können Sie Betriebssystembefehle ausführen, bevor der Client für Sichern/Archivieren eine Momentaufnahme startet.

Dadurch sind Sie in der Lage, eine Anwendung in den Wartemodus zu versetzen, bevor der Client während einer Sicherung oder Archivierung auf Momentaufnahmebasis die Momentaufnahme startet.

Nur für AIX: Diese Option ist nur für JFS2-Dateisicherung oder -archivierung auf Momentaufnahmebasis und für Imagesicherung auf Momentaufnahmebasis gültig. Verwenden Sie diese Option bei Dateisicherungen oder -archivierungen auf Momentaufnahmebasis im Befehl **backup**, mit der Option `include.fs` oder in der Datei `dsm.sys`.

Nur für Linux: Diese Option ist nur gültig, wenn der LVM auf Ihrem System installiert und so konfiguriert ist, dass Sie eine Imagesicherung auf Momentaufnahmebasis ausführen können.

Nur für AIX und Linux: Verwenden Sie diese Option für eine Imagesicherung auf Momentaufnahmebasis im Befehl **backup image**, mit der Option `include.image` oder in der Datei `dsm.sys`.

Wenn `presnapshotcmd` fehlschlägt, wird angenommen, dass die Anwendung nicht in einem konsistenten Status ist, und der Client stoppt die Verarbeitung und zeigt die entsprechende Fehlernachricht an.

Unterstützte Clients

Diese Option ist nur für AIX JFS2- und Linux x86_64-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auch auf der Registerkarte **Momentaufnahmeimage** des Profileditors definieren.

Syntax

►►—PRESNAPSHOTcmd— —"*Befehlszeichenfolge*"——►►

Parameter

"Befehlszeichenfolge"

Gibt einen Befehl an, der verarbeitet werden soll.

Verwenden Sie die Option `srvprepostsnapdisabled`, um zu verhindern, dass der IBM Spectrum Protect-Serveradministrator Betriebssystembefehle auf dem Clientsystem ausführt.

Wenn die Befehlszeichenfolge Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden:

```
"quiesce database myDb"
```

Haben Sie innerhalb der Befehlszeichenfolge Anführungszeichen verwendet, müssen Sie die gesamte Befehlszeichenfolge in Hochkommas einschließen:

```
'resume database "myDb"'
```

Beispiele

Optionsdatei:

```
presnapshotcmd "beliebiger Shellbefehl oder beliebiges Script"
```

Befehlszeile:

```
backup image -presnapshotcmd="beliebiger Shellbefehl oder beliebiges Script"
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Zugehörige Informationen

„Include-Optionen“ auf Seite 473

„Srvprepostscheddisabled“ auf Seite 596

Queryschedperiod

Mit der Option `queryschedperiod` kann die Anzahl Stunden festgelegt werden, die der Client-Scheduler zwischen den Versuchen, den Server nach geplanter Arbeit abzufragen, warten soll.

Diese Option ist nur gültig, wenn Sie die Option `schedmode` auf `polling` setzen. Diese Option wird nur verwendet, wenn der Scheduler aktiv ist.

Ihr Administrator kann diese Option auch definieren. Gibt Ihr Administrator einen Wert für diese Option an, überschreibt dieser den in Ihrer Clientoptionsdatei definierten Wert, nachdem Ihr Clientknoten erfolgreich den Kontakt zum Server hergestellt hat.

Tip: Wenn der durch die Option `queryschedperiod` festgelegte Zeitraum viel kleiner als das Randomisierungsfenster eines Zeitplans ist, das der Serveradministrator definiert, kann der Start eines Zeitplans verzögert werden. Passen Sie die folgenden Werte an, um eine solche Verzögerung zu vermeiden:

- Dauer von Clientaktionen (mit dem Serverbefehl `SET CLIENTACTDURATION`)
- Randomisierung von geplanten Startzeiten (mit dem Serverbefehl `SET RANDOMIZE`)
- Wert der Option `queryschedperiod`

Die folgenden Beispiele zeigen, wie das Intervall für Zeitplanabfragen berechnet wird, wenn die Einstellungen für die Dauer von Clientaktionen und das Randomisierungsfenster eines Zeitplans gegeben sind.

Beispiel 1:

Dauer von Clientaktionen: 1 Tag
 Zeitplanzufallsgenerierung (Prozent): 25 %
 Intervall für Zeitplanabfragen: 6 Stunden

Dauer von Clientaktionen ist 1 Tag = 24 Stunden
 $24 \text{ Stunden} \times 0,25 = 6 \text{ Stunden}$
 Verwenden Sie ein Intervall für Zeitplanabfragen von 6 Stunden oder höher.

Beispiel 2:

Dauer von Clientaktionen: 3 Tage
 Zeitplanzufallsgenerierung (Prozent): 10 %
 Intervall für Zeitplanabfragen: 8 Stunden

Dauer von Clientaktionen ist 3 Tage = 72 Stunden
 $72 \times 0,10 = 7,2$
 Verwenden Sie ein Intervall für Zeitplanabfragen von 8 Stunden oder höher.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Syntax

►—**QUERYSChedperiod**— *Stunden*—◄

Parameter

Stunden

Gibt die Anzahl Stunden an, die der Client-Scheduler zwischen den Versuchen, geplante Arbeit auf dem Server abzufragen, wartet. Der Wertebereich ist 1 - 9999; der Standardwert ist 4.

Beispiel

Optionsdatei:
 querysch 6

Querysummary

Die Option querysummary stellt Statistikdaten zu Dateien, Verzeichnissen und Objekten bereit, die von den Befehlen **query backup** oder **query archive** zurückgegeben werden.

Die Option querysummary stellt die folgenden Statistikdaten bereit:

- Die Gesamtanzahl der Dateien und Verzeichnisse, die vom Befehl query backup oder query archive zurückgegeben werden.
- Das gesamte Datenvolumen der Objekte, die vom Befehl query backup oder query archive zurückgegeben werden.
- Den Schätzwert für den erforderlichen Speicher, wenn die vom Befehl query backup oder query archive zurückgegebenen Objekte mit einer klassischen Zurschreibung zurückgeschrieben werden.

- Die Gesamtanzahl der eindeutigen Serverdatenträger, auf denen die Objekte gespeichert sind, die vom Befehl query zurückgegeben werden.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

►►—QUERYSUMMARY—◄◄

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
dsmc q ba '/usr/fs1/*' -sub=yes -querysummary
[root@kaveri:/home/cpark] $ dsmc q ba '/kalafs1/*' -sub=yes -querysummary
IBM Spectrum Protect
Befehlszeilenschnittstelle des Clients für Sichern/Archivieren
Clientversion 8, Release 1, Stufe 0.0
Clientdatum/-zeit: 09.12.2016 12:05:35
(c) Copyright IBM Corporation und andere 1990, 2016. Alle Rechte vorbehalten.
```

```
Knotenname: KAVERI
Sitzung hergestellt mit Server TEMPLAR: AIX-RS/6000
Serverversion 8, Release 1, Stufe 0.0
Serverdatum/-zeit: 09.12.2016 12:05:35 Letzter Zugriff: 07.12.2016 07:48:59
```

Größe		Sicher.-Datum		Verw.-Kl.		A/I	Datei
----		-----		-----		----	
4,096	B	08/07/08	12:07:30	BASVT2	A		/kalafs1/
256	B	08/07/08	12:07:30	BASVT2	A		/kalafs1/dir1
10,485,760	B	08/07/08	12:07:30	DEFAULT	A		/kalafs1/info1
5,242,880	B	08/07/08	12:07:30	DEFAULT	A		/kalafs1/info2
1,044	B	08/07/08	12:07:30	DEFAULT	A		/kalafs1/dir1/subfile1
1,044	B	08/07/08	12:07:30	DEFAULT	A		/kalafs1/dir1/subfile2

Übersichtsstatistik

Anz. Dat.	Anz. Verz.	Dsn. Dat.-Größe	Gesamtdaten	Gesch. Sp.
-----	-----	-----	-----	-----
4	2	3.75 MB	15.00 MB	1.07 KB

Geschätzte Anzahl Datenträger: 2

```
[root@kaveri:/home/cpark] $
```

Quiet

Mit der Option quiet wird die Anzahl der Nachrichten, die während der Verarbeitung auf dem Bildschirm angezeigt werden, begrenzt.

Bei der Ausführung der Befehle **incremental**, **selective** oder **archive** können beispielsweise Informationen zu allen Dateien, die gesichert werden, angezeigt werden. Verwenden Sie die Option **quiet**, wenn diese Informationen nicht angezeigt werden sollen.

Wenn die Option **quiet** verwendet wird, werden Fehler- und Verarbeitungsdaten weiterhin angezeigt, und die Nachrichten werden in Protokolldateien geschrieben. Wird **quiet** nicht angegeben, wird die Standardoption **verbose** verwendet.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die Option **quiet** kann auch auf dem Server definiert werden; sie überschreibt dann die Clienteneinstellung. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (**dsm.opt**) ein. Sie können diese Option auf der Registerkarte **Befehlszeile** über das Kontrollkästchen **Keine Verarbeitungsdaten auf dem Bildschirm anzeigen** im Profileditor definieren.

Syntax

►►—QUIET—◄◄

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Optionsdatei:

`quiet`

Befehlszeile:

`-quiet`

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Quotesareliteral

Die Option **quotesareliteral** gibt an, ob einfache Anführungszeichen (') oder doppelte Anführungszeichen (") buchstäblich interpretiert werden, wenn sie in einer Dateilistenspezifikation in einer Option **filelist** angegeben werden.

Normalerweise müssen Sie im Client Dateispezifikationen, die Leerzeichen enthalten, mit einfachen oder doppelten Anführungszeichen begrenzen. In einigen Dateisystemen sind Hochkommas oder Anführungszeichen in Datei- und Verzeichnisnamen zulässig.

Um Fehler zu verhindern, die auftreten, wenn in einer Option **filelist** Dateispezifikationen angegeben werden, die einfache Anführungszeichen (') oder doppelte Anführungszeichen (") enthalten, definieren Sie **quotesareliteral yes**. Wenn **quotesareliteral** auf **yes** gesetzt ist, werden Anführungszeichen, die in einer Da-

teilstenspezifikation in einer Option `filelist` enthalten sind, buchstäblich als Anführungszeichen und nicht als Begrenzungszeichen interpretiert.

Diese Option ist für jeden Befehl gültig, der eine Option `filelist` als Befehlsparameter akzeptiert.

Unterstützte Clients

Diese Option ist für alle unterstützten Plattformen gültig. Die Option wird auf jeden Befehl angewendet, der eine Dateilistenspezifikation als Parameter akzeptiert.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (`dsm.opt`) ein.

Syntax



Parameter

no Gibt an, dass einfache Anführungszeichen (') und doppelte Anführungszeichen (") als Begrenzungszeichen für Dateilistenspezifikationen in einer Option `filelist` interpretiert werden. No ist die Standardeinstellung.

yes

Gibt an, dass einfache Anführungszeichen (') und doppelte Anführungszeichen (") buchstäblich und nicht als Begrenzungszeichen für Dateilistenspezifikationen in einer Option `filelist` interpretiert werden. Geben Sie diesen Wert an, wenn Sie Dateien aus einem Dateisystem sichern, in dem Anführungszeichen in Datei- oder Verzeichnisnamen zulässig sind.

Beispiele

Optionsdatei:

```
QUOTESARELITERAL YES
```

Befehlszeile:

Bei den folgenden Beispielen wird vorausgesetzt, dass das Dateisystem Hochkommas und Anführungszeichen in Pfadangaben zulässt. Die Beispiele zeigen Dateien in einer Dateilistenspezifikation, die erfolgreich verarbeitet werden können, wenn `QUOTESARELITERAL` auf `YES` gesetzt wird.

Der ausgegebene Befehl ist `dsmc sel -filelist=/home/user1/important_files`, wobei `important_files` die Liste der zu verarbeitenden Dateien enthält.

```
/home/user1/myfiles/"file"1000  
/home/user1/myfiles/'file'  
/home/user1/myfiles/file'ABC  
/home/user1/myfiles/ABC"file"
```

Zugehörige Informationen

Informationen zur Option `filelist` finden Sie in „Filelist“ auf Seite 453.

Informationen zur Syntax für Dateispezifikationen finden Sie in „Eingabezeichenfolgen angeben, die Leerzeichen oder Hochkommas oder Anführungszeichen enthalten“ auf Seite 156.

„Wildcardsareliteral“ auf Seite 681

Removeoperandlimit

Die Option `removeoperandlimit` gibt an, dass der Client die Beschränkung auf 20 Operanden entfernt.

Wenn Sie die Option `removeoperandlimit` mit dem Befehl **incremental**, **selective**, **archive** oder **backup image** angeben, wird die Beschränkung auf 20 Operanden nicht umgesetzt und nur durch die verfügbaren Ressourcen oder andere Begrenzungen des Betriebssystems eingeschränkt.

Die Option `removeoperandlimit` kann nützlich sein, wenn Sie Scripts generieren, die den Befehlszeilenclient unter Umständen mit einer großen Anzahl Operanden aufrufen. So können Sie beispielsweise auf der Suche nach zu sichernden Dateien eine Verzeichnisbaumstruktur durchsuchen. Jede *in Frage kommende* Datei, die erkannt wird, wird zur Operandenliste des Befehls **selective** hinzugefügt. Später wird dieser Befehl **selective** von einem Steuerungsscript übergeben. In diesem Fall wird durch Angabe der Option `removeoperandlimit` die Beschränkung auf 20 Operanden entfernt.

Anmerkung:

1. Die Option `removeoperandlimit` *muss* unmittelbar nach den Befehlen **incremental**, **selective**, **archive** oder **backup image** vor allen Dateispezifikationen angegeben werden.
2. Diese Option akzeptiert keinen Wert. Wird diese Option in einem Befehl angegeben, wird die Beschränkung auf 20 Operanden entfernt.
3. Da die Erlaubnis der Shell zum Erweitern von Platzhalterzeichen die Leistung nachteilig beeinflusst, sollten Sie die Option `removeoperandlimit` in Sicherungs- oder Archivierungsoperationen einsetzen, in denen keine Platzhalterzeichen verwendet werden.
4. Die Option `removeoperandlimit` ist nur in den Befehlen **incremental**, **selective**, **archive** und **backup image** im Stapelbetrieb gültig. In der Clientoptionsdatei (`dsm.opt`) oder Datei `dsm.sys` ist sie nicht gültig.

Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients gültig.

Syntax

►►—`REMOVEOPerandlimit`—◄◄

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

`-removeoperandlimit`

Replace

Die Option `replace` gibt an, ob vorhandene Dateien auf Ihrer Workstation überschrieben werden sollen oder ob Sie zur Eingabe Ihrer Auswahl aufgefordert werden sollen, wenn Sie Dateien zurückschreiben oder abrufen.

Wichtig: Die Option `replace` hat keinen Einfluss auf die Wiederherstellung von Verzeichnisobjekten. Verzeichnisobjekte werden immer wiederhergestellt, auch bei Angabe von `replace=no`. Sollen vorhandene Verzeichnisse nicht überschrieben werden, müssen Sie die Option `filesonly` verwenden.

Diese Option können Sie in folgenden Befehlen verwenden:

- **restore**
- **restore backupset**
- **restore group**
- **retrieve**

Anmerkung: Bei geplanten Operationen erfolgt keine Eingabeaufforderung für das Überschreiben. Wenn Sie die Option `replace` auf `prompt` setzen, überspringt der Client für Sichern/Archivieren bei einer geplanten Operation Dateien ohne Eingabeaufforderung.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (`dsm.opt`) ein. Sie können diese Option auf der Registerkarte **Restore** im Abschnitt **Aktion für bereits vorhandene Dateien** im Profileditor definieren.

Syntax



Parameter

Prompt

Bei nicht geplanten Operationen geben Sie an, ob vorhandene Dateien überschrieben werden sollen. Bei geplanten Operationen werden vorhandene Dateien nicht überschrieben und keine Bedienerführungen angezeigt. Dies ist der Standardwert.

All

Alle vorhandenen Dateien werden überschrieben, auch schreibgeschützte Dateien. Wird der Zugriff auf eine Datei verweigert, hat der Benutzer die Auswahl, die Datei zu überspringen oder zu überschreiben. Die Datei wird erst bearbeitet, wenn die Bedienerführung beantwortet wurde.

Yes

Mit Ausnahme von schreibgeschützten Dateien werden alle vorhandenen Datei-

en überschrieben. Bei nicht geplanten Operationen geben Sie an, ob vorhandene schreibgeschützte Dateien überschrieben werden sollen. Bei geplanten Operationen werden vorhandene schreibgeschützte Dateien nicht überschrieben und keine Bedienerführungen angezeigt. Wird der Zugriff auf eine Datei verweigert, wird sie übersprungen.

No Vorhandene Dateien werden nicht überschrieben. Eingabeaufforderungen werden nicht angezeigt.

Beispiele

Optionsdatei:

replace all

Befehlszeile:

-replace=no

Diese Option ist in der Anfangsbefehlszeile und im interaktiven Modus gültig. Wird die Option im interaktiven Modus eingegeben, ist nur der Befehl betroffen, mit dem sie eingegeben wird. Wenn dieser Befehl beendet ist, wird der Wert auf den Wert zu Beginn der interaktiven Sitzung zurückgesetzt. Dies ist der Wert aus der Datei dsm.opt, sofern er nicht durch die Anfangsbefehlszeile oder eine vom Server erzwungene Option überschrieben wurde.

Replserverguid

Die Option replserverguid gibt die global eindeutige ID (GUID) an, die verwendet wird, wenn der Client während der Übernahme eine Verbindung zum Sekundärserver herstellt. Mit der GUID wird der Sekundärserver validiert, um sicherzustellen, dass es sich um den erwarteten Server handelt.

Die Replikations-GUID weicht von der Maschinen-GUID des Servers ab. Sie wird einmal für einen Server generiert, der die Replikation ausführt, und ändert sich nie.

Diese Option muss in einer Zeilengruppe **replservername** in der Clientoptionsdatei angegeben werden. Die Zeilengruppe **replservername** enthält Verbindungsdaten des Sekundärservers.

Diese Option wird vom Administrator des IBM Spectrum Protect-Servers für den Clientknoten definiert. Während des normalen Anmeldeprozesses (ohne Übernahme) wird die Option an den Client gesendet und in der Clientoptionsdatei gespeichert.

Bearbeiten Sie diese Option nicht während des Normalbetriebs.

Bearbeiten Sie diese Option nur in Situationen wie den folgenden:

- Der Primärserver ist offline und die Informationen für den Sekundärserver befinden sich nicht in der Optionsdatei.
- Die Informationen des Sekundärservers sind nicht auf dem neuesten Stand oder falsch.

Alle von Ihnen bearbeiteten Werte werden bei Ihrer nächsten Anmeldung am Primärserver entfernt oder aktualisiert.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Diese Option wird in der Datei `dsm.sys` in die Zeilengruppe `replservername` eingefügt.

Syntax

►—`replserverguid—Server-GUID`—►

Parameter

Server-GUID

Gibt die GUID des Sekundärservers an, der im Fall einer Übernahme verwendet wird.

Beispiele

Optionsdatei:

```
REPLSERVERGUID 91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.02
```

Befehlszeile:

Nicht zutreffend.

Optionsdatei:

Das folgende Beispiel zeigt, wie Optionen für drei unterschiedliche Server in der Datei `dsm.sys` angegeben werden und wie ein Verweis auf den Sekundärserver aussieht.

Verbindungsdaten für mehrere Sekundärserver liegen in Zeilengruppen vor. Jede Zeilengruppe wird durch die Option **replservername** und den Namen des Sekundärservers angegeben.

Die Zeilengruppe **servername** muss die Option **myreplicationserver** enthalten, die auf den Sekundärserver verweist, der durch die Zeilengruppe **replservername** angegeben wird.

Nur ein Sekundärserver kann für jeweils eine Zeilengruppe **servername** angegeben werden.

```
REPLSERVERNAME    TargetReplicationServer1
REPLTCPSERVERADDRESS TargetReplicationServer1
REPLTCPPOrt       1505
REPLSSLPORT       1506
REPLSERVERGUID    91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00
```

```
REPLSERVERNAME    TargetReplicationServer2
REPLTCPSERVERADDRESS TargetReplicationServer2
REPLTCPPOrt       1505
REPLSSLPORT       1506
REPLSERVERGUID    91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.02
```

```
SErvername        server_a
  COMMMethod       TCPip
  TCPPOrt          1500
  TCPServeraddress server_hostname1.example.com
  PASSWORDAccess   prompt
  MYREPLICATIONServer TargetReplicationServer1
```

```
SErvername        server_b
  COMMMethod       TCPip
  TCPPOrt          1500
  TCPServeraddress server_hostname2.example.com
  PASSWORDAccess   generate
```

INCLExc1	/adm/tsm/archive.exc1
MYREPLICATIONServer	TargetReplicationServer2
Servename	server_c
COMMethod	TCPip
TCPPort	1500
TCPServeraddress	server_hostname3.example.com
PASSWORDAccess	generate
MYREPLICATIONServer	TargetReplicationServer1

Zugehörige Konzepte:

„Konfiguration und Verwendung der automatisierten Clientübernahme“ auf Seite 98

Zugehörige Tasks:

„Client für automatisierte Übernahme konfigurieren“ auf Seite 102

Replservername

Die Option `replservername` gibt den Namen des Sekundärservers an, zu dem der Client während einer Übernahme eine Verbindung herstellt.

Die Option `replservername` beginnt eine Zeilengruppe in der Clientoptionsdatei, die Verbindungsdaten zu dem Sekundärserver enthält.

Diese Option wird vom Administrator des IBM Spectrum Protect-Servers für den Clientknoten definiert. Während des normalen Anmeldeprozesses (ohne Übernahme) wird die Option an den Client gesendet und in der Clientoptionsdatei gespeichert.

Bearbeiten Sie diese Option nicht während des Normalbetriebs.

Bearbeiten Sie diese Option nur in Situationen wie den folgenden:

- Der Primärserver ist offline und die Informationen für den Sekundärserver befinden sich nicht in der Optionsdatei.
- Die Informationen des Sekundärservers sind nicht auf dem neuesten Stand oder falsch.

Alle von Ihnen bearbeiteten Werte werden bei Ihrer nächsten Anmeldung am Primärserver entfernt oder aktualisiert.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Diese Option wird in die Clientssystemoptionsdatei (`dsm.sys`) eingefügt.

Syntax

►►—`replservername`—*Replikationsservername*—►►

Parameter

Replikationsservername

Gibt den Namen des Sekundärservers an, der im Fall einer Übernahme verwendet werden soll. Dieser Wert ist in der Regel der Name des Sekundärservers, nicht der Hostname des Servers.

Beispiele

Optionsdatei:

```
REPLSERVERNAME    TargetReplicationServer1
```

Befehlszeile:

Nicht zutreffend.

Optionsdatei:

Das folgende Beispiel zeigt, wie Optionen für drei unterschiedliche Server in der Datei `dsm.sys` angegeben werden und wie ein Verweis auf den Sekundärserver aussieht.

Verbindungsdaten für mehrere Sekundärserver liegen in Zeilengruppen vor. Jede Zeilengruppe wird durch die Option **replservername** und den Namen des Sekundärservers angegeben.

Die Zeilengruppe **servername** muss die Option **myreplicationserver** enthalten, die auf den Sekundärserver verweist, der durch die Zeilengruppe **replservername** angegeben wird.

Nur ein Sekundärserver kann für jeweils eine Zeilengruppe **servername** angegeben werden.

```
REPLSERVERNAME    TargetReplicationServer1
REPLTCPSEVERADDRESS TargetReplicationServer1
REPLTCPPOINT      1505
REPLSSLPORT       1506
REPLSERVERGUID    91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00
```

```
REPLSERVERNAME    TargetReplicationServer2
REPLTCPSEVERADDRESS TargetReplicationServer2
REPLTCPPOINT      1505
REPLSSLPORT       1506
REPLSERVERGUID    91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02
```

```
SErvername        server_a
  COMMMethod      TCPip
  TCPPOINT        1500
  TCPSEVERADDRESS server_hostname1.example.com
  PASSWORDACCESS  prompt
  MYREPLICATIONSERVER TargetReplicationServer1
```

```
SErvername        server_b
  COMMMethod      TCPip
  TCPPOINT        1500
  TCPSEVERADDRESS server_hostname2.example.com
  PASSWORDACCESS  generate
  INCLExc1        /adm/tsm/archive.exc1
  MYREPLICATIONSERVER TargetReplicationServer2
```

```
SErvername        server_c
  COMMMethod      TCPip
  TCPPOINT        1500
  TCPSEVERADDRESS server_hostname3.example.com
  PASSWORDACCESS  generate
  MYREPLICATIONSERVER TargetReplicationServer1
```

Zugehörige Konzepte:

„Konfiguration und Verwendung der automatisierten Clientübernahme“ auf Seite 98

Zugehörige Tasks:

„Client für automatisierte Übernahme konfigurieren“ auf Seite 102

Replsslport

Die Option `replsslport` gibt den SSL-aktivierten TCP/IP-Anschluss des Sekundär-servers an. Die Option `replsslport` wird verwendet, wenn der Client während einer Übernahme eine Verbindung zum Sekundärserver herstellt. Diese Option wird nicht mehr unterstützt, wenn Sie die Verbindung zu einem IBM Spectrum Protect-Server der Version 8.1.2 und höheren Stufen sowie der Version 7.1.8 und höheren Stufen der Version 7 herstellen.

Der Primärserver sendet die Option `replsslport` nur dann an den Client, wenn der Sekundärserver für SSL konfiguriert ist.

Diese Option ist nur anwendbar, wenn der Client für die Verwendung von SSL für die sichere Kommunikation zwischen dem IBM Spectrum Protect-Server und -Client konfiguriert ist. Wenn der Client nicht für die Verwendung von SSL konfiguriert ist, wird der durch die Option `repltcpport` angegebene Anschluss verwendet. Wenn Sie feststellen wollen, ob der Client SSL verwendet, prüfen Sie die Clientoption SSL.

Diese Option muss in einer Zeilengruppe **replservername** in der Clientoptionsdatei angegeben werden. Die Zeilengruppe **replservername** enthält Verbindungsdaten des Sekundärservers.

Während des normalen Anmeldeprozesses (ohne Übernahme) wird diese Option an den Client gesendet und in der Clientoptionsdatei gespeichert.

Bearbeiten Sie diese Option nicht während des Normalbetriebs.

Bearbeiten Sie diese Option nur in Situationen wie den folgenden:

- Der Primärserver ist offline und die Informationen für den Sekundärserver befinden sich nicht in der Optionsdatei.
- Die Informationen des Sekundärservers sind nicht auf dem neuesten Stand oder falsch.

Alle von Ihnen bearbeiteten Werte werden bei Ihrer nächsten Anmeldung am Primärserver entfernt oder aktualisiert.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Diese Option wird in der Datei `dsm.sys` in die Zeilengruppe **replservername** eingefügt.

Syntax

►►—`replsslport`—*Anschlussadresse*—►►

Parameter

Anschlussadresse

Gibt die SSL-aktivierte TCP/IP-Anschlussadresse für die Datenübertragung mit dem Sekundärserver an.

Beispiele

Optionsdatei:

REPLSSLPORT 1506

Befehlszeile:

Nicht zutreffend.

Optionsdatei:

Das folgende Beispiel zeigt, wie Optionen für drei unterschiedliche Server in der Datei `dsm.sys` angegeben werden und wie ein Verweis auf den Sekundärserver aussieht.

Verbindungsdaten für mehrere Sekundärserver liegen in Zeilengruppen vor. Jede Zeilengruppe wird durch die Option **replservername** und den Namen des Sekundärservers angegeben.

Die Zeilengruppe **servername** muss die Option **myreplicationserver** enthalten, die auf den Sekundärserver verweist, der durch die Zeilengruppe **replservername** angegeben wird.

Nur ein Sekundärserver kann für jeweils eine Zeilengruppe **servername** angegeben werden.

```
REPLSERVERNAME    TargetReplicationServer1
REPLTCPSEVERADDRESS TargetReplicationServer1
REPLTCPPOrt       1505
REPLSSLPORT       1506
REPLSERVERGUID    91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00
```

```
REPLSERVERNAME    TargetReplicationServer2
REPLTCPSEVERADDRESS TargetReplicationServer2
REPLTCPPOrt       1505
REPLSSLPORT       1506
REPLSERVERGUID    91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02
```

```
SErvername        server_a
  COMMMethod      TCPip
  TCPPOrt         1500
  TCPSEveraddress  server_hostname1.example.com
  PASSWORDAccess  prompt
  MYREPLICATIONServer TargetReplicationServer1
```

```
SErvername        server_b
  COMMMethod      TCPip
  TCPPOrt         1500
  TCPSEveraddress  server_hostname2.example.com
  PASSWORDAccess  generate
  INCLExc1        /adm/tsm/archive.exc1
  MYREPLICATIONServer TargetReplicationServer2
```

```
SErvername        server_c
  COMMMethod      TCPip
  TCPPOrt         1500
  TCPSEveraddress  server_hostname3.example.com
  PASSWORDAccess  generate
  MYREPLICATIONServer TargetReplicationServer1
```

Zugehörige Konzepte:

„Konfiguration und Verwendung der automatisierten Clientübernahme“ auf Seite 98

Zugehörige Tasks:

„Client für automatisierte Übernahme konfigurieren“ auf Seite 102

Repltcpport

Die Option `repltcpport` gibt den TCP/IP-Anschluss des Sekundärservers an, der verwendet werden soll, wenn der Client während einer Übernahme eine Verbindung zum Sekundärserver herstellt.

Diese Option muss in einer Zeilengruppe **replservername** in der Clientoptionsdatei angegeben werden. Die Zeilengruppe **replservername** enthält Verbindungsdaten des Sekundärservers.

Diese Option wird vom Administrator des IBM Spectrum Protect-Servers für den Clientknoten definiert. Während des normalen Anmeldeprozesses (ohne Übernahme) wird die Option an den Client gesendet und in der Clientoptionsdatei gespeichert.

Bearbeiten Sie diese Option nicht während des Normalbetriebs.

Bearbeiten Sie diese Option nur in Situationen wie den folgenden:

- Der Primärserver ist offline und die Informationen für den Sekundärserver befinden sich nicht in der Optionsdatei.
- Die Informationen des Sekundärservers sind nicht auf dem neuesten Stand oder falsch.

Alle von Ihnen bearbeiteten Werte werden bei Ihrer nächsten Anmeldung am Primärserver entfernt oder aktualisiert.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Diese Option wird in der Datei `dsm.sys` in die Zeilengruppe **replservername** eingefügt.

Syntax

►►—`repltcpport`—*Anschlussadresse*—►►

Parameter

Anschlussadresse

Gibt die TCP/IP-Anschlussadresse für die Datenübertragung mit dem Sekundärserver an.

Beispiele

Optionsdatei:

REPLTCPport 1500

Befehlszeile:

Nicht zutreffend.

Optionsdatei:

Das folgende Beispiel zeigt, wie Optionen für drei unterschiedliche Server in der Datei `dsm.sys` angegeben werden und wie ein Verweis auf den Sekundärserver aussieht.

Verbindungsdaten für mehrere Sekundärserver liegen in Zeilengruppen vor. Jede Zeilengruppe wird durch die Option **replservername** und den Namen des Sekundärservers angegeben.

Die Zeilengruppe **servername** muss die Option **myreplicationserver** enthalten, die auf den Sekundärserver verweist, der durch die Zeilengruppe **replservername** angegeben wird.

Nur ein Sekundärserver kann für jeweils eine Zeilengruppe **servername** angegeben werden.

```
REPLSERVERNAME      TargetReplicationServer1
REPLTCPSEVERADDRESS TargetReplicationServer1
REPLTCPPOrt         1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00
```

```
REPLSERVERNAME      TargetReplicationServer2
REPLTCPSEVERADDRESS TargetReplicationServer2
REPLTCPPOrt         1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02
```

```
SErvername      server_a
COMMMethod      TCPip
TCPPOrt         1500
TCPSEveraddress server_hostname1.example.com
PASSWORDAccess  prompt
MYREPLICATIONServer TargetReplicationServer1
```

```
SErvername      server_b
COMMMethod      TCPip
TCPPOrt         1500
TCPSEveraddress server_hostname2.example.com
PASSWORDAccess  generate
INCLExcl        /adm/tsm/archive.excl
MYREPLICATIONServer TargetReplicationServer2
```

```
SErvername      server_c
COMMMethod      TCPip
TCPPOrt         1500
TCPSEveraddress server_hostname3.example.com
PASSWORDAccess  generate
MYREPLICATIONServer TargetReplicationServer1
```

Zugehörige Konzepte:

„Konfiguration und Verwendung der automatisierten Clientübernahme“ auf Seite 98

Zugehörige Tasks:

„Client für automatisierte Übernahme konfigurieren“ auf Seite 102

Repltcpserveraddress

Die Option `repltcpserveraddress` gibt die TCP/IP-Adresse des Sekundärservers an, die verwendet werden soll, wenn der Client während einer Übernahme eine Verbindung zum Sekundärserver herstellt.

Diese Option muss in einer Zeilengruppe **replservername** in der Clientoptionsdatei angegeben werden. Die Zeilengruppe **replservername** enthält Verbindungsdaten des Sekundärservers.

Diese Option wird vom Administrator des IBM Spectrum Protect-Servers für den Clientknoten definiert. Während des normalen Anmeldeprozesses (ohne Übernahme) wird die Option an den Client gesendet und in der Clientoptionsdatei gespeichert.

Bearbeiten Sie diese Option nicht während des Normalbetriebs.

Bearbeiten Sie diese Option nur in Situationen wie den folgenden:

- Der Primärserver ist offline und die Informationen für den Sekundärserver befinden sich nicht in der Optionsdatei.
- Die Informationen des Sekundärservers sind nicht auf dem neuesten Stand oder falsch.

Alle von Ihnen bearbeiteten Werte werden bei Ihrer nächsten Anmeldung am Primärserver entfernt oder aktualisiert.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Diese Option wird in der Datei `dsm.sys` in die Zeilengruppe **replservername** eingefügt.

Syntax

►—REPLTCPServeraddress—*Serveradresse*—►

Parameter

Serveradresse

Gibt eine TCP/IP-Adresse für einen Server mit einer Länge von 1 - 64 Zeichen an. Geben Sie einen TCP/IP-Domännennamen oder eine numerische IP-Adresse an. Die numerische IP-Adresse kann entweder eine TCP/IP-V4- oder eine TCP/IP-V6-Adresse sein. Sie können IPv6-Adressen nur verwenden, wenn Sie die Option `commethod V6Tcpip` angegeben haben.

Beispiele

Optionsdatei:

```
REPLTCPServeraddress dsmchost.example.com
```

Befehlszeile:

Nicht zutreffend.

Optionsdatei:

Das folgende Beispiel zeigt, wie Optionen für drei unterschiedliche Server in der Datei `dsm.sys` angegeben werden und wie ein Verweis auf den Sekundärserver aussieht.

Verbindungsdaten für mehrere Sekundärserver liegen in Zeilengruppen vor. Jede Zeilengruppe wird durch die Option **replservername** und den Namen des Sekundärservers angegeben.

Die Zeilengruppe **servername** muss die Option **myreplicationserver** enthalten, die auf den Sekundärserver verweist, der durch die Zeilengruppe **replservername** angegeben wird.

Nur ein Sekundärserver kann für jeweils eine Zeilengruppe **servername** angegeben werden.

```
REPLSERVERNAME      TargetReplicationServer1
REPLTCPSERVERADDRESS TargetReplicationServer1
REPLTCPSPORT        1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00
```

```
REPLSERVERNAME      TargetReplicationServer2
REPLTCPSERVERADDRESS TargetReplicationServer2
REPLTCPSPORT        1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02
```

```
SErvername      server_a
  COMMMethod          TCPip
  TCPPort            1500
  TCPServeraddress    server_hostname1.example.com
  PASSWORDAccess      prompt
  MYREPLICATIONServer TargetReplicationServer1
```

```
SErvername      server_b
  COMMMethod          TCPip
  TCPPort            1500
  TCPServeraddress    server_hostname2.example.com
  PASSWORDAccess      generate
  INCLExc1            /adm/tsm/archive.exc1
  MYREPLICATIONServer TargetReplicationServer2
```

```
SErvername      server_c
  COMMMethod          TCPip
  TCPPort            1500
  TCPServeraddress    server_hostname3.example.com
  PASSWORDAccess      generate
  MYREPLICATIONServer TargetReplicationServer1
```

Zugehörige Konzepte:

„Konfiguration und Verwendung der automatisierten Clientübernahme“ auf Seite 98

Zugehörige Tasks:

„Client für automatisierte Übernahme konfigurieren“ auf Seite 102

Resourceutilization

Mit der Option **resourceutilization** in Ihrer Optionsdatei können Sie den Umfang der Ressourcen steuern, die der IBM Spectrum Protect-Server und -Client während der Verarbeitung verwenden können.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Datei `dsm.sys` innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Allgemein** im Feld **Ressourcen-auslastung** des Profileditors definieren.

Syntax

►—RESOURCEutilization— *Nummer*—►

Parameter

Zahl

Gibt den Umfang der Ressourcen an, die der IBM Spectrum Protect-Server und -Client während der Verarbeitung verwenden können. Der Wertebereich, der angegeben werden kann, ist 1 bis 100. Der Standardwert ist 2.

Beispiele

Optionsdatei:

```
resourceutilization 7
```

Befehlszeile:

```
-resourceutilization=7
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Sicherungs- und Archivierungssitzungen steuern

Wenn Sie eine Sicherung oder Archivierung anfordern, kann der Client mehrere Sitzungen mit dem Server verwenden.

Standardmäßig werden maximal zwei Sitzungen verwendet, eine für die Abfrage des Servers und eine zum Senden von Dateidaten. Der Client kann nur eine Serversitzung verwenden, wenn Sie die Option **resourceutilization** auf 1 setzen.

Ein Client kann mehr als die standardmäßige Anzahl Sitzungen verwenden, wenn er eine Verbindung zum IBM Spectrum Protect-Server herstellt. Bei der Angabe `resourceutilization 10` sind beispielsweise bis zu acht Sitzungen mit dem Server möglich. Mehrere Sitzungen können zur Abfrage des Servers und zum Senden von Dateidaten verwendet werden.

Mehrere Abfragesitzungen werden verwendet, wenn in einem Sicherungs- oder Archivierungsbefehl mehrere Dateispezifikationen angegeben sind. Wenn Sie beispielsweise die folgenden Befehle eingeben und `resourceutilization 5` angeben, könnte der Client eine zweite Sitzung starten, um Dateien im Dateibereich B abzufragen.

```
inc /Volumes/filespaceA /Volumes/filespaceB
```

Ob die zweite Sitzung tatsächlich gestartet wird, hängt davon ab, wie lange es dauert, den Server nach Dateien abzufragen, die in Dateibereich A gesichert sind. Außerdem könnte der Client versuchen, Daten aus dem Dateisystem zu lesen und in mehreren Sitzungen an den Server zu senden.

Anmerkung: Wenn Sie während einer Sicherungsoperation mehrere Dateispezifikationen eingeben, kann dies unter Umständen dazu führen, dass Dateien von ei-

ner Dateispezifikation auf mehreren Bändern gespeichert und mit Dateien von anderen Dateispezifikationen durchsetzt werden. Dies kann die Zurückschreibungsleistung verringern. Durch das Setzen der Option **collocatebyfilespec** auf yes wird das Durchsetzen von Dateien von unterschiedlichen Dateispezifikationen eliminiert, indem der Client auf eine Serversitzung pro Dateispezifikation begrenzt wird. Wenn Sie Daten auf Band speichern, werden Dateien für jede Dateispezifikation deshalb zusammen auf einem Band gespeichert (sofern auf Grund erhöhter Kapazität kein weiteres Band erforderlich ist).

Zugehörige Verweise:

„Collocatebyfilespec“ auf Seite 375

Zurückschreibungssitzungen steuern

Wenn Sie eine Zurückschreibung anfordern, wird standardmäßig maximal eine Sitzung verwendet.

Weitere Zurückschreibungssitzungen basieren auf den folgenden Faktoren:

- Wert der Option **resourceutilization**
- Auf wie vielen Bändern die angeforderten Daten gespeichert sind
- Wie viele Bandlaufwerke verfügbar sind
- Die für den Knoten zulässige maximale Anzahl der Mountpunkte

Anmerkung:

1. Wenn alle Dateien auf Platte sind, wird nur eine Sitzung verwendet. Für eine reine Plattenspeicherpoolzurückschreibung gibt es keine Mehrfachszitzung. Wenn Sie jedoch eine Zurückschreibung ausführen, bei der sich die Dateien auf 4 Bändern und andere auf der Platte befinden, könnten Sie während der Zurückschreibung bis zu 5 Sitzungen verwenden.
2. Der IBM Spectrum Protect-Server kann die maximale Anzahl Mountpunkte, die ein Knoten auf dem Server verwenden kann, mit Hilfe des Parameters **MAXNUMMP** definieren. Wenn der Wert der Option **resourceutilization** den Wert für **MAXNUMMP** auf dem Server für einen Knoten überschreitet, kann die Sicherung mit der Nachricht Unbekannter Systemfehler fehlschlagen.
3. Sie können eine Zurückschreibung in Mehrfachszitzung aus Ihrem einzelnen Zurückschreibungsbefehl (**restore**) und von einem einzelnen Datenträger auf dem Server abrufen, wenn dieser Datenträger die Einheitenklasse FILE aufweist.

Befinden sich die Daten, die Sie zurückschreiben wollen, beispielsweise auf 5 verschiedenen Banddatenträgern, beträgt die maximale Anzahl Mountpunkte für Ihren Knoten 5 und ist für **resourceutilization** 3 definiert, werden 3 Sitzungen zum Zurückschreiben verwendet. Wenn Sie die Einstellung für **resourceutilization** auf 5 erhöhen, werden 5 Sitzungen zum Zurückschreiben verwendet. Es gibt eine Eins-zu-Eins-Beziehung zwischen der zulässigen Anzahl Zurückschreibungssitzungen und der Einstellung für **resourceutilization**. Mehrere Zurückschreibungssitzungen sind nur für Zurückschreibungsoperationen ohne Abfrage zulässig.

Hinweise für mehrere Clientsitzungen

In diesem Abschnitt sind einige Hinweise aufgeführt, die Sie beachten sollten, wenn Sie mit mehreren Clientsitzungen arbeiten.

Folgende Faktoren können den Durchsatz von Mehrfachszitzungen beeinflussen:

- Die Fähigkeit des Servers, mehrere Clientsitzungen auszuführen. Sind ausreichender Speicher, mehrere Speicherdatenträger und Prozessorzyklen zur Steigerung des Sicherungsdurchsatzes vorhanden?

- Die Fähigkeit des Clients, mehrere Sitzungen auszuführen (genügend Prozessorzyklen, Speicher etc.).
- Die Konfiguration des Clientspeichersubsystems. Dateisysteme, die über mehrere Datenträger einheitenübergreifend gespeichert sind, entweder durch einheitenübergreifendes Lesen und Schreiben von Daten (Software Striping) oder RAID-5, können eine Zunahme wahlfreier Leseanforderungen besser bearbeiten als ein Dateisystem mit einem einzigen Laufwerk. Außerdem ist in einem Dateisystem mit einem einzigen Laufwerk möglicherweise keine Leistungsverbesserung zu verzeichnen, wenn es versucht, viele wahlfreie, gleichzeitige Leseanforderungen zu bearbeiten.
- Ausreichende Bandbreite im Netz zur Unterstützung des erhöhten Datenaustauschs.

Zu den möglichen unerwünschten Aspekten der Ausführung von Mehrfachsitzen gehören:

- Der Client könnte mehrere Abrechnungssätze generieren.
- Der Server könnte nicht genügend gleichzeitige Sitzungen starten. Um dies zu vermeiden, muss der Parameter *maxsessions* überprüft und eventuell geändert werden.
- Ein Befehl *query node* könnte die Clientaktivität nicht zusammenfassen.
- Es ist möglich, dass Dateien anstelle von festen Verbindungen zurückgeschrieben werden.

Dateien können anstelle von festen Verbindungen zurückgeschrieben werden, wenn alle der folgenden Bedingungen zutreffen:

- Sie schreiben ein gesamtes Dateisystem zurück.
- Während der Zurückschreibungsoperation ist der Wert der Option *resourceutilization* größer als 1.
- Das Dateisystem enthielt bei seiner Sicherung feste Verbindungen.

Die Wahrscheinlichkeit, dass verbundene Dateien anstelle von festen Verbindungen zurückgeschrieben werden, erhöht sich mit der Anzahl der Sitzungen. Wenn Sie ein Dateisystem zurückschreiben, das bei seiner Sicherung feste Verbindungen enthielt, geben Sie *resourceutilization=1* an, um sicherzustellen, dass feste Verbindungen zurückgeschrieben werden.

Retryperiod

Mit der Option *retryperiod* wird die Wartezeit (in Minuten) des Client-Schedulers zwischen den Versuchen, einen geplanten Befehl, der fehlgeschlagen ist, auszuführen oder zwischen fehlgeschlagenen Versuchen, Ergebnisse an den Server zu melden, angegeben. Verwenden Sie diese Option nur, wenn der Scheduler aktiv ist.

Ihr Administrator kann diese Option auch definieren. Gibt Ihr Administrator einen Wert für diese Option an, überschreibt dieser den Wert in Ihrer *Clientsystemoptionsdatei*, nachdem Ihr Clientknoten erfolgreich den Kontakt zum Server hergestellt hat.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Scheduler** im Feld **Wiederholungszeitlimit** im Profileditor definieren.

Syntax

►►—RETRYPeriod— *Minuten*—►►

Parameter

Minuten

Gibt die Anzahl Minuten an, die der Client-Scheduler zwischen den Versuchen wartet, eine Verbindung zum Server herzustellen oder einen geplanten Befehl, der fehlschlägt, zu verarbeiten. Der Wertebereich ist 1 bis 9999; Standardwert ist 20.

Beispiele

Optionsdatei:

retryp 10

Befehlszeile:

-retryperiod=10

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Revokeremoteaccess

Die Option `revokeremoteaccess` schränkt den Zugriff eines Administrators mit Clientzugriffsberechtigung auf eine Client-Workstation, auf der der Web-Client aktiv ist, ein.

Diese Option schränkt den Zugriff von Administratoren mit Clienteigner-, System- oder Maßnahmenberechtigung auf die Workstation des Benutzers mit Hilfe des Web-Clients nicht ein.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Web-Client** im Profileditor definieren.

Syntax

►►—REVOKERemoteaccess—

None
Access

—►►

Parameter

None

Der Zugriff von Administratoren mit Clientzugriffsberechtigung für den Client wird nicht widerrufen. Dies ist der Standardwert.

Access

Der Zugriff von Administratoren mit Clientzugriffsberechtigung für den Client wird widerrufen.

Beispiele

Optionsdatei:

```
revokeremoteaccess none
```

Befehlszeile:

Nicht zutreffend.

Schedcmddisabled

Die Option `schedcmddisabled` gibt an, ob die Zeitplanung von Befehlen durch die Serveroption `action=command` im Serverbefehl **define schedule** inaktiviert werden soll.

Durch diese Option werden die Befehle `preschedulecmd` und `postschedulecmd` nicht inaktiviert. Sie können jedoch `preschedulecmd` oder `postschedulecmd` mit einem Leerzeichen oder einer Nullzeichenfolge angeben, um die Zeitplanung dieser Befehle zu inaktivieren.

Sie können die Zeitplanung von Befehlen, die von Ihrem IBM Spectrum Protect-Administrator definiert wurden, inaktivieren, indem Sie die Option `schedcmddisabled` auf `yes` setzen.

Verwenden Sie den Befehl **query schedule**, um die von Ihrem Administrator definierten Zeitpläne abzufragen.

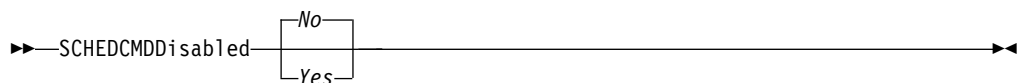
Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Datei `dsm.sys` innerhalb einer Serverzeilengruppe ein.

Syntax



Parameter

Yes

Gibt an, dass der Server die Planung von Befehlen mit der Option `action=command` des Serverbefehls **DEFINE SCHEDULE** inaktiviert.

No Gibt an, dass der Server die Planung von Befehlen mit der Option `action=command` des Serverbefehls `DEFINE SCHEDULE` nicht inaktiviert. Dies ist der Standardwert.

Beispiele

Optionsdatei:

`schedcmddisabled no`

Befehlszeile:

Nicht zutreffend.

Zugehörige Informationen

„Query Schedule“ auf Seite 765

Schedcmdexception

Die Option `schedcmdexception` wird in Kombination mit der Option `schedcmddisabled` verwendet, um die Planung von Befehlen durch die Serveroption `action=command` im Serverbefehl `DEFINE SCHEDULE` zu inaktivieren, mit Ausnahme bestimmter Befehlszeichenfolgen.

Sie müssen die genaue Zeichenfolge angeben, die mit der Definition des „Objekts“ im Zeitplan übereinstimmt, damit der geplante Serverbefehl akzeptiert wird. Stimmt die Zeichenfolge nicht genau überein (sie enthält beispielsweise ein zusätzliches Leerzeichen oder die Groß-/Kleinschreibung unterscheidet sich), wird die geplante Befehlsaktion blockiert.

Sie können mehrere Optionen `schedcmdexception` in der Optionsdatei angeben. Diese Option wird nur berücksichtigt, wenn die Option `schedcmddisabled` aktiviert ist. Die Position dieser Option in der Optionsdatei ist unabhängig von der Position der Option `schedcmddisabled`.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option ist nicht in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server gültig.

Optionsdatei

Fügen Sie diese Option in die Datei `dsm.sys` innerhalb einer Serverzeilengruppe ein.

Syntax

►►—`SCHEDCMDException—string`—◄◄

Parameter

Zeichenfolge

Für Befehle, die mit der Option `action=command` im Serverbefehl `DEFINE SCHEDULE` geplant werden, gibt dieser Parameter das Objektmuster an, das zu aktivieren ist, wenn die Option `schedcmddisabled=yes` angegeben wird. Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden und der Parameter muss genau mit der Befehlszeichenfolge in der Zeitplandefinition auf dem IBM Spectrum Protect-Server übereinstimmen.

Beispiel

Optionsdatei:

```
schedcmddisabled yes  
  
schedcmdexception "start echo hello, world!"
```

Zugehörige Informationen

„Schedcmddisabled“ auf Seite 562

Schedgroup

Mit der Option `schedgroup` wird ein Zeitplan einer Gruppe zugeordnet.

Ein Beispiel für die Verwendung dieser Option ist die Gruppierung mehrerer Zeitpläne zur täglichen lokalen Sicherung in einem einzigen Zeitplan zur Sicherung des Servers.

Unterstützte Clients

Diese Option ist für alle Clients als Befehlszeilenoption für den Serverbefehl **DEFINE SCHEDULE** gültig. Diese Option kann nicht einer Clientoptionsgruppe auf dem IBM Spectrum Protect-Server hinzugefügt werden.

Syntax

►►—SCHEDGROUP— *—Name_der_Zeitplangruppe—*◄◄

Parameter

Name_der_Zeitplangruppe

Gibt den Namen der Zeitplangruppe an. Sie können bis zu 30 Zeichen für den Namen angeben.

Eine Liste der gültigen Zeichen, die im Namen der Zeitplangruppe verwendet werden können, finden Sie in IBM Spectrum Protect-Objekte benennen.

Beispiele

Mit den folgenden Beispielbefehlen werden die Zeitpläne `SCHED_A_1`, `SCHED_A_2`, `SCHED_A_3` und `SCHED_A_4` in der Zeitplangruppe `GROUP_A` gruppiert.

Befehlszeile:

Dieses Beispiel zeigt eine lokale Sicherung um 6 Uhr:

```
define schedule standard SCHED_A_1 Type=Client ACTION=Backup  
SUBACTION=VM OPTIONS='-vmfulltype=vstor -vmbackuptype=fullvm  
-vmbackuplocation=local -domain.vmfull="SCHEDULE-TAG"  
-asnodename=DC_SARTRE_WB -SCHEDGROUP=GROUP_A STARTDate=02/06/2017  
STARTTime=06:00:00 SCHEDStyle=Enhanced DAYofweek=ANY
```

Dieses Beispiel zeigt eine lokale Sicherung um 12 Uhr:

```
define schedule standard SCHED_A_2 Type=Client ACTION=Backup  
SUBACTION=VM OPTIONS='-vmfulltype=vstor -vmbackuptype=fullvm  
-vmbackuplocation=local -domain.vmfull="SCHEDULE-TAG"
```



```
-asnodename=DC_SARTRE_WB -SCHEDGROUP=GROUP_A' STARTDate=02/06/2017  
STARTTime=12:00:00 SCHEDStyle=Enhanced DAYofweek=ANY
```

Dieses Beispiel zeigt eine lokale Sicherung um 18 Uhr:

```
define schedule standard SCHED_A_3 Type=Client ACTION=Backup  
SUBACTION=VM OPTIONS='-vmfulltype=vstor -vmbackuptype=fullvm  
-vmbackuplocation=local -domain.vmfull="SCHEDULE-TAG"  
-asnodename=DC_SARTRE_WB -SCHEDGROUP=GROUP_A' STARTDate=02/06/2017  
STARTTime=18:00:00 SCHEDStyle=Enhanced DAYofweek=ANY
```

Dieses Beispiel zeigt eine lokale Sicherung und eine Serversicherung um Mitternacht:

```
define schedule standard SCHED_A_4 Type=Client ACTION=Backup  
SUBACTION=VM OPTIONS='-vmfulltype=vstor -vmbackuptype=fullvm  
-vmbackuplocation=both -domain.vmfull="SCHEDULE-TAG"  
-asnodename=DC_SARTRE_WB -SCHEDGROUP=GROUP_A' STARTDate=02/06/2017  
STARTTime=00:00:00 SCHEDStyle=Enhanced DAYofweek=ANY
```

Tipp: Stellen Sie sicher, dass jeder Zeitplan in der Gruppe vor dem festgelegten Start des nächsten Zeitplans vollständig ausgeführt werden kann.

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Schedlogmax

Die Option schedlogmax gibt die maximale Größe des Planungsprotokolls (dsm-sched.log) und des Web-Client-Protokolls (dsmwebcl.log) in Megabyte an.

Diese Option bewirkt, dass bei den Protokolldateien, die für Schedulerereignisse (dmsched.log) und für Web-Client-Ereignisse (dsmwebcl.log) erstellt werden, ein Umlauf stattfindet, wenn sie ihre maximale Größe erreichen. Bei der Protokollierung von Scheduler- und Web-Client-Ereignissen werden Protokollsätze bis zum Erreichen der angegebenen maximalen Größe an das Ende der Protokolldateien angefügt. Wenn die maximale Größe erreicht ist, wird ein Protokollsatz mit dem Inhalt der Datei am Dateianfang fortgesetzt als letzter Satz in die Datei gestellt. Die nachfolgende Protokollierung wird am Anfang der Datei wieder aufgenommen. Das Ende des Umlaufprotokolls wird durch einen Satz mit dem Inhalt DATENENDE angezeigt.

Wenn Sie die Option schedlogmax angeben, werden Scheduler- und Web-Client-Protokollnachrichten nicht in einer bereinigten Datei gespeichert. Wenn Sie Protokolle bereinigen und die bereinigten Protokolleinträge in einer anderen Datei speichern wollen, lesen Sie die Informationen zur Option schedlogretention.

Wenn Sie vom Protokollumlauf (Option schedlogmax) zur Protokollbereinigung (Option schedlogretention) wechseln, werden alle vorhandenen Protokolleinträge aufbewahrt, und das Protokoll wird mit den neuen Kriterien von schedlogretention bereinigt.

Wenn Sie von der Protokollbereinigung (Option schedlogretention) zum Protokollumlauf (Option schedlogmax) wechseln, werden alle Sätze in den vorhandenen Protokollen in eine Datei kopiert, die die bereinigten Einträge enthält. Aus der Datei dmsched.log bereinigte Protokollsätze werden beispielsweise in die Datei dmsched.pru kopiert. Aus der Datei dsmwebcl.log bereinigte Protokollsätze wer-

den in die Datei `dsmweblog.pru` kopiert. Die vorhandenen Protokolle (`dsmsched.log` und `dsmwebcl.log`) werden geleert und die Protokollierung beginnt mit den neuen Protokollumlaufbedingungen.

Wenn Sie lediglich den Wert der Option `schedlogmax` ändern, wird das vorhandene Protokoll erweitert oder gekürzt, um der neuen Größe zu entsprechen. Wird der Wert verkleinert, werden die ältesten Einträge gelöscht, um die Datei auf die neue Größe zu verkleinern.

Wird weder `schedlogmax` noch `schedlogretention` angegeben, kann das Fehlerprotokoll uneingeschränkt wachsen. Sie müssen den Protokollinhalt manuell verwalten, um zu verhindern, dass das Protokoll die Plattenressourcen verbraucht. Wenn das Protokoll ohne eine der beiden Optionen erstellt wurde und wenn Sie später einen Befehl mit der Option `schedlogretention` ausgeben, wird das Protokoll mit dem angegebenen Wert für die Aufbewahrungsdauer bereinigt. Wenn das Protokoll ohne eine der beiden Optionen erstellt wurde und wenn Sie später einen Befehl mit der Option `schedlogmax` ausgeben, wird das vorhandene Protokoll als bereinigtes Protokoll behandelt. Das heißt, der Inhalt der Datei `dsmsched.log` wird in eine Datei mit dem Namen `dsmsched.pru` kopiert, der Inhalt der Datei `dsmwebcl.log` wird in eine Datei mit dem Namen `dsmwebcl.pru` kopiert und sowohl in `dsmsched.log` als auch in `dsmwebcl.log` werden neue Protokolleinträge erstellt. In beiden Dateien findet ein Umlauf statt, wenn sie ihre maximale Größe erreichen.

Anmerkung: Wenn Sie für `schedlogmax` einen Wert ungleich null angeben (wodurch der Protokollumlauf aktiviert wird), können Sie nicht die Option `schedlogretention` verwenden, um bereinigte Protokolle zu erstellen. Für Protokolle kann entweder eine Bereinigung oder ein Umlauf durchgeführt werden, aber nicht beides.

Mit der Option `schedlogmax` erstellte Protokolle enthalten einen Protokollkopfsatz, der Informationen wie in dem folgenden Beispieldatensatz enthält:

```
LOGHEADERREC 661 104857600 IBM Spectrum Protect 8.1.0.0 Fri Dec 9 06:46:53 2014
```

Beachten Sie, dass die Datums- und Zeitmarkenangaben im Text von LOGHEADERREC nicht mithilfe der Einstellungen übersetzt oder formatiert werden, die in den Optionen `dateformat` und `timeformat` angegeben sind.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein.

Sie können diese Option auch auf der Registerkarte **Clientvorgaben > Scheduler** in der GUI definieren. Wählen Sie hierfür **Umlauf für Schedulerprotokolldatei aktivieren** aus und geben Sie einen Wert ungleich null für **Maximale Größe** der Protokolldatei an. Geben Sie für die **maximale Größe** null an, um den Umlauf der Protokolldatei zu verhindern. Wenn die maximale Größe auf null gesetzt ist, bleibt die Option **Umlauf für Schedulerprotokolldatei aktivieren** wirkungslos. Es findet kein Protokollumlauf statt, wenn die **maximale Größe** auf null gesetzt ist.

Syntax

►—SCHEDLOGMAX— Größe—►

Parameter

Größe

Gibt die maximale Größe für die Protokolldatei in Megabyte an. Der Wertebereich ist 0 bis 2047. Der Standardwert ist 0, wodurch der Protokolldateiurnlauf inaktiviert und die Größe der Protokolldatei unbeschränkt wird.

Beispiele

Optionsdatei:

```
schedlogmax 100
```

Befehlszeile:

```
-schedlogmax=100
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Schedlogname

Die Option `schedlogname` gibt den Pfad und den Namen der Datei an, in der Planungsprotokollinformationen gespeichert werden sollen.

Verwenden Sie diese Option nur, wenn Sie Planungsprotokollinformationen speichern wollen. Diese Option wird nur angewendet, wenn der Scheduler aktiv ist.

Wird diese Option nicht verwendet, wird die Datei `dsmsched.log` in demselben Verzeichnis erstellt wie die Datei `dsmerror.log`.

Wenn Sie den Befehl **schedule** ausführen, wird die Ausgabe geplanter Befehle auf Ihrem Bildschirm angezeigt. Außerdem wird die Ausgabe in die mit dieser Option angegebene Datei gesendet. Wenn ein Teil des von Ihnen angegebenen Pfads nicht vorhanden ist, versucht der Client, ihn zu erstellen.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Scheduler** im Textfeld **Planungsprotokoll** im Profileditor definieren.

Anmerkung: Geben Sie für die Umgebungsvariable `DSM_LOG` ein Verzeichnis an, in das das Protokoll gestellt werden soll. Das angegebene Verzeichnis muss Berechtigungen aufweisen, die einen Schreibzugriff von dem Konto zulassen, unter dem der Client ausgeführt wird. Das Stammverzeichnis ist kein gültiger Wert für `DSM_LOG`.

Syntax

►—SCHEDLOGName— *—Dateispezifikation—* ◄

Parameter

Dateispezifikation

Gibt den Pfad und den Namen der Datei an, in der Planungsprotokolldaten bei der Verarbeitung geplanter Arbeit gespeichert werden sollen. Wenn ein Teil des von Ihnen angegebenen Pfads nicht vorhanden ist, versucht der Client, ihn zu erstellen.

Wird nur ein Dateiname angegeben, wird die Datei im aktuellen Verzeichnis gespeichert. Standardwert ist das aktuelle Arbeitsverzeichnis und der Dateiname `dsmsched.log`. Die Datei `dsmsched.log` darf *keine* symbolische Verbindung sein.

Für Mac OS X: Wenn Sie nur einen Dateinamen angeben, wird die Datei in Ihrem Standardordner gespeichert. Die Standardverzeichnisse sind:

```
~/Library/Logs/tivoli/tsm  
/Library/Logs/tivoli/tsm
```

Beispiele

Optionsdatei:

```
SCHEDLOGN /Users/user1/Library/Logs/schedlog.jan  
schedlogname /home/mydir/schedlog.jan
```

Befehlszeile:

```
-schedlogname=/Users/user1/Library/Logs/schedlog.jan
```

Befehlszeile:

```
-schedlogname=/home/mydir/schedlog.jan
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Zugehörige Informationen

Unter „Errorlogname“ auf Seite 435 finden Sie weitere Informationen zur Position der Datei `dsmsched.log`.

Schedlogretention

Mit der Option `schedlogretention` kann die Aufbewahrungsdauer in Tagen für Einträge im Planungsprotokoll (`dsmsched.log`) und im Web-Client-Protokoll (`dsmwebcl.log`) festgelegt werden und ob bereinigte Einträge in einer anderen Datei gespeichert werden sollen.

Das Planungsprotokoll (`dsmsched.log`) wird beim Start des Schedulers und nach Beendigung eines geplanten Ereignisses bereinigt. Bereinigte Einträge werden in eine Datei mit dem Namen `dsmsched.pru` geschrieben.

Das Web-Client-Protokoll (`dsmwebcl.log`) wird beim anfänglichen Start des Clientakzeptordämons bereinigt. Bereinigte Einträge werden in eine Datei mit dem Namen `dsmwebcl.pru` geschrieben.

Wenn Sie von der Protokollbereinigung (Option `shedlogretention`) zum Protokollumlauf (Option `shedlogmax`) wechseln, werden alle Sätze im vorhandenen Protokoll in das bereinigte Protokoll (`dsmsched.pru` und `dsmwebcl.pru`) kopiert und die vorhandenen Protokolle (`dsmsched.log` und `dsmwebcl.log`) werden geleert. Die Protokollierung beginnt dann mit den neuen Protokollumlaufbedingungen.

Wenn Sie vom Protokollumlauf (Option `shedlogmax`) zur Protokollbereinigung (Option `shedlogretention`) wechseln, werden alle vorhandenen Protokolleinträge aufbewahrt, und das Protokoll wird mit den neuen Kriterien von `shedlogretention` bereinigt. Die bereinigten Einträge werden in den entsprechenden *.pru-Dateien gespeichert.

Wird weder `shedlogmax` noch `shedlogretention` angegeben, können die Protokolle uneingeschränkt wachsen. Sie müssen den Protokollinhalt manuell verwalten, um zu verhindern, dass das Protokoll die Plattenressourcen verbraucht. Wenn das Protokoll ohne eine der beiden Optionen erstellt wurde und wenn Sie später einen Befehl mit der Option `shedlogretention` ausgeben, wird das Protokoll mit dem angegebenen Wert für die Aufbewahrungsdauer bereinigt. Wenn das Protokoll ohne eine der beiden Optionen erstellt wurde und wenn Sie später einen Befehl mit der Option `shedlogmax` ausgeben, wird das vorhandene Protokoll als bereinigtes Protokoll behandelt. Das heißt, der Inhalt der Datei `dsmsched.log` wird in eine Datei mit dem Namen `dsmsched.pru` kopiert, der Inhalt der Datei `dsmwebcl.log` wird in `dsmwebcl.pru` kopiert und sowohl in `dsmsched.log` als auch in `dsmwebcl.log` werden neue Protokolleinträge erstellt. In beiden Dateien findet ein Umlauf statt, wenn sie ihre maximale Größe erreichen.

Anmerkung: Wenn Sie die Option `shedlogretention` angeben, um bereinigte Protokolle zu erstellen, können Sie die Option `shedlogmax` nicht angeben. Für Protokolle kann entweder eine Bereinigung oder ein Umlauf durchgeführt werden, aber nicht beides.

Unterstützte Clients

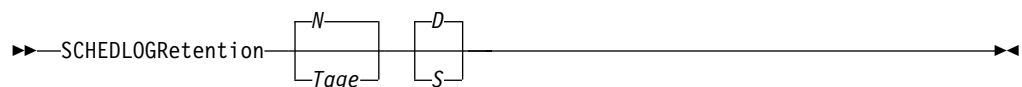
Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein.

Sie können diese Option auch auf der Registerkarte **Clientvorgaben > Scheduler** in der grafischen Benutzerschnittstelle definieren. Wählen Sie hierfür **Alte Einträge bereinigen** aus und geben Sie einen Wert für **Einträge bereinigen, die älter sind als** an. Durch Auswahl der Option **Bereinigte Einträge sichern** werden die bereinigten Schedulerprotokolleinträge in der Protokolldatei `dsmsched.pru` gespeichert. Durch die Auswahl von **Bereinigte Einträge sichern** werden außerdem die Protokolleinträge des Web-Clients in der Protokolldatei `dsmwebcl.pru` gespeichert.

Syntax



Parameter

N oder *Tage*

Gibt die Wartezeit vor dem Bereinigen des Protokolls an.

N Das Protokoll nicht bereinigen. Das Protokoll kann unendlich groß werden. Dies ist der Standardwert.

Tage

Gibt die Anzahl Tage an, die Protokolldateieinträge vor dem Bereinigen aufbewahrt werden sollen. Der Wertebereich ist 0 bis 9999.

D oder *S*

Gibt an, ob bereinigte Einträge gesichert werden sollen. Ein Leerzeichen oder ein Komma verwenden, um diesen Parameter vom vorherigen zu trennen.

D Löscht die Protokolleinträge, wenn das Protokoll bereinigt wird. Dies ist der Standardwert.

S Sichert die Protokolleinträge, wenn das Protokoll bereinigt wird.

Bereinigte Einträge werden in die Datei der bereinigten Einträge (dsmsched.pru oder dsmsched.pru) kopiert, die in demselben Verzeichnis gespeichert ist wie das Protokoll.

Beispiele

Optionsdatei:

```
schedlogretention 30 S
```

Befehlszeile:

```
-schedlogretention=30,S
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Schedmode

Mit der Option schedmode kann angegeben werden, ob der Modus Polling (Clientsendeaufwurf: der Clientknoten fragt den Server regelmäßig nach geplanter Arbeit) oder der Modus Prompted (Servergesteuerte Ausführung: der Server stellt eine Verbindung zum Clientknoten her, wenn eine geplante Operation gestartet werden muss) verwendet werden soll.

'Polling' (Clientsendeaufwurf) kann für alle Übertragungsmethoden verwendet werden, 'Prompted' (Servergesteuerte Ausführung) jedoch nur für TCP/IP.

Diese Option ist nur gültig, wenn Sie die TCP/IP-Übertragungsmethode verwenden und der Befehl **schedule** aktiv ist.

Der Administrator kann angeben, dass der Server beide Modi oder nur einen Modus unterstützt. Gibt der Administrator an, dass beide Modi unterstützt werden, können Sie einen der beiden Planungsmodi auswählen. Gibt der Administrator nur einen Modus an, müssen Sie diesen Modus in Ihrer Datei dsm.sys angeben, damit geplante Arbeit verarbeitet wird.

Wenn Sie den Modus prompted angeben, empfiehlt es sich, Werte für die Optionen tcpclientaddress und tcpclientport in Ihrer Datei dsm.sys oder im Befehl schedule anzugeben; der Client kann dann entweder an einer Adresse oder an einem Anschluss Ihrer Wahl kontaktiert werden (nützlich für Clientsysteme mit mehreren Netzschnittstellenkarten).

Anmerkung:

1. Wenn Sie die Einstellung dieser Option in der Datei dsm.sys ändern, müssen Sie den Scheduler-Service stoppen und erneut starten, damit die Einstellung wirksam wird.
2. Diese Option kann auch auf dem Server definiert werden.

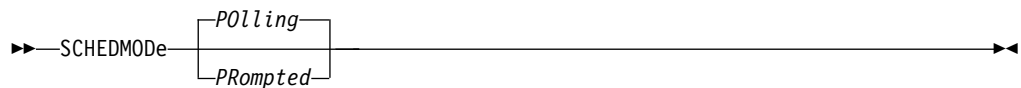
Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Scheduler** im Abschnitt **Planungsmodus** im Profileditor definieren.

Syntax



Parameter

POLLing

Der Client-Scheduler fragt den Server in festgelegten Zeitintervallen nach geplanter Arbeit ab. Dies ist der Standardwert. Die Zeitintervalle werden mit der Option `querryschedperiod` festgelegt.

PRompted

Der Client-Scheduler wartet, bis der Server eine Verbindung zum Clientknoten herstellt, wenn geplante Arbeit ausgeführt werden muss.

Anmerkung:

1. Wenn Sie den Befehl **dsmc schedule** verwenden und sowohl `schedmode prompted` als auch `commethod V6Tcpip` angegeben sind, müssen der Client und der IBM Spectrum Protect-Server für IPv6 konfiguriert sein. Darüber hinaus muss der Client-Hostname für die IPv6-Adresse definiert sein.

Beispiele

Optionsdatei:

```
schedmode prompted
```

Befehlszeile:

```
-schedmod=po
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Zugehörige Verweise:

„Cadlistenonport“ auf Seite 372

„Tcpclientaddress“ auf Seite 611

„Tcpclientport“ auf Seite 612

Schedrestretrdisabled

Die Option `schedrestretrdisabled` gibt an, ob die Ausführung von Zurückschreibungs- oder Abrufplanungsoperationen inaktiviert werden soll.

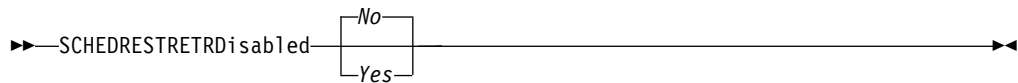
Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann nicht auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Datei `dsm.sys` innerhalb einer Serverzeilengruppe für den Scheduler ein. Sie können diese Option auf der Registerkarte **Scheduler** im Abschnitt **Befehl für Zeitplan** im Profileditor definieren.

Syntax



Parameter

No Gibt an, dass der Client die Ausführung von Zurückschreibungs- und Abrufplanungsoperationen nicht inaktiviert. Dieser Parameter ist der Standardwert.

Yes

Gibt an, dass der Client die Ausführung von Zurückschreibungs- und Abrufplanungsoperationen inaktiviert.

Beispiele

Optionsdatei:

```
schedrestretrdisabled yes
```

Befehlszeile:

Nicht zutreffend.

Scrolllines

Mit der Option `scrolllines` wird die Anzahl Datenzeilen angegeben, die gleichzeitig auf dem Bildschirm angezeigt werden.

Verwenden Sie diese Option, wenn Sie die Option `scrollprompt` auf *Yes* setzen.

Die Option `scrolllines` können Sie nur mit den folgenden Befehlen verwenden:

- **delete filespace**
- **query archive**
- **query backup**
- **query backupset**
- **query filespace**
- **query group**
- **query image**
- **query nas**
- **query node**
- **query options**

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein. Sie können diese Option im Feld **Befehlszeile > Anzahl Zeilen, die angezeigt werden sollen** im Profileditor definieren.

Syntax

►—SCROLLLines— *Nummer* —►

Parameter

Zahl

Gibt die Anzahl Datenzeilen an, die gleichzeitig auf dem Bildschirm angezeigt werden. Der Wertebereich ist 1 bis 80; Standardwert ist 20.

Beispiele

Optionsdatei:

scrolllines 25

Befehlszeile:

-scroll=25

Diese Option ist in der Anfangsbefehlszeile und im interaktiven Modus gültig. Wird die Option im interaktiven Modus eingegeben, ist nur der Befehl betroffen, mit dem sie eingegeben wird. Wenn dieser Befehl beendet ist, wird der Wert auf den Wert zu Beginn der interaktiven Sitzung zurückgesetzt. Dies ist der Wert aus der Datei dsm.opt, sofern er nicht durch die Anfangsbefehlszeile oder eine vom Server erzwungene Option überschrieben wurde.

Scrollprompt

Die Option scrollprompt gibt an, ob der Client für Sichern/Archivieren nach dem Anzeigen der Anzahl Datenzeilen, die Sie in der Option scrolllines angegeben haben, stoppen und warten soll oder ob er alle Zeilen durchblättern und am Ende der Datenliste stoppen soll.

Die Option scrollprompt können Sie nur mit den folgenden Befehlen verwenden:

- delete filespace
- query archive
- query backup
- query backupset
- query filespace
- query group
- query image
- query nas
- query node
- query options

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte **Befehlszeile** im Feld **Nach dem Anzeigen der folgenden Anzahl Zeilen anhalten** definieren.

Syntax



Parameter

No Bis zum Ende der Liste blättern und stoppen. Dies ist der Standardwert.

Yes

Nach dem Anzeigen der Anzahl Zeilen, die in der Option `scrolllines` angegeben wird, stoppen und warten. Die folgende Bedienerführung wird angezeigt:

Zum Verlassen 'Q', für fortlaufendes Blättern 'C' oder zum Fortfahren 'Eingabe' drücken.

Beispiele

Optionsdatei:

```
scrollprompt yes
```

Befehlszeile:

```
-scrollp=yes
```

Diese Option ist in der Anfangsbefehlszeile und im interaktiven Modus gültig. Wird die Option im interaktiven Modus eingegeben, ist nur der Befehl betroffen, mit dem sie eingegeben wird. Wenn dieser Befehl beendet ist, wird der Wert auf den Wert zu Beginn der interaktiven Sitzung zurückgesetzt. Dies ist der Wert aus der Datei `dsm.opt`, sofern er nicht durch die Anfangsbefehlszeile oder eine vom Server erzwungene Option überschrieben wurde.

Servername

In Ihrer Datei `dsm.sys` gibt die Option `servername` den Namen an, den Sie für die Identifikation eines Servers und am Anfang einer Zeilengruppe mit Optionen für diesen Server verwenden wollen. Es können mehrere Server benannt und Optionen für sie angegeben werden.

Das folgende Beispiel zeigt, wie Optionen für zwei unterschiedliche Server angegeben werden:

```

SErvername      server_a
COMMMethod      TCPip
TCPPort         1500
TCPServeraddress server_hostname2.domain.company.com
PASSWORDAccess  prompt
GRoups          tsm
USERS           sullivan mushock tallan
INCLExcl        /adm/tsm/backup.excl

SErvername      server_b
COMMMethod      SHAREdmem
shmport         1520
PASSWORDAccess  generate
GRoups          system tsm
INCLExcl        /adm/tsm/archive.excl

```

In Ihrer Clientbenutzeroptionsdatei (dsm.opt) gibt die Option `servername` an, zu welchem der in Ihrer Datei `dsm.sys` genannten Server zwecks Sicherungs-/Archivierungsservices der Kontakt hergestellt werden soll. Wird die Option `servername` in einer Clientbenutzeroptionsdatei (dsm.opt) oder in der Befehlszeile angegeben, überschreibt sie den Standardserver, der in Ihrer Clientsystemoptionsdatei angegeben ist.

Anmerkung:

1. Der Server, der in der Clientsystemoptionsdatei für die Umlagerung angegeben ist, kann mit der Option `servername` nicht überschrieben werden.
2. Wenn sich der Name des IBM Spectrum Protect-Servers ändert oder Clients für Sichern/Archivieren zu einem anderen IBM Spectrum Protect-Server geleitet werden, muss für alle Clients ein neues Kennwort für den neuen Servernamen initialisiert werden.

Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) und in die Clientsystemoptionsdatei (dsm.sys) ein. In der Datei `dsm.sys` bildet die Option `servername` den Anfang einer Serverzeilengruppe.

Ändern Sie diese Option nicht in `dsm.opt`, wenn Sie den Client für Sichern/Archivieren in einer Befehlszeilensitzung ausführen oder wenn Sie die grafische Benutzerschnittstelle des Clients für Sichern/Archivieren ausführen.

Syntax

►►—SErvername— —Servername—►►

Parameter

Servername

Geben Sie in Ihrer Datei `dsm.sys` den Namen an, der einem bestimmten Server zugeordnet werden soll. Geben Sie in Ihrer Clientbenutzeroptionsdatei (dsm.opt) oder in der Befehlszeile den Namen des Servers an, zu dem zwecks Sicherungs-/Archivierungsservices der Kontakt hergestellt werden soll. Der

Wert von *Servername* in dsm.opt muss einem *Servername*-Wert in dsm.sys entsprechen. Andernfalls kann der Client keinen Kontakt zum Server herstellen.

Ein Servername ist nicht von der Groß-/Kleinschreibung abhängig; er kann bis zu 64 Zeichen haben.

Beispiele

Optionsdatei:

```
servername server_a
```

Befehlszeile:

```
-se=server_b
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Sessioninitiation

Verwenden Sie die Option *sessioninitiation*, um zu steuern, ob der Server oder der Client Sitzungen durch eine Firewall einleiten soll. Standardwert ist, dass der Client Sitzungen einleitet. Sie können diese Option im Befehl **schedule** verwenden.

Für den Client-Scheduler ist es nicht erforderlich, Anschlüsse in der Firewall zu öffnen. Wenn Sie die Option *sessioninitiation* auf *serveronly* setzen, versucht der Client nicht, Kontakt zum Server aufzunehmen. Alle Sitzungen müssen durch die Zeitplanung über Serversystemanfrage an dem mit der Option *tcpclientport* auf dem Client definierten Anschluss eingeleitet werden. Die Option *sessioninitiation* beeinflusst nur das Verhalten des Client-Schedulers, der im Modus mit Bedienerführung ausgeführt wird. Wenn Sie die Option *sessioninitiation* auf *serveronly* setzen, versuchen der Befehlszeilenclient und die GUI des Clients für Sichern/Archivieren - mit Ausnahme der Scheduler, die vom Clientakzeptordämon verwaltet werden - dennoch, Sitzungen einzuleiten.

Achtung: Sie können den **dsmcad** nicht für die Planung verwenden, wenn Sie die Option *sessioninitiation* auf *serveronly* setzen.

Anmerkung: Wenn Sie die Option *sessioninitiation* auf *serveronly* setzen, sind der Client-Setup-Assistent und der Scheduler-Service nicht in der Lage, sich beim IBM Spectrum Protect-Server zu authentifizieren. In diesem Fall können Sie den Scheduler von der Befehlszeile aus ausführen (**dsmc schedule**) und bei der entsprechenden Aufforderung das Kennwort für Ihren Knoten eingeben.

Ein ähnliches Problem kann auftreten, wenn ein Chiffrierschlüssel für Sicherungsoperationen erforderlich ist. In diesem Fall können Sie den Scheduler von der Befehlszeile aus ausführen (**dsmc schedule**) und den Chiffrierschlüssel eingeben, wenn Sie dazu aufgefordert werden. Nachdem das Kennwort und der Chiffrierschlüssel aktualisiert worden sind, müssen Sie den Scheduler erneut starten.

Wenn Sie die Option *sessioninitiation* auf *client* setzen, leitet der Client Sitzungen mit dem Server ein, indem er über den TCP/IP-Anschluss kommuniziert, der durch die Serveroption *tcpport* definiert ist. Dies ist der Standardwert. Mit der Zeitplanung über Serversystemanfrage kann der Client dazu aufgefordert werden, eine Verbindung zum Server herzustellen.

Anmerkung:

1. Der IBM Spectrum Protect-Server kann **SESSIONINITiation=clientorserver** oder **SESSIONINITiation=serveronly** in den Befehlen **register node** und **update**

node angeben. Wenn der Server SESSIONINITiation=clientorserver angibt, kann der Client entscheiden, welche Methode verwendet werden soll. Wenn der Server SESSIONINITiation=serveronly angibt, werden alle Sitzungen vom Server eingeleitet.

2. Wird sessioninitiation auf serveronly gesetzt, muss der Wert für die Clientoption tcpclientaddress mit dem Wert für die Option HAddress im Serverbefehl **update node** oder **register node** übereinstimmen. Der Wert für die Clientoption tcpclientport muss mit dem Wert für die Option LAddress im Serverbefehl **update node** oder **register node** übereinstimmen.

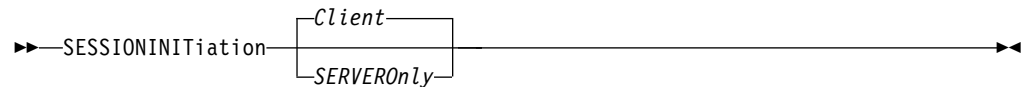
Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Scheduler** im Feld **Sitzungsstart** im Profileditor definieren.

Syntax



Parameter

Client

Gibt an, dass der Client Sitzungen mit dem Server einleitet, indem er über den TCP/IP-Anschluss kommuniziert, der durch die Serveroption TCPPORT definiert ist. Dies ist der Standardwert. Mit der Zeitplanung über Serversystemanfrage kann der Client dazu aufgefordert werden, 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 mit der Option tcpclientport auf dem Client definierten Anschluss eingeleitet werden. Mit Ausnahme der Scheduler, die vom Clientakzeptordämon verwaltet werden, versuchen der Befehlszeilenclient und die GUI des Clients für Sichern/Archivieren dennoch, Sitzungen einzuleiten.

Wenn die Serveroption AUTHENTICATION auf LDAP gesetzt ist, geben Sie für die Clientoption sessioninitiation nicht serveronly an; andernfalls können keine Zeitpläne ausgeführt werden.

Beispiele

Optionsdatei:

```
sessioninitiation serveronly
```

Befehlszeile:

```
schedule -sessioninitiation=serveronly
```

- | Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist
- | sie nicht gültig.
- | Zugehörige Informationen
- | „Scheduler konfigurieren“ auf Seite 69
- | „Tcpclientport“ auf Seite 612

Setwindowtitle

Verwenden Sie die Option `setwindowtitle`, um den Titel des Befehlsfensters für den Verwaltungsclient während der Verarbeitung zu ändern.

Wenn Sie beispielsweise den Befehl des Verwaltungsclients (**dsmadmc**) auf dem Clientknoten ausführen und der Verwaltungsclient die Verbindung zum IBM Spectrum Protect-Server herstellt, wird im Titel des Befehlsfensters der folgende Text angezeigt:

VERBUNDEN MIT SERVER: *Servername(Server-Hostname)*

Dabei ist *Servername* der Name des IBM Spectrum Protect-Servers und *Server-Hostname* der Hostname des IBM Spectrum Protect-Servers.

Wenn Sie die Option `setwindowtitle` verwenden, wird jeder benutzerdefinierte Titel des Befehlsfensters überschrieben. Nachdem die Verbindung zwischen dem Verwaltungsclient und dem IBM Spectrum Protect-Server getrennt wurde, wird der Fenstertitel auf den benutzerdefinierten Fenstertitel zurückgesetzt.

Unter AIX-, Linux- und Oracle Solaris-Betriebssystemen wird der Titel des Terminalfensters auf den Titel "Terminal" zurückgesetzt, nachdem die Verbindung zum Server getrennt wurde.

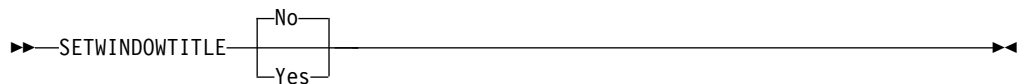
Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (`dsm.opt`) oder die Client-systemoptionsdatei (`dsm.sys`) ein.

Syntax



Parameter

No Der Titel des Befehlsfensters für den Verwaltungsclient wird während der Verarbeitung nicht geändert. Dieser Parameter ist der Standardwert.

Yes

Der IBM Spectrum Protect-Servername und der Host-Server-Name werden im Titel des Befehlsfensters für den Verwaltungsclient angezeigt.

Beispiele

Optionsdatei:

```
SETWINDOWTITLE YES
```

Befehlszeile:

```
-setwindowtitle=yes
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Shmport

Die Option `shmport` gibt die TCP/IP-Anschlussadresse eines Servers an, wenn gemeinsam genutzter Speicher verwendet wird. Alle Übertragungen mit gemeinsam genutztem Speicher starten mit einer TCP/IP-Verbindung.

Anmerkung: Der für die Option `shmport` in der Datei `dsm.sys` angegebene Wert muss mit dem Wert übereinstimmen, der für `shmport` in der Serveroptionsdatei angegeben ist.

Unterstützte Clients

Diese Option ist für AIX-, Linux- und Oracle Solaris-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein.

Syntax

►►—SHMPort— —Anschlussnummer—◄◄

Parameter

Anschlussnummer

Gibt die Anschlussnummer an. Sie können einen Wert zwischen 1000 und 32767 angeben. Der Standardwert ist 1510.

Beispiele

Optionsdatei:

```
shmport 1580
```

Befehlszeile:

Nicht zutreffend.

Showmembers

Verwenden Sie die Option `showmembers`, um alle Member einer Gruppe anzuzeigen.

Sie können die Option `showmembers` in den Befehlen **query group** und **restore group** verwenden.

Die Option `showmembers` ist mit der Option `inactive` nicht gültig. Um Member in einer Gruppe anzuzeigen, die zurzeit nicht aktiv sind, die Optionen `pitdate` und `pittime` verwenden.

Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients außer Mac OS X gültig.

Syntax

►—SHOWMembers—►

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
restore group /virtfs/* -pick -showmembers
```

Skipacl

Mit der Option `skipacl` können Sie ACL-Daten während einer Sicherungs- oder Archivierungsoperation einschließen oder ausschließen (ACL = Access Control List, Zugriffssteuerungsliste). ACL-Daten werden standardmäßig eingeschlossen.

Wenn diese Option auf `yes` gesetzt ist, schließt der Client für Sichern/Archivieren bei der Sicherung oder Archivierung von Dateien und Verzeichnissen keine ACL-Daten ein. Der Standardwert ist `no`. Dadurch ist es möglich, die ACL-Daten beim Kopieren von Objekten auf den Server einzuschließen. Sie sollten die Option `skipacl` nur dann auf `yes` setzen, wenn im Dateisystem keine Zugriffssteuerungslisten definiert sind oder wenn Sie sicher sind, dass Sie die ACL-Daten nicht benötigen, wenn die Dateien abgerufen oder zurückgeschrieben werden.

Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients gültig. Wenn `skipacl` auf Linux- und AIX-Systemen auf `yes` gesetzt wird, werden auch die erweiterten Attribute übergangen.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (`dsm.opt`) ein.

Syntax

►—SKIPACL—
No
Yes

Parameter

No Bei der Angabe *No* werden die ACL-Daten gesichert. Dies ist der Standardwert.

Yes

Bei der Angabe *Yes* werden die ACL-Daten nicht gesichert und können folglich nicht zurückgeschrieben werden. `skipacl=yes` überschreibt die Einstellungen für `skipaclupdatecheck`.

Beispiele

Optionsdatei:
skipacl yes

Skipaclupdatecheck

Die Option skipaclupdatecheck inaktiviert Kontrollsummen- und Größenvergleiche von ACL-Daten.

Wird diese Option auf yes gesetzt (der Standardwert ist no), führt der Client für Sichern/Archivieren vor oder nach einer Sicherung und während der Teilsicherungsverarbeitung (ACL-Kontrollsumme von vorheriger Sicherung und aktueller ACL) keine Kontrollsummen- und Größenvergleiche durch, um ACL-Aktualisierungen zu ermitteln. Aktuelle ACL-Daten werden jedoch gesichert, wenn die Datei aus anderen Gründen zum Sichern ausgewählt wird. Werden nur die ACLs für eine Datei aktualisiert, wird bei der nächsten Teilsicherung diese ACL-Aktualisierung nicht erkannt und die Datei wird nicht gesichert.

Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients gültig.

Optionsdatei

Fügen Sie diese Option in in die Clientbenutzeroptionsdatei (dsm.opt) ein.

Syntax



Parameter

No Wenn Sie No angeben, führt der Client vor und nach einer Sicherung und während der Teilsicherungsverarbeitung Kontrollsummen- und Größenvergleiche der ACL-Daten durch. Dies ist der Standardwert.

Yes Wenn Sie Yes angeben, führt der Client keine Kontrollsummen- und Größenvergleiche der ACL-Daten durch.

Beispiele

Optionsdatei:
skipaclup yes

Snapdiff

Die Verwendung der Option snapdiff (Momentaufnahmedifferenz) mit dem Befehl **incremental** optimiert den Teilsicherungsprozess. Der Befehl führt eine Teilsicherung der Dateien aus, die von NetApp als geändert zurückgemeldet wurden, und durchsucht nicht den gesamten Datenträger nach geänderten Dateien.

Die Option snapdiff wird für das Sichern der Datenträger von NAS-/N-Series-Dateiservern verwendet, die über NFS angeschlossen sind.

Sie müssen eine Benutzer-ID und ein Kennwort auf dem Client für Sichern/ Archivieren konfigurieren, um die Momentaufnahmedifferenzverarbeitung zu aktivieren. Weitere Informationen zum Definieren der Option `snappdiff` befinden sich in „NetApp und IBM Spectrum Protect für Teilsicherungen unter Verwendung der Momentaufnahmedifferenz konfigurieren“ auf Seite 119.

Verwenden Sie diese Option bei einer Teilsicherung eines Datenträgers eines NAS-Dateiservers anstelle einer einfachen Teilsicherung oder einer Teilsicherung mit der Option `snapshotroot`, wenn auf dem NAS-Dateiserver ONTAP 7.3.0 oder höher ausgeführt wird. Verwenden Sie die Optionen `snappdiff` und `snapshotroot` nicht zusammen.

Einschränkung: Teilsicherungen mit Momentaufnahmedifferenzverarbeitung sind nur für den Linux x86_64-Client für Sichern/ Archivieren verfügbar.

Bei der ersten Ausführung einer Teilsicherung mit der Option für die Momentaufnahmedifferenz wird eine Momentaufnahme (die Basismomentaufnahme) erstellt und eine traditionelle Teilsicherung ausgeführt, wobei diese Momentaufnahme als Quelle verwendet wird. Der Name der erstellten Momentaufnahme wird in der IBM Spectrum Protect-Serverdatenbank aufgezeichnet. Die erste Teilsicherung muss fehlerfrei ausgeführt werden, damit bei der nächsten Sicherungsoperation die Momentaufnahmedifferenzverarbeitung verwendet werden kann.

Bei der zweiten Ausführung einer Teilsicherung mit dieser Option wird entweder eine neue Momentaufnahme erstellt oder eine vorhandene Momentaufnahme verwendet (abhängig vom Wert für die Option `diffsnapshot`), um die Unterschiede zwischen diesen beiden Momentaufnahmen zu ermitteln. Die zweite Momentaufnahme wird als *diffsnapshot* (Differenzmomentaufnahme) bezeichnet. Anschließend sichert der Client die Dateien, die von NetApp als geändert aufgelistet werden, über eine Teilsicherung auf dem IBM Spectrum Protect-Server. Das Dateisystem, das für die Momentaufnahmedifferenzverarbeitung ausgewählt wird, muss an das Stammverzeichnis des Datenträgers angehängt sein. Sie können die Option `snappdiff` nicht für Dateisysteme verwenden, die nicht an das Stammverzeichnis des Datenträgers angehängt sind. Nach der Sicherung der Daten mit der Option `snappdiff` wird die Momentaufnahme, die als Basismomentaufnahme verwendet wurde, aus dem Momentaufnahmeverzeichnis gelöscht.

Auf Linux-Systemen befindet sich das Momentaufnahmeverzeichnis in `.snapshot`.

Der Client löscht nur Momentaufnahmen, die er selbst erstellt hat.

Wenn eine Teilsicherungsoperation unter Verwendung der Momentaufnahmedifferenz beendet wird, stellt der Client sicher, dass nur die zuletzt registrierte Basismomentaufnahme auf dem Dateiserverdatenträger verbleibt. Alle Momentaufnahmen, die durch eine Momentaufnahmedifferenzteilsicherung auf dem Client für Sichern/ Archivieren erstellt werden, beginnen mit den Zeichen "TSM_". Wenn Sie Momentaufnahmen mit einem anderen Momentaufnahme-Tool als dem Client für Sichern/ Archivieren erstellen, müssen Sie sicherstellen, dass nicht die Zeichenfolge "TSM_" am Anfang des Momentaufnahmenamens verwendet wird. Wenn die Momentaufnahmenamen mit "TSM_" beginnen, werden die Dateien gelöscht, wenn der Client die nächste Teilsicherungsoperation unter Verwendung der Momentaufnahmedifferenz einleitet.

Um eine Momentaufnahmedifferenzteilsicherung von schreibgeschützten NetApp-Dateiserverdatenträgern auszuführen, muss die Option `useexistingbase` angegeben werden, um zu verhindern, dass eine Momentaufnahme auf dem schreibgeschütz-

ten Datenträger erstellt wird. Geben Sie außerdem den Namen der zu verwendenden Basismomentaufnahme (Option `basesnapshotname`) und den Namen der zu verwendenden Differenzmomentaufnahme (Option `diffsnapshotname`) an.

Bei NAS- und N-Series-Dateiservern, auf denen ONTAP 7.3.0 oder höher ausgeführt wird, können Sie die Option `createnewbase` verwenden, um alle Dateien zu sichern, die aufgrund einer der folgenden Ursachen übersprungen wurden:

- Eine Datei wird ausgeschlossen, da die Einschluss-/Ausschlussdatei über eine Ausschlussregel verfügt, die wirksam ist. Eine Datei wird ausgeschlossen, wenn Sie die Einschluss-/Ausschlussdatei nicht geändert, aber die Regel entfernt haben, die die Datei ausgeschlossen hat. Die NetApp-API erkennt nur Dateiänderungen zwischen zwei Momentaufnahmen, aber keine Änderungen an der Einschluss-/Ausschlussdatei.
- Wenn Sie der Optionsdatei eine Einschlussanweisung hinzugefügt haben, tritt diese Einschlussoption erst in Kraft, wenn NetApp feststellt, dass die Datei sich geändert hat. Der Client überprüft während einer Sicherung nicht jede Datei auf dem Datenträger.
- Sie haben mit dem Befehl **`dsmdc delete backup`** explizit eine Datei aus dem IBM Spectrum Protect-Serverbestand gelöscht. NetApp erkennt nicht, dass eine Datei manuell auf dem Server gelöscht wurde. Daher verbleibt die Datei ungeschützt im IBM Spectrum Protect-Speicher, bis sie auf dem Datenträger geändert wird, diese Änderung von NetApp festgestellt wird und der Client angewiesen wird, die Datei erneut zu sichern.
- Maßnahmenänderungen wie die Änderung der Maßnahme von `mode=modified` in `mode=absolute` werden nicht festgestellt.
- Der gesamte Dateibereich wird aus dem IBM Spectrum Protect-Datenbestand gelöscht. Diese Aktion bewirkt, dass die Option für die Momentaufnahmedifferenz eine Momentaufnahme erstellt, die als Quelle verwendet wird, und dass eine vollständige Teilsicherung ausgeführt wird.
- Eine Datei wird von der Sicherung ausgeschlossen, da der Dateiname ein Zeichen enthält, das im 7-Bit-ASCII-Zeichensatz nicht enthalten ist. Die Option `createnewbase` erstellt eine Basismomentaufnahme und verwendet sie als Quelle für die Ausführung einer vollständigen Teilsicherung. NetApp steuert, was als geändertes Objekt angesehen wird.

Tipp: Sie können mit der Option `snappdiffhttps` Momentaufnahmedifferenzteilsicherungen von NetApp-Dateiservern mit einer sicheren HTTPS-Verbindung ausführen. Damit Momentaufnahmedifferenzteilsicherungen erfolgreich ausgeführt werden konnten, musste in früheren Releases des Clients für Sichern/Archivieren HTTP-Verwaltungszugriff auf dem NetApp-Dateiserver aktiviert sein. Mit der Option `snappdiffhttps` können Sie eine sichere Verwaltungssitzung mit dem NetApp-Dateiserver aufbauen, ohne dass hierfür der HTTP-Verwaltungszugriff auf dem Dateiserver aktiviert sein muss.

Momentaufnahmedifferenzsicherungsoperationen werden in der IBM Spectrum Protect for Virtual Environments-Umgebung nicht unterstützt. Sie können keine Momentaufnahmedifferenzsicherungsoperationen für ein Dateisystem ausführen, das sich auf einem NetApp-Dateiserver auf einem Host befindet, auf dem auch die Einheit zum Versetzen von Daten von Data Protection for VMware oder Data Protection for Microsoft Hyper-V installiert ist.

In der Liste der vom traditionellen Befehl **`incremental`** verwendeten Optionen zeigt die letzte Spalte die Interaktion jeder Option mit der Option `snappdiff` an. Die Definitionen der Begriffe *gültig*, *nicht gültig* und *keine Auswirkung* lauten wie folgt:

Gültig Die Verarbeitung verläuft normal, wenn die Option verwendet wird.

Nicht gültig

Wird die Option mit der Option snapdiff verwendet, wird eine Fehler-
nachricht generiert.

Keine Auswirkung

Die Option kann verwendet werden; sie wird jedoch ignoriert.

Tabelle 76. Befehl Incremental: Zugehörige Optionen

Option	Verwendung	Mit snapdiff
asnodename „Asnodename“ auf Seite 359	Clientsystemoptionsdatei (dsm.sys) oder Befehlszeile.	Gültig
automount „Automount“ auf Seite 368	Clientoptionsdatei (dsm.opt).	Keine Auswirkung
basesnapshotname „Basesnapshotname“ auf Seite 371	Clientoptionsdatei (dsm.opt) oder Befehlszeile.	Gültig
changingretries „Changingretries“ auf Seite 373	Clientsystemoptionsdatei (dsm.sys) oder Befehlszeile.	Keine Auswirkung
compressalways „Compressalways“ auf Seite 379	Clientoptionsdatei (dsm.opt) oder Befehlszeile.	Gültig
compression „Compression“ auf Seite 380	Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe oder Befehlszeile.	Gültig
createnewbase „Createnewbase“ auf Seite 383	Nur in der Befehlszeile.	Gültig
diffsnapshot „Diffsnapshot“ auf Seite 400	Nur in der Befehlszeile.	Gültig
diffsnapshotname „Diffsnapshotname“ auf Seite 401	Clientoptionsdatei (dsm.opt) oder Befehlszeile.	Gültig
dirsonly „Dirsonly“ auf Seite 403	Nur in der Befehlszeile.	Gültig
domain „Domain“ auf Seite 407	Clientsystemoptionsdatei (dsm.sys), Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.	Gültig
efsdecrypt „Efsdecrypt“ auf Seite 424	Clientsystemoptionsdatei (dsm.sys), Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.	Keine Auswirkung
enablelanfree „Enablelanfree“ auf Seite 429	Clientsystemoptionsdatei (dsm.sys) oder Befehlszeile.	Gültig
encryptiontype „Encryptiontype“ auf Seite 431	Systemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe.	Gültig
encryptkey „Encryptkey“ auf Seite 431	Systemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe.	Gültig
exclude.fs.nas „Exclude-Optionen“ auf Seite 438	Clientsystemoptionsdatei (dsm.sys).	Keine Auswirkung
filelist „Filelist“ auf Seite 453	Nur in der Befehlszeile.	Nicht gültig
filesonly „Filesonly“ auf Seite 457	Nur in der Befehlszeile.	Gültig

Tabelle 76. Befehl Incremental: Zugehörige Optionen (Forts.)

Option	Verwendung	Mit snapdiff
followsymboliclink „Followsymbolic“ auf Seite 458	Clientoptionsdatei (dsm.opt).	Keine Auswirkung
include.fs.nas „Include-Optionen“ auf Seite 473	Clientsystemoptionsdatei (dsm.sys) oder Befehlszeile.	Keine Auswirkung
inlexcl „Inlexcl“ auf Seite 471	Clientsystemoptionsdatei (dsm.sys).	Gültig, jedoch nur, wenn NetApp eine Dateiänderung feststellt.
incrbydate „Incrbydate“ auf Seite 490	Nur in der Befehlszeile.	Nicht gültig
memoryefficientbackup „Memoryefficientbackup“ auf Seite 507	Diese Option ist sowohl in dsm.sys als auch in dsm.opt zulässig; der Wert in dsm.opt wird jedoch ignoriert, wenn die Option auch in dsm.sys vorhanden ist. Sie können diese Option auch innerhalb einer Serverzeilengruppe oder in der Anfangsbefehlszeile verwenden.	Keine Auswirkung
monitor „Monitor“ auf Seite 512	Nur in der Befehlszeile.	Nicht gültig
nojurnal „Nojournal“ auf Seite 519	Nur in der Befehlszeile.	Nicht gültig
postsnapshotcmd „Postsnapshotcmd“ auf Seite 533	Clientsystemoptionsdatei (dsm.sys) oder mit der Option include.fs.	Gültig
preservelastaccessdate „Preservelastaccessdate“ auf Seite 536	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.	Gültig
presnapshotcmd „Presnapshotcmd“ auf Seite 540	Clientsystemoptionsdatei (dsm.sys) oder mit der Option include.fs.	Gültig
removeoperandlimit „Removeoperandlimit“ auf Seite 546	Nur in der Befehlszeile.	Gültig
skipaclupdatecheck „Skipaclupdatecheck“ auf Seite 581	Clientoptionsdatei (dsm.opt).	Gültig
snapdiffhttps „Snapdiffhttps“ auf Seite 588	Nur in der Befehlszeile.	Gültig
snapshotcachesize „Snapshotcachesize“ auf Seite 590	Clientsystemoptionsdatei (dsm.sys) oder mit der Option include.fs.	Keine Auswirkung
snapshotproviderfs „Snapshotproviderfs“ auf Seite 591	Systemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe oder mit der Option include.fs.	Nicht gültig
snapshotproviderimage „Snapshotproviderimage“ auf Seite 592	Clientsystemoptionsdatei (dsm.sys) oder mit der Option include.image.	Nicht gültig
snapshotroot „Snapshotroot“ auf Seite 593	Nur in der Befehlszeile.	Nicht gültig
subdir „Subdir“ auf Seite 605	Clientoptionsdatei (dsm.opt) oder Befehlszeile.	Nicht gültig

Tabelle 76. Befehl *Incremental*: Zugehörige Optionen (Forts.)

Option	Verwendung	Mit snapdiff
tapeprompt „Tapeprompt“ auf Seite 607	Clientoptionsdatei (dsm.opt) oder Befehlszeile.	Gültig
toc „Toc“ auf Seite 619	Nur in der Befehlszeile.	Nicht gültig
useexistingbase „Useexistingbase“ auf Seite 625	Nur in der Befehlszeile.	Gültig
virtualfsname „Virtualfsname“ auf Seite 630	Nur in der Befehlszeile.	Nicht gültig
virtualmountpoint „Virtualmountpoint“ auf Seite 630	Clientsystemoptionsdatei (dsm.sys).	Nicht gültig

Unterstützte Clients

Diese Option ist für Linux x86_64-Clients gültig.

Syntax

►►—SNAPDiff—◄◄

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

Eine Teilsicherung unter Verwendung der Momentaufnahmedifferenz für das über NFS-Mount angehängte Dateisystem /vol/vol1 ausführen, das sich auf dem Dateiserver homestore.example.com befindet. Dabei ist /net/home1 der Mountpunkt von /vol/vol1.

```
incremental -snapdiff -diffsnapshot=latest /net/home1
```

Befehlszeile:

Eine einmalige vollständige Teilsicherung ausführen, nachdem festgestellt wurde, dass der NetApp-Dateiserver von einer Version, die keine Unicode-Dateinamen unterstützt hat, auf einen Unicode-fähigen Dateiserver migriert wurde.

```
dsmc incremental -snapdiff -createnewbase=migrate /net/home1
```

Eine Teilsicherung unter Verwendung der Momentaufnahmedifferenz ausführen, nachdem festgestellt wurde, dass der NetApp-Dateiserver von einer Version, die keine Unicode-Dateinamen unterstützt hat, auf einen Unicode-fähigen Dateiserver migriert wurde. Dieser Befehl unterdrückt die Warnung.

```
dsmc incremental -snapdiff -createnewbase=ign /net/home1
```

Eine vollständige Teilsicherung ausführen, da einige Einschluss- oder Ausschlussänderungen vorgenommen wurden:

```
dsmc incremental -snapdiff -createnewbase=yes /net/home1
```

Zugehörige Konzepte:

„Momentaufnahmedifferenzsicherung mit einer HTTPS-Verbindung“ auf Seite 190

„SnapMirror-Unterstützung für momentaufnahmegestützte progressive Teilsicherung von NetApp (snapdiff)“ auf Seite 124

Zugehörige Tasks:

„NetApp und IBM Spectrum Protect für Teilsicherungen unter Verwendung der Momentaufnahmedifferenz konfigurieren“ auf Seite 119

Zugehörige Verweise:

„Snapdiffhttps“ auf Seite 588

„Basesnapshotname“ auf Seite 371

„Diffsnapshotname“ auf Seite 401

„Useexistingbase“ auf Seite 625

„Diffsnapshot“ auf Seite 400

„Set Password“ auf Seite 820

Snapdiffchangelogdir

Die Option `snapdiffchangelogdir` definiert die Position, an der der Client persistente Änderungsprotokolle speichert, die für Momentaufnahmedifferenzsicherungsoperationen verwendet werden.

Wichtig: Wenn Sie zuvor Momentaufnahmedifferenzsicherungen mit einem Client für Sichern/Archivieren einer älteren Version als Version 8.1.2 verwendet haben, ist die erste Momentaufnahmedifferenzsicherung, die Sie mit dem Client der Version 8.1.2 oder höher ausführen, eine progressive vollständige Teilsicherung. Um diese progressive vollständige Teilsicherung zu verhindern, versetzen Sie die vorhandenen Änderungsprotokolldateien von der alten Position, die durch die Option `stagingdirectory` angegeben wird, an die neue Position, die durch die Option `snapdiffchangelogdir` angegeben wird, bevor Sie die erste Momentaufnahmedifferenzsicherung ausführen.

Führen Sie beispielsweise den folgenden Kopierbefehl aus:

```
cp -R /tmp/TSM/TsmSnapDiff /opt/tivoli/tsm/client/ba/TsmSnapDiff
```

Die Änderungsprotokolldateien haben die folgenden Benennungsmuster:

```
.../TSM/TsmSnapDiff/.TsmSnapdiffChangeLogs/NetApp-Dateiserver/  
SnapdiffChangeLog__Datenträgername__.tsmDB  
.../TSM/TsmSnapDiff/.TsmSnapdiffChangeLogs/NetApp-Dateiserver/  
SnapdiffChangeLog__Datenträgername__.tsmDB.Lock
```

Hierbei gilt Folgendes:

- *NetApp-Dateiserver* ist der Hostname oder die IP-Adresse der Storage Virtual Machine (SVM) des Cluster-Management-Servers oder des 7-Mode-Dateiservers an.
- *Datenträgername* ist der Datenträger, der geschützt werden soll.

Unterstützte Clients

Diese Option ist für Linux x86_64-Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (`dsm.opt`) ein. Wird `snapdiffchangelogdir` in der Befehlszeile angegeben, überschreibt diese Angabe die Werte, die in der Optionsdatei angegeben sind. Sie können diese Option auf der Registerkarte **Allgemein** des Profileditors definieren.

Syntax

►—SNAPDIFFCHANGELOGDir—Pfad—◄

Parameter

Pfad

Gibt den Verzeichnispfad an, in dem der Client persistente Änderungsprotokolle für Momentaufnahmedifferenzsicherungsoperationen speichert. Wenn Sie die Option `snapdiffchangelogdir` nicht angeben, verwendet der Client das Verzeichnis, in dem der Client installiert ist. Das Standardinstallationsverzeichnis ist:

`/opt/tivoli/tsm/client/ba`

Der exakte Name der Änderungsprotokolldatei hat das folgende Format:

`Verzeichnis_des_Momentaufnahmedifferenzänderungsprotokolls/TsmSnapDiff/.TsmSnapdiffChangeLogs/NetApp-Dateiserver/SnapdiffChangeLog__Datenträgername__.tsmDB`

Hierbei gilt Folgendes:

- *Verzeichnis_des_Momentaufnahmedifferenzänderungsprotokolls* ist der Name des Verzeichnisses zum Speichern der Änderungsprotokolle für Momentaufnahmedifferenzsicherungen, das durch die Option `snapdiffchangelogdir` angegeben wird.
- *NetApp-Dateiserver* ist der Hostname oder die IP-Adresse der Storage Virtual Machine (SVM) des Cluster-Management-Servers oder des 7-Mode-Dateiservers an.
- *Datenträgername* ist der Datenträger, der geschützt werden soll.

Außerdem wird eine Sperrdatei erstellt, um zu verhindern, dass die Änderungsprotokolldatei durch unterschiedliche Momentaufnahmedifferenzsicherungen, die gleichzeitig ausgeführt werden, aktualisiert wird.

Beispiele

Optionsdatei:

`snapdiffchangelogdir /tmp/tsmdata`

Befehlszeile:

`-snapdiffchangelogd=/tmp/tsmdata`

Zugehörige Verweise:

„Diffsnapshot“ auf Seite 400

„Snapdiff“ auf Seite 581

Snapdiffhttps

Geben Sie die Option `snapdiffhttps` an, um eine sichere HTTPS-Verbindung für die Kommunikation mit einem NetApp-Dateiserver während einer Momentaufnahmedifferenzsicherung zu verwenden.

Wenn Sie diese Option angeben, kann der Client für Sichern/Archivieren eine sichere Verwaltungssitzung mit dem NetApp-Dateiserver aufbauen, ohne dass hierfür der HTTP-Verwaltungszugriff auf dem NetApp-Dateiserver aktiviert sein muss.

Wichtig: Das Standardübertragungsprotokoll, mit dem der Client für Sichern/Archivieren eine Verwaltungssitzung mit dem NetApp-Dateiserver aufbaut, ist

HTTP. Damit eine sichere HTTPS-Verbindung verwendet werden kann, müssen Sie die Option `snappdiffhttps` bei jeder Ausführung einer Momentaufnahmedifferenzsicherung angeben.

Einschränkungen:

Für Momentaufnahmedifferenzsicherungen mit HTTPS gelten die folgenden Einschränkungen:

- Die HTTPS-Verbindung wird nur für die sichere Übertragung von Daten über die Verwaltungssitzung zwischen dem Client für Sichern/Archivieren und dem NetApp-Dateiserver verwendet. Zu den Daten der Verwaltungssitzung gehören z. B. Berechtigungsnachweise des Dateiservers, Momentaufnahmeinformationen sowie Dateinamen und Attribute, die durch den Momentaufnahmedifferenzierungsprozess generiert werden. Über die HTTPS-Verbindung werden keine normalen Dateidaten übertragen, auf die der Client über die Dateifreigabe auf dem Dateiserver zugreift. Die HTTPS-Verbindung ist auch nicht für normale Dateidaten gültig, die der Client über das normale IBM Spectrum Protect-Client/Server-Protokoll an den IBM Spectrum Protect-Server überträgt.
- Die Option `snappdiffhttps` gilt nicht für vFilers, da das HTTPS-Protokoll auf dem NetApp vFiler nicht unterstützt wird.
- Die Option `snappdiffhttps` ist nur bei Verwendung der Befehlszeilenschnittstelle verfügbar. In der grafischen Benutzerschnittstelle (GUI) des Clients für Sichern/Archivieren kann sie nicht verwendet werden.

Unterstützte Clients

Diese Option ist für Linux x86_64-Clients gültig.

Optionsdatei

Diese Option ist nur in der Befehlszeilenschnittstelle gültig. Sie können sie nicht in einer Clientoptionsdatei angeben.

Syntax

►—SNAPDIFFHTTPS—◄

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

Geben Sie den folgenden Befehl auf einem Linux-System mit einem über NFS-Mount angehängten Dateisystem `/vol/vol1` aus, das sich auf dem Dateiserver `homestore.example.com` befindet; dabei ist `/net/home1` der Mountpunkt von `/vol/vol1`.

```
dsmc incr /net/home1 -snapdiff -snappdiffhttps
```

Zugehörige Konzepte:

„Momentaufnahmedifferenzsicherung mit einer HTTPS-Verbindung“ auf Seite 190

Zugehörige Verweise:

„Snapdiff“ auf Seite 581

Snapshotcachesize

Verwenden Sie die Option `snapshotcachesize`, um eine angemessene Cachegröße zum Erstellen der Momentaufnahme anzugeben.

Die geschätzte Größe muss ausreichen, um die Originaldatenblöcke für geänderte und gelöschte Daten für den Zeitpunkt zu speichern, zu dem die Momentaufnahme erstellt wurde.

Für eine Dateisicherung oder -archivierung auf Momentaufnahmebasis verwenden Sie die Option `snapshotcachesize` zusammen mit der Option `include.fs` oder in der Serverzeilengruppe der Datei `dsm.sys`.

Für Imagesicherungen auf Momentaufnahmebasis verwenden Sie die Option `snapshotcachesize` im Befehl **backup image**, mit der Option `include.image` oder in Ihrer Datei `dsm.sys`.

Unterstützte Clients

Diese Option ist *nur* für AIX- und Linux-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Serverzeilengruppe in der Datei `dsm.sys` ein. Sie können diese Option auf der Registerkarte **Momentaufnahmeimage** im Profileditor definieren.

Syntax

►►—SNAPSHOTCACHESize— Größe—►►

Parameter

Größe

Gibt eine entsprechende Momentaufnahmengröße zum Erstellen der Momentaufnahme an, damit die Originaldatenblöcke für geänderte und gelöschte Daten für den Zeitpunkt gespeichert werden können, als die Momentaufnahme erstellt wurde. Der Wert ist der Prozentsatz der Dateisystemgröße, die sich auf Grund der Dateisystemaktivität ändert. Der Wertebereich ist 1 bis 100 Prozent. Für AIX JFS2 und Linux beträgt der Standardwert 100 Prozent der Dateisystemgröße. Falls nicht genügend freier Speicherbereich verfügbar ist, um die Momentaufnahme zu erstellen, schlägt der Befehl mit einer Fehlermeldung fehl. Sie können dann entweder die Größe der Datenträgergruppe erhöhen oder die Operation wiederholen. Wenn Sie auf der Grundlage Ihrer Erfahrung mit der Aktivität des AIX JFS2-Dateisystems glauben, dass eine Momentaufnahmengröße von 100 Prozent nicht notwendig ist, können Sie den Wert optimieren.

Beispiele

Optionsdatei:

```
snapshotcachesize 95
```

```
Nur für AIX: include.fs /kalafs1
```

```
snapshotproviderfs=JFS2 snapshotcachesize=95
```

```
Nur für AIX: include.image /kalafs2
             snapshotcachesize=95
Nur für Linux: include.image /linuxfs1
             snapshotcachesize=100
```

Befehlszeile:

```
-snapshotcachesize=95
```

Zugehörige Informationen

Unter „Include-Optionen“ auf Seite 473 finden Sie weitere Informationen über `include.fs`.

Snapshotproviderfs

Verwenden Sie die Option `snapshotproviderfs`, um Dateisicherungs- und Dateiarchivierungsoperationen auf Momentaufnahmebasis zu aktivieren und einen Momentaufnahmeprovider anzugeben.

Sie müssen Root sein, um eine Dateisicherungs- oder Dateiarchivierungsoperation auf Momentaufnahmebasis auszuführen. Wenn Sie kein Rootbenutzer sind, schlägt die Operation mit einer Fehlermeldung fehl.

Unterstützte Clients

Diese Option ist nur für AIX-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Geben Sie diese Option in der Serverzeilengruppe der Systemoptionsdatei `dsm.sys` an, um Momentaufnahmen für alle JFS2-Dateisysteme auf dem Client zu aktivieren. Sie können die clientweite Option für eine bestimmte Operation überschreiben, indem Sie diese Option in der Befehlszeile für die Sicherungs- und Archivierungsbefehle angeben. Sie können die clientweite Option auch für ein bestimmtes Dateisystem überschreiben, indem Sie die Anweisung `include.fs` in der Datei `dsm.sys` verwenden. Sie können diese Option auch mit Hilfe des Profileditors setzen.

Syntax

►►—SNAPSHOTPROVIDERFS— —Wert—►►

Parameter

Wert

Gibt einen der folgenden Werte an:

JFS2

Gibt an, dass Sie eine Dateisicherung oder -archivierung auf Momentaufnahmebasis ausführen wollen, während das Dateisystem für andere Systemanwendungen verfügbar ist. *Nur* für JFS2-Dateisysteme auf AIX-Clients gültig.

NONE

Gibt an, dass keine Momentaufnahmen verwendet werden sollen. Für das angegebene Dateisystem wird eine Dateisicherungs- oder -archivierungsoperation ausgeführt. Dies ist der Standardwert.

Beispiele

Optionsdatei:

```
snapshotproviderfs JFS2
include.fs /kalafs1 snapshotproviderfs=JFS
```

Befehlszeile:

```
-SNAPSHOTPROVIDERFS=JFS2
```

Snapshotproviderimage

Verwenden Sie die Option `snapshotproviderimage`, um Imagesicherung auf Momentaufnahmebasis zu aktivieren und einen Momentaufnahmeprovider anzugeben.

Sie müssen Root sein, um eine Imagesicherungsoperation auf Momentaufnahmebasis auszuführen. Wenn Sie kein Rootbenutzer sind, schlägt die Operation mit einer Fehlermeldung fehl.

Unterstützte Clients

Diese Option ist nur für AIX- und Linux-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Geben Sie diese Option in der Serverzeilengruppe der Systemoptionsdatei `dsm.sys` an, um Momentaufnahmen für alle Dateisysteme auf dem Client zu aktivieren. Sie können die clientweite Option für eine bestimmte Operation überschreiben, indem Sie diese Option in der Befehlszeile für den Befehl **backup image** angeben. Sie können die clientweite Option auch für ein bestimmtes Dateisystem überschreiben, indem Sie die Anweisung `include.image` in der Datei `dsm.sys` verwenden. Sie können diese Option auch mit Hilfe des Profileditors setzen.

Syntax

►►—SNAPSHOTPROVIDERImage— Wert —◄◄

Parameter

Wert

Gibt einen der folgenden Werte an:

JFS2

Gibt an, dass Sie eine Imagesicherung auf Momentaufnahmebasis ausführen wollen, während das Dateisystem für andere Systemanwendungen verfügbar ist. Dies ist der Standardwert für JFS2-Dateisysteme. *Nur* für AIX-Clients gültig.

LINUX_LVM

Gibt an, dass Sie eine Imagesicherung auf Momentaufnahmebasis ausführen wollen, während das Dateisystem für andere Systemanwendungen verfügbar ist. Dies ist der Standardwert für Dateisysteme, die sich auf logischen Datenträgern befinden, die durch den Linux Logical Volume Manager erstellt wurden. *Nur* für Linux-Clients gültig.

NONE

Gibt an, dass Sie keine Imagesicherungsoperation auf Momentaufnahmebasis ausführen wollen. Damit wird für das angegebene Dateisystem eine statische Imagesicherungsoperation ausgeführt. Dies ist der Standardwert für andere Dateisysteme als AIX JFS2 und Linux LVM.

Beispiele

Optionsdatei:

```
snapshotprovideri JFS2
include.image /kalafs1 snapshotprovideri=JFS2
```

Befehlszeile:

```
-SNAPSHOTPROVIDERImage=NONE
```

Snapshotroot

Wenn Sie eine Anwendung eines unabhängigen Softwareanbieters zur Erstellung einer Momentaufnahme eines logischen Datenträgers benutzen, verwenden Sie die Option **snapshotroot** im Befehl **incremental**, **selective** oder **archive**, um die Daten der lokalen Momentaufnahme den originalen Dateibereichsdaten zuzuordnen, die auf dem IBM Spectrum Protect-Server gespeichert sind.

Die Option **snapshotroot** kann zum Sichern von über NFS-Mount zugeordneten Dateisystemen verwendet werden. Sowohl die Sicherungsspezifikation (Quelle) als auch der Wert für **snapshotroot** kann über NFS-Mount zugeordnete Dateien angegeben. Die Option **snapshotroot** kann beispielsweise zum Sichern eines NFS-Dateisystems verwendet werden, das sich auf einem NAS (Network-Attached Storage) befindet, der Momentaufnahmen unterstützt.

Aus Leistungsgründen sollte diese Option bei einer Teilsicherung eines Datenträgers eines NAS-Dateiservers anstelle einer einfachen Teilsicherung oder einer Teilsicherung mit der Option **snapshotroot** verwendet werden, wenn auf dem NAS-Dateiserver ONTAP V7.3 ausgeführt wird. Die Optionen **snappdiff** und **snapshotroot** sollten nicht gemeinsam verwendet werden.

Im folgenden Beispiel ist das Dateisystem **test495** ein vom NAS-Dateiserver **philo** über NFS-Mount zugeordnetes Dateisystem und **/philo/test945/.snapshot/backupsnap** stellt die auf dem NAS-Dateiserver erstellte Momentaufnahme dar.

```
dsmc i /philo/test945 -snapshotroot=/philo/test945/.snapshot/backupsnap
```

Sie können ein Verzeichnis auch mit der Option **snapshotroot** angeben, wenn Sie jede Dateigruppe als separaten Dateibereich sichern.

Die Option **snapshotroot** bietet keine Funktionen zur Erstellung einer Datenträgermomentaufnahme, sondern ausschließlich Funktionen zur Verwaltung von Daten, die durch Erstellen einer Datenträgermomentaufnahme generiert werden.

Beispiel: Eine Anwendung erstellt eine Momentaufnahme des Dateisystems **/usr** und hängt sie als **/snapshot/day1** an. Wenn Sie diese Daten mit dem folgenden Befehl sichern, wird ein eindeutiger Dateibereich mit dem Namen **/snapshot/day1** auf dem Server erstellt.

```
dsmc incremental /snapshot/day1
```

Möglicherweise möchten Sie die Momentaufnahmedaten den Daten zuordnen, die für das Dateisystem **/usr** bereits verarbeitet wurden. Mit der Option **snapshotroot**

können Sie die Daten dem Dateibereich zuordnen, der der Dateisystem /usr auf dem IBM Spectrum Protect-Server entspricht:

```
dsmc incremental /usr -snapshotroot=/snapshot/day1
```

An einem späteren Tag können Sie eine Momentaufnahme sichern, die an einer anderen Position gespeichert wurde, jedoch unter demselben Dateibereich auf dem Server verwaltet wird:

```
dsmc incremental /usr -snapshotroot=/snapshot/day2
```

Mit Hilfe der Option snapshotroot können Sie Teilsicherungen, selektive Sicherungen oder Archivierungen von einzelnen Verzeichnissen, Verzeichnisstrukturen oder einzelnen Dateien ausführen. In allen Fällen muss die Option snapshotroot den logischen Datenträger angeben, der durch die Momentaufnahme erstellt wurde. Zum Beispiel:

```
dsmc incremental /usr/dir1/* -subdir=yes  
-snapshotroot=/snapshot/day1  
dsmc selective /usr/dir1/sub1/file.txt  
-snapshotroot=/snapshot/day1  
dsmc archive /usr/dir1/sub1/*.txt  
-snapshotroot=/snapshot/day1
```

Sollen bestimmte Dateispezifikationen ein- oder ausgeschlossen werden, müssen die entsprechenden Include- und Exclude-Anweisungen den Namen des Dateisystems enthalten, das die Quelle der Momentaufnahme (Dateisystem /usr) darstellt, und nicht den Namen des Ziels der Momentaufnahme (/snapshot/day1). Auf diese Weise ist die Beibehaltung eines Satzes von Include- und Exclude-Anweisungen möglich, auch wenn der Name des logischen Datenträgers, auf den die Momentaufnahme geschrieben wird, sich ändert. Die folgenden Beispiele zeigen Include- und Exclude-Anweisungen.

```
include /usr/dir1/*.txt lyrmgmtclass  
exclude /usr/mydocs/*.txt
```

Die folgenden Include-/Exclude-Anweisungen sind nicht gültig, da sie den Namen der Momentaufnahme enthalten:

```
include /snapshot/day1/dir1/*.txt lyrmgmtclass  
exclude /snapshot/day1/mydocs/*.txt
```

Bei Teilsicherungen, selektiven Sicherungen oder Archivierungen müssen Sie die Option snapshotroot mit einer einzelnen Dateispezifikation verwenden. Es ist nicht möglich, mehrere Dateispezifikationen oder keine Dateispezifikation anzugeben. Die folgenden Befehle sind beispielsweise gültig:

```
dsmc incremental /usr -snapshotroot=/snapshot/day1  
dsmc incremental /usr/dir1/* -snapshotroot=/snapshot/day1
```

Der folgende Befehl ist ungültig, da er zwei Dateispezifikationen enthält:

```
dsmc incremental /usr/dir1/* /home/dir2/*  
-snapshotroot=/snapshot/day1
```

Der folgende Befehl ist ungültig, da er keine Dateispezifikation enthält:

```
dsmc incremental -snapshotroot=/snapshot/day1
```

Anmerkungen:

1. Stellen Sie sicher, dass die Option snapshotroot auf eine Momentaufnahme des richtigen Datenträgers verweist. Stellen Sie sicher, dass die snapshotroot-Position auf das Stammverzeichnis der Momentaufnahme verweist. Werden diese Re-

geln nicht befolgt, kann es zu unbeabsichtigten Ergebnissen kommen, sodass Dateien z. B. fälschlicherweise als verfallen markiert werden.

2. Wenn Sie die Option `filelist` und die Option `snapshotroot` angeben, wird angenommen, dass sich alle in der Option `filelist` angegebenen Dateien in demselben Dateisystem befinden. Befinden sich Einträge in der Option `filelist` in einem anderen Dateisystem, werden sie übersprungen und ein Fehler wird protokolliert. Enthält die Option `filelist` Dateien, die nach der Erstellung der Momentaufnahme in dem Dateisystem erstellt wurden, werden diese Einträge ebenfalls übersprungen und ein Fehler wird protokolliert.
3. Sie können die Option `snapshotroot` nicht mit der Option `snaptiff` verwenden.
4. Sie können die Option `snapshotroot` mit den Optionen `preschedulecmd` und `postschedulecmd` oder in automatisierten Scripts verwenden, die Sie mit dem Client-Scheduler ausführen.

Unterstützte Clients

Diese Option ist für die folgenden Clients gültig:

- UNIX- und Linux-Clients mit Ausnahme von Mac OS X.

Syntax

►—SNAPSHOTRoot =— —*Momentaufnahmedatenträgername*————►

Parameter

Momentaufnahmedatenträgername

Gibt das Stammverzeichnis des logischen Datenträgers an, der durch die Anwendung eines unabhängigen Softwareanbieters zur Momentaufnahmenerstellung generiert wurde.

Beispiele

Befehlszeile:

```
dsmc incremental /usr -SNAPSHOTRoot=/snapshot/day1
```

Srvoptsetencryptiondisabled

Die Option `srvoptsetencryptiondisabled` ermöglicht es dem Client, die Verschlüsselungsoptionen in einer Clientoptionsgruppe auf dem IBM Spectrum Protect-Server zu ignorieren.

Ist die Option in der Clientoptionsdatei auf `yes` gesetzt, ignoriert der Client die folgenden Optionen in einer Clientoptionsgruppe auf dem Server:

- `encryptkey generate`
- `exclude.encrypt`
- `include.encrypt`

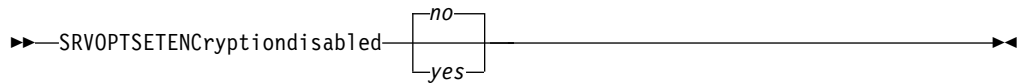
Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Syntax



Parameter

yes

Der Client für Sichern/Archivieren ignoriert die Werte der aufgelisteten Verschlüsselungsoptionen in einer Clientoptionsgruppe auf dem IBM Spectrum Protect-Server.

no Der Client für Sichern/Archivieren verarbeitet die Einstellung der aufgelisteten Verschlüsselungsoptionen in einer Clientoptionsgruppe auf dem IBM Spectrum Protect-Server. Dies ist der Standardwert.

Beispiele

Optionsdatei:

```
srvoptsetencryptiondisabled no
```

Befehlszeile:

Nicht zutreffend.

Srvprepostscheddisabled

Die Option `srvprepostscheddisabled` gibt an, ob verhindert werden soll, dass die vom IBM Spectrum Protect-Administrator angegebenen Befehle vor und nach dem Zeitplan bei der Ausführung geplanter Operationen auf dem Clientsystem ausgeführt werden.

Die Option `srvprepostscheddisabled` kann zusammen mit den Optionen `schedcmddisabled` und `srvprepostscheddisabled` verwendet werden, um die Ausführung unerwünschter Betriebssystembefehle durch den IBM Spectrum Protect-Administrator auf einem Clientknoten zu inaktivieren.

Unterstützte Clients

Diese Option ist für alle Clients für Sichern/Archivieren gültig, die den IBM Spectrum Protect-Client-Scheduler verwenden. Diese Option kann nicht auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Datei `dsm.sys` innerhalb einer Serverzeilengruppe für den Scheduler ein. Sie können diese Option auf der Registerkarte **Scheduler** des Profileditors im Abschnitt **Befehl für Zeitplan** definieren.

Syntax



Parameter

No Gibt an, dass der Client die Ausführung von Befehlen vor und nach dem Zeitplan, die vom IBM Spectrum Protect-Administrator definiert wurden, bei der Ausführung geplanter Operationen auf dem Clientsystem zulässt. Wird ein Befehl vor oder nach dem Zeitplan sowohl vom Client als auch vom IBM Spectrum Protect-Administrator definiert, überschreibt der vom Administrator definierte Befehl den entsprechenden in der Clientoptionsdatei definierten Befehl. Dies ist der Standardwert.

Yes

Gibt an, dass der Client die Ausführung von Befehlen vor und nach dem Zeitplan, die vom IBM Spectrum Protect-Administrator definiert wurden, bei der Ausführung geplanter Operationen auf dem Clientsystem verhindert. Wird ein Befehl vor oder nach dem Zeitplan sowohl vom Client als auch vom IBM Spectrum Protect-Administrator definiert, überschreibt der vom Administrator definierte Befehl *nicht* den entsprechenden in der Clientoptionsdatei definierten Befehl. Diese Option kann zusammen mit den Optionen `schedcmddisabled` und `srvprepostscheddisabled` verwendet werden.

Beispiele

Optionsdatei:

`srvprepostscheddisabled yes`

Befehlszeile:

Nicht zutreffend.

Srvprepostsnapdisabled

Die Option `srvprepostsnapdisabled` gibt an, ob verhindert werden soll, dass die vom IBM Spectrum Protect-Administrator angegebenen Befehle vor und nach der Momentaufnahme bei der Ausführung geplanter Sicherungsoperationen für Image-Momentaufnahmen ausgeführt werden.

Die Option `srvprepostsnapdisabled` kann zusammen mit den Optionen `schedcmddisabled` und `srvprepostscheddisabled` verwendet werden, um die Ausführung unerwünschter Betriebssystembefehle durch den IBM Spectrum Protect-Administrator auf einem Clientknoten zu inaktivieren.

Unterstützte Clients

Diese Option ist für Linux-Clients gültig, die den Befehl zum Sichern von Image-Momentaufnahmen unterstützen. Diese Option kann nicht auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Datei `dsm.sys` innerhalb einer Serverzeilengruppe für den Scheduler ein. Sie können diese Option auf der Registerkarte **Momentaufnahme** des Profileditors im Abschnitt **Momentaufnahmeoptionen** definieren.

Syntax



Parameter

No Gibt an, dass der Client die Ausführung von Befehlen vor und nach der Momentaufnahme, die vom IBM Spectrum Protect-Administrator definiert wurden, bei der Ausführung geplanter Operationen für Image-Momentaufnahmesicherungen auf dem Clientsystem zulässt. Wird ein Befehl vor oder nach der Momentaufnahme sowohl vom Client als auch vom IBM Spectrum Protect-Administrator definiert, überschreibt der vom Administrator definierte Befehl den entsprechenden in der Clientoptionsdatei definierten Befehl. Dies ist der Standardwert.

Yes

Gibt an, dass der Client die Ausführung von Befehlen vor und nach der Momentaufnahme, die vom IBM Spectrum Protect-Administrator definiert wurden, bei der Ausführung geplanter Operationen für Image-Momentaufnahmesicherungen auf dem Clientsystem nicht zulässt. Wird ein Befehl vor oder nach der Momentaufnahme sowohl vom Client als auch vom IBM Spectrum Protect-Administrator definiert, überschreibt der vom Administrator definierte Befehl *nicht* den entsprechenden in der Clientoptionsdatei definierten Befehl. Diese Option kann zusammen mit den Optionen `schedcmddisabled` und `srvprepostsnapdisabled` verwendet werden.

Beispiele

Optionsdatei:

`srvprepostsnapdisabled yes`

Befehlszeile:

Nicht zutreffend.

Ssl

Verwenden Sie die Option `ssl`, um Secure Sockets Layer (SSL) für eine sichere Client- und Serverkommunikation zu aktivieren. Wenn der Client für Sichern/Archivieren mit einem IBM Spectrum Protect-Server der Version 8.1.1 und früheren Stufen der Version 8 bzw. Version 7.1.7 und früheren Stufen kommuniziert, legt der Client fest, ob SSL aktiviert wird. Wenn der Client für Sichern/Archivieren mit einem IBM Spectrum Protect-Server der Version 8.1.2 und höheren Stufen bzw. der Version 7.1.8 und höheren Stufen der Version 7 kommuniziert, wird SSL immer verwendet und mithilfe dieser Option gesteuert, ob Objektdaten verschlüsselt werden oder nicht. Aufgrund von Leistungsaspekten ist es möglicherweise sinnvoll, die Objektdaten nicht zu verschlüsseln.

Unterstützte Clients

Diese Option ist für alle unterstützten Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auch auf der Registerkarte **Übertragung** des Profileditors definieren.

Syntax



Parameter für die Kommunikation mit einem IBM Spectrum Protect-Server der Version 8.1.1 und früheren Stufen der Version 8 bzw. Version 7.1.7 und früheren Stufen

No Gibt an, dass der Client für Sichern/Archivieren SSL nicht verwendet, um Informationen zu verschlüsseln. *No* ist der Standardwert.

Yes

Gibt an, dass der Client für Sichern/Archivieren SSL verwendet, um Informationen zu verschlüsseln.

Um SSL zu aktivieren, geben Sie *SSL Yes* an und ändern Sie den Wert der Option *TCPPOPT*. Die Änderung des Werts der Option *TCPPOPT* ist im Allgemeinen erforderlich, da der IBM Spectrum Protect-Server in der Regel so konfiguriert ist, dass er an einem anderen Anschluss für SSL-Verbindungen empfangsbereit ist.

Parameter für die Kommunikation mit einem IBM Spectrum Protect-Server der Version 8.1.2 und höheren Stufen bzw. der Version 7.1.8 und höheren Stufen der Version 7.

No Gibt an, dass der Client für Sichern/Archivieren bei der Kommunikation mit dem Server SSL nicht verwendet, um Objektdaten zu verschlüsseln. Alle anderen Informationen werden verschlüsselt. *No* ist der Standardwert.

Yes

Gibt an, dass der Client für Sichern/Archivieren bei der Kommunikation mit dem Server SSL für die Verschlüsselung aller Informationen, einschließlich Objektdaten, verwendet.

Um SSL für alle Daten zu verwenden, geben Sie *SSL Yes* an.

Beispiele

Optionsdatei:

ssl yes

Befehlszeile:

Nicht zutreffend.

Zugehörige Informationen

„IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren“ auf Seite 77.

„*Sslrequired*“ auf Seite 602

„*Tcpport*“ auf Seite 614

Sslacceptcertfromserv

Mithilfe der Option *sslacceptcertfromserv* können Sie steuern, ob der Client für Sichern/Archivieren oder die API-Anwendung das öffentliche SSL-Zertifikat des IBM Spectrum Protect-Servers akzeptiert und als vertrauenswürdig anerkennt,

wenn das erste Mal eine Verbindung zwischen ihnen hergestellt wird. Diese Option gilt nur für das erste Herstellen der Verbindung zwischen dem Client für Sichern/Archivieren oder der API-Anwendung und dem IBM Spectrum Protect-Server. Wenn das öffentliche SSL-Zertifikat akzeptiert wird, werden zukünftige Änderungen an dem Zertifikat nicht automatisch akzeptiert; sie müssen manuell in den Client für Sichern/Archivieren importiert werden. Mit dieser Option können Sie die Verbindung nur zu einem IBM Spectrum Protect-Server der Version 8.1.2 und höher sowie der Version 7.1.8 und höheren Stufen der Version 7 herstellen.

Unterstützte Clients

Diese Option ist für alle unterstützten Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Syntax



Parameter

Yes

Gibt an, dass der Client für Sichern/Archivieren das öffentliche Zertifikat des IBM Spectrum Protect-Servers automatisch akzeptiert. Yes ist der Standardwert.

No

Gibt an, dass der Client für Sichern/Archivieren das öffentliche Zertifikat des IBM Spectrum Protect-Servers nicht automatisch akzeptiert.

Um SSLACCEPTCERTFROMSERV zu inaktivieren, geben Sie `sslacceptcertfromserv no` an.

Beispiele

Optionsdatei:

```
sslacceptcertfromserv no
```

Befehlszeile:

Nicht zutreffend.

Zugehörige Informationen

„Ssl“ auf Seite 598

„Sslrequired“ auf Seite 602

Ssldisablelegacytls

Verwenden Sie die Option `ssldisablelegacytls`, um die Verwendung von SSL-Protokollen mit einer niedrigeren Stufe als TLS 1.2 nicht zuzulassen.

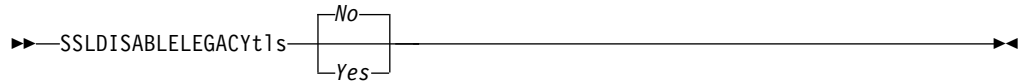
Unterstützte Clients

Diese Option ist für alle unterstützten Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Datei `dsm.sys` ein. Sie können diese Option auch in der GUI definieren, indem Sie das Kontrollkästchen **TLS 1.2 oder höher erforderlich** auf der Registerkarte **Übertragung** des Profileditors auswählen. Sie können diese Option nicht in der Befehlszeile definieren.

Syntax



Parameter

No Gibt an, dass beim Client für Sichern/Archivieren für SSL-Sitzungen nicht TLS 1.2 erforderlich ist. Der Client lässt Verbindungen mit TLS 1.1 und niedrigeren SSL-Protokollen zu. Wenn der Client für Sichern/Archivieren mit einem IBM Spectrum Protect-Server der Version 8.1.1 und früheren Stufen der Version 8 bzw. Version 7.1.7 und früheren Stufen kommuniziert, ist No der Standardwert.

Yes

Gibt an, dass beim Client für Sichern/Archivieren für alle SSL-Sitzungen das Protokoll TLS 1.2 (oder höher) erforderlich ist. Wenn der Client für Sichern/Archivieren mit einem IBM Spectrum Protect-Server der Version 8.1.2 und höheren Stufen bzw. der Version 7.1.8 und höheren Stufen der Version 7 kommuniziert, ist Yes der Standardwert.

Beispiele

Optionsdatei:

```
ssldisablelegacytls yes
```

Befehlszeile:

Nicht zutreffend.

Zugehörige Informationen:

Ssl

Sslrequired

Tcpport

Sslfipsmode

Die Option `sslfipsmode` gibt an, ob der Client den FIPS-Modus (FIPS = Federal Information Processing Standards) für die SSL-Übertragung (SSL = Secure Sockets Layer) mit dem Server verwendet. Der Standardwert ist No.

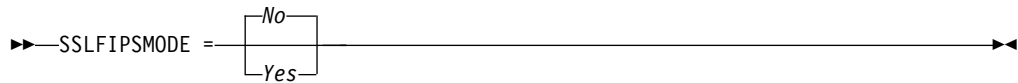
Unterstützte Clients

Diese Option wird auf allen Clients unterstützt.

Optionsdatei

Definieren Sie diese Option in der Clientoptionsdatei. Sie können die Option weder als Befehlszeilenparameter angeben noch in einer Clientoptionsgruppe definieren.

Syntax



Parameter

No Gibt an, dass der Client den SSL FIPS-Modus nicht für die sichere Kommunikation mit dem Server verwendet. SSL im FIPS-Modus wird nur von Version 6.3 und neueren Versionen des Servers unterstützt. Setzen Sie diese Clientoption auf `no`, wenn der Client SSL verwendet, um eine Verbindung zu einem Server herzustellen, der nicht Version 6.3 oder eine neuere Version aufweist.

Yes

Gibt an, dass der Client den SSL FIPS-Modus für die sichere Kommunikation mit dem Server verwendet. Die Angabe von `yes` für diese Option beschränkt die SSL-Sitzungsvereinbarung auf die Verwendung von FIPS-konformen Cipher-Suites. SSL im FIPS-Modus wird nur vom Server der Version 6.3 (oder neueren Versionen) unterstützt.

Beispiel

Folgendes angeben, um den SSL FIPS-Modus auf dem Client zu aktivieren:

```
SSLFIPSMODE yes
```

Sslrequired

Die Option `sslrequired` gibt die Bedingungen an, unter denen SSL erforderlich ist, wenn sich der Client beim IBM Spectrum Protect-Server oder bei den Speicheragenten anmeldet. Um SSL zu aktivieren, damit die Kommunikation zwischen Client und Server sowie Client und Speicheragent sicher ist, müssen Sie die Clientoption `ssl` auf `yes` setzen. Bei der Kommunikation mit dem IBM Spectrum Protect-Server der Version 8.1.2 und höheren Stufen sowie der Version 7.1.8 und höheren Stufen der Version 7 ist diese Option nicht mehr gültig, da SSL immer verwendet wird.

Unterstützte Clients

Diese Option wird auf allen Clients unterstützt.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei oder, in der grafischen Benutzeroberfläche, auf der Registerkarte 'Übertragung' ein. Sie können diese Option nicht in der Befehlszeile definieren.

Syntax



Parameter

Default

Diese Einstellung gibt an, dass SSL zum Schützen der Kommunikation zwischen dem Client und dem Server sowie dem Client und den Speicheragenten erforderlich ist, wenn AUTHENTICATION=LDAP auf dem Server definiert ist. Um die Kommunikation mit SSL zu sichern, müssen Sie außerdem ssl=yes auf dem Client definieren.

Ist AUTHENTICATION=LOCAL auf dem Server definiert, gibt diese Einstellung an, dass SSL nicht erforderlich ist. Auch wenn SSL nicht erforderlich ist, wenn AUTHENTICATION=LOCAL und sslrequired=default definiert sind, können Sie SSL dennoch verwenden, indem Sie die Clientoption ssl auf yes setzen.

Yes

Gibt an, dass SSL immer erforderlich ist, um die Kommunikation zwischen dem Client und dem Server sowie dem Client und den Speicheragenten zu schützen. sslrequired=yes ist nicht von der Serveroption AUTHENTICATION abhängig. Wenn Sie sslrequired=yes auf dem Client definieren, müssen Sie auch ssl=yes auf dem Client angeben.

No Gibt an, dass SSL nicht erforderlich ist, um die Kommunikation zwischen dem Client und dem Server oder dem Client und den Speicheragenten zu schützen. Wählen Sie diese Option nur aus, wenn Sie ein virtuelles privates Netz oder eine andere Methode zum Schützen Ihrer Sitzungskommunikation verwenden. Sie können SSL dennoch aktivieren, indem Sie ssl=yes auf dem Client definieren; sslrequired=no gibt jedoch an, dass SSL keine Voraussetzung ist.

SERVERonly

Gibt an, dass SSL für die Kommunikation zwischen dem Client und dem Server erforderlich ist und für die Kommunikation zwischen dem Server und dem Speicheragenten nicht erforderlich ist. Soll SSL für die Kommunikation zwischen dem Client und dem Server verwendet werden, definieren Sie sslrequired=serveronly und ssl=yes. Die Servereinstellung für die Option AUTHENTICATION kann LOCAL oder LDAP lauten.

Verwenden Sie für die Kommunikation zwischen dem Client und dem Speicheragenten die Clientoption lanfreessl, um SSL zu aktivieren.

Die folgende Tabelle enthält Beschreibungen der Situationen, in denen die Authentifizierung erfolgreich ist oder fehlschlägt, je nach Einstellung der Option SSLREQUIRED auf dem Server und dem Client und der Einstellung der Option ssl auf dem Client. Voraussetzung ist, dass gültige Berechtigungsnachweise angegeben werden.

Tabelle 77. Auswirkungen der SSL-Einstellungen des Servers und des Clients auf den Erfolg bzw. Misserfolg von Anmeldeversuchen

Option SSLREQUIRED (Servereinstellung)	Option sslrequired (Clienteneinstellung)	Option ssl (Clienteneinstellung)	Erfolg oder Misserfolg der Authentifizierung
Yes	Yes	Yes	Authentifizierung erfolgreich
Yes	Yes	No	Authentifizierung schlägt fehl; der Client weist die Sitzung zurück
Yes	No	Yes	Authentifizierung erfolgreich
Yes	No	No	Authentifizierung schlägt fehl; der Server weist die Sitzung zurück
No	Yes	Yes	Authentifizierung erfolgreich

Tabelle 77. Auswirkungen der SSL-Einstellungen des Servers und des Clients auf den Erfolg bzw. Misserfolg von Anmeldeversuchen (Forts.)

Option SSLREQUIRED (Servereinstellung)	Option sslrequired (Clienteneinstellung)	Option ssl (Clienteneinstellung)	Erfolg oder Misserfolg der Authentifizierung
No	Yes	No	Authentifizierung schlägt fehl; der Client weist die Sitzung zurück
No	No	Yes	Authentifizierung erfolgreich
No	No	No	Authentifizierung erfolgreich

Im folgenden Text wird beschrieben, wie sich die Einstellungen SSLREQUIRED=DEFAULT und SSLREQUIRED=SERVERONLY auf dem Server auf die Option ssl auf dem Client auswirken.

Wenn auf dem Server SSLREQUIRED=DEFAULT und AUTHENTICATION=LDAP definiert sind, muss auf dem Client ssl=yes definiert werden. Andernfalls schlägt die Authentifizierung fehl.

Wenn auf dem Server SSLREQUIRED=DEFAULT und AUTHENTICATION=LOCAL definiert sind, kann auf dem Client ssl=yes oder ssl=no definiert werden.

Wenn auf dem Server SSLREQUIRED=SERVERONLY definiert ist, muss auf dem Client ssl=yes definiert werden. Die Clientoption lanfreessl kann auf yes gesetzt werden, um die Kommunikation mit einem Speicheragenten zu schützen, oder kann auf no gesetzt werden, wenn die sichere Kommunikation mit Speicheragenten nicht erforderlich ist.

Beispiele

Optionsdatei:

```
sslrequired yes
sslrequired no
sslrequired default
sslrequired serveronly
```

Befehlszeile:

Nicht gültig; Sie können diese Option nicht in der Befehlszeile definieren.

Stagingdirectory

Die Option stagingdirectory definiert die Position, an der der Client alle Daten speichert, die er zum Ausführen seiner Operationen generiert. Die Daten werden gelöscht, wenn die Verarbeitung beendet ist.

Wichtig: Ab Version 8.1.2 wird die Option snapdiffchangelogdir verwendet, um die Position zum Speichern von Änderungsprotokollen für Momentaufnahme-differenzierungsoperationen anzugeben. Die Option stagingdirectory wird nicht mehr zu diesem Zweck verwendet. Weitere Informationen finden Sie in „Snapdiffchangelogdir“ auf Seite 587.

Unterstützte Clients

Diese Option ist für Linux-Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (`dsm.opt`) ein. Wird `stagingdirectory` in der Befehlszeile angegeben, überschreibt diese Angabe die Werte, die in der Optionsdatei angegeben sind.

Syntax

►—`STAGINGDIRectory`—*Pfad*—►

Parameter

Pfad

Gibt den Verzeichnispfad an, in den der Client zwischenspeichernde Daten schreibt. Wenn Sie kein Zwischenspeichungsverzeichnis angeben, speichert der Client temporäre Daten im temporären Dateisystem (normalerweise `/tmp`).

Beispiele

Optionsdatei:

`stagingdirectory /usr/tsmdata`

`stagingdirectory /private/tmp`

Befehlszeile:

`-stagingdir="/tmp/tsmtempdata"`

Zugehörige Verweise:

„Diffsnapshot“ auf Seite 400

„Snapdiff“ auf Seite 581

Subdir

Die Option `subdir` gibt an, ob Unterverzeichnisse benannter Verzeichnisse bei der Verarbeitung berücksichtigt werden sollen.

Die Option `subdir` können Sie in folgenden Befehlen verwenden:

- **archive**
- **delete archive**
- **delete backup**
- **incremental**
- **query archive**
- **query backup**
- **restore**
- **restore backupset**
- **restore group**
- **retrieve**
- **selective**

Wenn Sie beim Sichern eines bestimmten Pfads und einer bestimmten Datei die Option `subdir` auf `yes` setzen, durchsucht der Client für Sichern/Archivieren rekursiv alle Unterverzeichnisse unter diesem Pfad und sucht nach allen Instanzen der angegebenen Datei, die sich unter einem dieser Unterverzeichnisse befinden. Beispiel: Angenommen, eine Datei mit dem Namen `myfile.txt` ist auf einem Client in den folgenden Verzeichnissen vorhanden:

```
//myfile.txt  
/dir1/myfile.txt  
/dir1/dir_a/myfile.txt  
/dir1/dir_b/myfile.txt
```

Wenn eine selektive Sicherung dieser Datei durchgeführt wird, werden alle vier Instanzen von myfile.txt gesichert:

```
dsmc sel /myfile.txt -subdir=yes
```

Dementsprechend werden mit dem folgenden Befehl alle Instanzen von myfile.txt angezeigt, wenn Sie subdir=yes in der Clientoptionsdatei oder einer Clientoptionsgruppe angeben.

```
dsmc restore /myfile.txt -pick
```

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein.

Syntax



Parameter

No Unterverzeichnisse werden nicht verarbeitet. Dies ist der Standardwert.

Yes

Unterverzeichnisse werden verarbeitet. Da das Clientprogramm alle Unterverzeichnisse eines Verzeichnisses, das verarbeitet wird, durchsucht, kann die Verarbeitung länger dauern. *Yes* sollte nur im Bedarfsfall angegeben werden.

Wenn Sie die Option *preservepath* zusätzlich zu *subdir=yes* verwenden, kann dies einen Einfluss darauf haben, welche Unterverzeichnisse verarbeitet werden.

Handelt es sich bei einem Unterverzeichnis um ein angehängtes Dateisystem, wird es nicht verarbeitet, auch wenn Sie *subdir=yes* angeben.

Anmerkung:

1. Wenn Sie den Client im interaktiven Modus ausführen und die Option *-subdir=yes* verwenden, bleibt die Einstellung für alle Befehle bestehen, die im interaktiven Modus eingegeben werden, bis Sie den interaktiven Modus durch Eingabe von *Quit* beenden.
2. Ist *subdir=yes* wirksam, wenn Sie mehrere Dateien zurückschreiben, fügen Sie am Ende der Zieldateispezifikation einen Verzeichnisbegrenzer ein. Wird der Begrenzer nicht angegeben, zeigt der Client eine Nachricht an, die angibt, dass die Zieldateispezifikation nicht gültig ist.
3. Es wird empfohlen, nur den Standardwert für *subdir* (*No*) in eine Clientoptionsdatei oder eine Clientoptionsgruppe einzuschließen.

Beispiele

Optionsdatei:

```
subdir no
```

Befehlszeile:

Zum Zurückschreiben der Struktur:

```
/Users/mike/dir1
/Users/mike/dir1/file1
/Users/mike/dir1/dir2
/Users/mike/dir1/dir2/file1
```

einen der folgenden Befehle eingeben:

```
dsmc rest "/Users/van/dir1/*" /Users/mike/ -su=yes
dsmc rest "/Users/van/dir1/file*" /Users/mike/ -su=yes
dsmc rest "/Users/van/dir1/file1*" /Users/mike/ -su=yes
```

Zum Zurückschreiben der Struktur:

```
/path2/dir1
/path2/dir1/file1
/path2/dir1/dir2
/path2/dir1/dir2/file1
```

einen der folgenden Befehle eingeben:

```
dsmc rest "/path/dir1/*" /path2/ -su=yes
dsmc rest "/path/dir1/file*" /path2/ -su=yes
dsmc rest "/path/dir1/file1*" /path2/ -su=yes
```

Diese Option ist in der Anfangsbefehlszeile und im interaktiven Modus gültig. Wird die Option im interaktiven Modus eingegeben, ist nur der Befehl betroffen, mit dem sie eingegeben wird. Wenn dieser Befehl beendet ist, wird der Wert auf den Wert zu Beginn der interaktiven Sitzung zurückgesetzt. Dies ist der Wert aus der Datei dsm.opt, sofern er nicht durch die Anfangsbefehlszeile oder eine vom Server erzwungene Option überschrieben wurde.

Zugehörige Informationen

„Preservepath“ auf Seite 537

Tapeprompt

Die Option tapeprompt gibt an, ob der Client für Sichern/Archivieren auf einen Bandladevorgang warten soll, der für eine Sicherung, Archivierung, Zurückschreibung oder einen Abruf erforderlich ist, oder ob eine Bedienerführung für die Auswahl angezeigt werden soll.

In der GUI des Clients für Sichern/Archivieren kann im Dialog 'Datenträgermount' der Wert Informationen nicht verfügbar in den Feldern für Einheit und Datenträgerkennsatz angezeigt werden, wenn Sie eine standardmäßige (auch als klassisch bezeichnete) Zurückschreibungs- oder Abrufoperation ausführen. Dieser Wert bedeutet, dass diese Informationen nur für Zurückschreibungs- oder Abrufoperationen ohne Abfrage verfügbar sind, nicht für eine Standardzurückschreibungs- oder -abrufoperation. Im Feld **Einheit** wird der Name der Einheit angezeigt, auf der der für die Verarbeitung eines Objekts benötigte Datenträger geladen werden soll. Im Feld **Datenträgerkennsatz** wird der Name des für die Verarbeitung benötigten Datenträgers angezeigt.

Unabhängig von der Einstellung der Option `tapeprompt` erfolgt während einer geplanten Operation keine Aufforderung zum Bandladevorgang.

Die Option `tapeprompt` kann in den folgenden Befehlen verwendet werden:

- **archive**
- **delete archive**
- **delete backup**
- **incremental**
- **restore**
- **retrieve**
- **selective**

Anmerkung: Diese Option kann auch auf dem Server definiert werden.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (`dsm.opt`) ein. Sie können diese Option auf der Registerkarte **Allgemein** über das Kontrollkästchen **Bedienerführung vor dem Bandladevorgang** im Profileditor definieren.

Syntax



Parameter

No Es wird keine Bedienerführung für die Auswahl angezeigt. Der Server wartet auf das Laden des entsprechenden Bandes. Dies ist der Standardwert.

Anmerkung: Für API-Anwendungen ermöglicht dies die direkte Sicherung auf Band.

Yes

Wenn zum Sichern, Archivieren, Zurückschreiben oder Abrufen von Daten ein Band erforderlich ist, wird eine Bedienerführung angezeigt. Auswahlmöglichkeiten der Bedienerführung: Auf das Laden des entsprechenden Bandes warten, immer auf das Laden eines Bandes warten, ein bestimmtes Objekt überspringen, alle Objekte auf einem Band überspringen, alle Objekte auf allen Bändern überspringen oder die gesamte Operation abbrechen.

Beispiele

Optionsdatei:

`tapeprompt yes`

Befehlszeile:

`-tapep=yes`

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Tcpadminport

Verwenden Sie die Option `tcpadminport`, um eine separate TCP/IP-Anschlussnummer anzugeben, an der der Server Anforderungen für Verwaltungsclientsitzungen erwartet. Dies ermöglicht sichere Verwaltungssitzungen innerhalb eines privaten Netzwerks.

Die Einstellung für die Clientoption `tcpadminport` ist davon abhängig, wie die IBM Spectrum Protect-Serveroptionen `tcpadminport` und `adminonclientport` konfiguriert sind. Der Server verfügt über eine Einstellung `tcpadminport`, die anzeigt, an welchem Anschluss der Server für Verwaltungssitzungen empfangsbereit ist, und über die Einstellung `adminonclientport`, die entweder `yes` oder `no` sein kann.

Ist tcpadminport auf dem Server nicht definiert, sind Verwaltungssitzungen an demselben Anschluss zulässig wie Clientsitzungen.

Ist `tcpadminport` auf dem Server definiert, sind Verwaltungssitzungen an dem durch diese Einstellung angegebenen Anschluss zulässig. In diesem Fall können die Verwaltungssitzungen, falls `adminonclientport` `yes` aktiv ist, entweder am regulären Clientanschluss eine Verbindung herstellen oder an dem Anschluss, der durch `tcpadminport` angegeben ist. Wenn `adminonclientport` `no` aktiv ist, können die Verwaltungssitzungen nur an dem Anschluss, der durch `tcpadminport` angegeben ist, eine Verbindung herstellen.

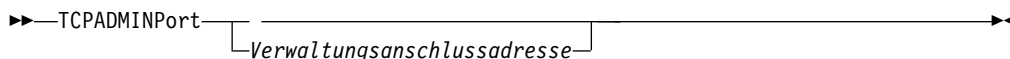
Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Übertragung** im Feld **Verwaltungsanschluss** des Profileditors definieren.

Syntax



Parameter

Verwaltungsanschlussadresse

Gibt die Anschlussnummer des Servers an. Der Standardwert ist der Wert der Option tcpport.

Beispiele

Optionsdatei:

```
tcpadminport 1502
```

Tcpbuffsize

Die Option `tcpbuffsize` gibt die Größe des internen TCP/IP-Kommunikationspuffers an, der verwendet wird, um Daten zwischen dem Clientknoten und dem Server zu übertragen. Ein größerer Puffer kann die Übertragungsleistung verbessern, benötigt jedoch mehr Speicher.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Übertragung** im Feld **Puffergröße** des Profileditors definieren.

Syntax

►►—TCPBuffsize— —Größe—◄◄

Parameter

Größe

Gibt die gewünschte Größe (in Kilobyte) für den internen TCP/IP-Kommunikationspuffer an. Der Wertebereich ist 1 bis 512; Standardwert ist 32.

Je nach den Betriebssystemeinstellungen für die Übertragung akzeptiert das System unter Umständen nicht alle Werte in dem Bereich von 1 bis 512.

Beispiele

Optionsdatei:

tcpb 32

Befehlszeile:

-tcpbuffsize=32

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Tcpcadaddress

Die Option tcpcadaddress gibt eine TCP/IP-Adresse für dsmcad an. Normalerweise wird diese Option nicht benötigt. Verwenden Sie diese Option nur, wenn Ihr Clientknoten mehrere TCP/IP-Adressen hat oder wenn TCP/IP nicht die Standardübertragungsmethode ist.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe ein.

Syntax

►►—TCPCADAddress— —CAD-Adresse—◄◄

Parameter

CAD-Adresse

Gibt einen TCP/IP-Internetdomännennamen oder eine numerische IP-Adresse an. Wenn Sie eine IPv6-Adresse angeben, müssen Sie die Option `commmethod V6Tcpip` angeben.

Beispiele

Optionsdatei:

```
tcpcada dsmclnt.example.com
```

Befehlszeile:

```
-tcpcadaddress=192.0.2.0  
-tcpcadaddress=mycompany.example.com  
-tcpcadaddress=2001:0DB8:0:0:0:0:0:0
```

Diese Option ist nur in der Anfangsbefehlszeile des Programms `dsmcad` gültig. Sie ist nicht mit anderen dsm-Modulen gültig.

Zugehörige Informationen

Mit Hilfe der Informationen unter „Commmethod“ auf Seite 376 können Sie feststellen, ob Ihr Clientknoten über mehrere TCP/IP-Adressen verfügt oder ob TCP/IP die Standardübertragungsmethode ist.

Tcpclientaddress

Mit der Option `tcpclientaddress` kann eine TCP/IP-Adresse angegeben werden, wenn der Clientknoten des Benutzers über mehrere Adressen verfügt und der Server eine Verbindung zu einer anderen Adresse herstellen soll, als die, mit der die erste Verbindung zum Server hergestellt wurde.

Der Server verwendet diese Adresse, wenn er die Operation mit Zeitplanung über Serversystemanfrage beginnt.

Diese Option darf nur verwendet werden, wenn Sie für die Option `schedmode` den Parameter `prompted` angeben.

Wird `sessioninitiation` auf `serveronly` gesetzt, sollte der Wert für die Clientoption `tcpclientaddress` mit dem Wert der Servereinstellung `HLAddress` übereinstimmen.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Datei `dsm.sys` *innerhalb* einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Scheduler** im Feld **Ihre TCP/IP-Adresse** im Profileditor definieren.

Syntax

►►—TCPCLIENTAddress— —*Clientadresse*—►►

Parameter

Clientadresse

Gibt die TCP/IP-Adresse an, die der Server für die Kommunikation mit Ihrem Clientknoten verwenden soll. Geben Sie einen TCP/IP-Internetdomännennamen oder eine numerische IP-Adresse an. Die numerische IP-Adresse kann entweder eine TCP/IPv4- oder eine TCP/IPv6-Adresse sein. Sie können IPv6-Adressen nur verwenden, wenn Sie die Option `commethod V6Tcpip` angegeben haben.

Beispiele

Optionsdatei:

```
tcpclienta dsmclnt.example.comoder  
tcpclienta 192.0.2.21
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Tcpclientport

Mit der Option `tcpclientport` wird eine TCP/IP-Anschlussnummer für den Server angegeben, mit der eine Verbindung zum Client hergestellt wird, wenn der Server die Operation mit Zeitplanung über Serversystemanfrage beginnt.

Diese Option darf nur verwendet werden, wenn Sie für die Option `schedmode` den Parameter `prompted` angeben.

Wird `sessioninitiation` auf `serveronly` gesetzt, sollte der Wert für die Clientoption `tcpclientport` mit dem Wert für die Serveroption `LLAddress` übereinstimmen.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Datei `dsm.sys` innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Scheduler** im Feld **Ihr TCP/IP-Anschluss** im Profileditor definieren.

Syntax

►►—TCPCLIENTPort— —*Clientanschlussadresse*—►►

Parameter

Clientanschlussadresse

Gibt die TCP/IP-Anschlussadresse an, die der Server für die Kommunikation mit Ihrem Clientknoten verwenden soll. Der Wertebereich ist 1 bis 32767; der Standardwert ist 1501.

Beispiele

Optionsdatei:

tcpclientp 1502

Befehlszeile:

-tcpclientport=1492

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Tcpnodelay

Die Option tcpnodelay gibt an, ob der Client die Verzögerung beim Senden aufeinanderfolgender kleiner Pakete im Netz pro Transaktion inaktiviert.

Ändern Sie den Wert nur unter den folgenden Bedingungen vom Standardwert in yes:

- Sie werden von der technischen Unterstützung von IBM aufgefordert, die Option zu ändern.
- Sie kennen die Auswirkung des TCP-Nagle-Algorithmus auf die Netzübertragung. Wird für die Option der Wert no angegeben, wird der Nagle-Algorithmus aktiviert, wodurch das Senden kleiner, aufeinanderfolgender Pakete verzögert wird.

Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Übertragung** des Profileditors definieren. Wählen Sie **Transaktion sofort an den Server senden** aus.

Syntax



Parameter

No Gibt an, dass der Server das Senden kleiner, aufeinanderfolgender Pakete über das Netz verzögert. Die Einstellung dieser Option auf no kann die Leistung herabsetzen.

Yes

Gibt an, dass der Server das sofortige Senden kleiner, aufeinanderfolgender Pakete über das Netz gestattet. Der Standardwert ist yes.

Beispiele

Optionsdatei:

tcpnodelay yes

Befehlszeile:
Nicht zutreffend.

Tcppport

Die Option tcppport gibt eine TCP/IP-Anschlussadresse für den IBM Spectrum Protect-Server an. Diese Adresse kann beim Administrator erfragt werden.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Übertragung** im Feld **Serveranschluss** des Profileditors definieren.

Syntax

►—TCPPort— —Anschlussadresse—►

Parameter

Anschlussadresse

Gibt die TCP/IP-Anschlussadresse für die Datenübertragung mit einem Server an. Der Wertebereich ist 1 bis 32767; der Standardwert ist 1500.

Beispiele

Optionsdatei:
tcpp 1501

Befehlszeile:
Nicht zutreffend.

Tcpserveraddress

Die Option tcpserveraddress gibt die TCP/IP-Adresse für den IBM Spectrum Protect-Server an. Sie können diese Serveradresse beim Administrator erfragen.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Übertragung** im Feld **Serveradresse** des Profileditors definieren.

Wird diese Option nicht angegeben, versucht der Client, einen Server zu kontaktieren, der auf demselben Computer wie der Client für Sichern/Archivieren ausgeführt wird.

Syntax

►—TCPServeraddress— —Serveradresse—►

Parameter

Serveradresse

Gibt eine 1- bis 64-stellige TCP/IP-Adresse für einen Server an. Geben Sie einen TCP/IP-Domännennamen oder eine numerische IP-Adresse an. Die numerische IP-Adresse kann entweder eine TCP/IP-V4- oder eine TCP/IP-V6-Adresse sein. Sie können IPv6-Adressen nur verwenden, wenn Sie die Option `commmethod V6Tcpip` angegeben haben.

Beispiele

Optionsdatei:

`tcps dsmchost.example.com`

Befehlszeile:

Nicht zutreffend.

Tcpwindow size

Mit der Option `tcpwindow size` können Sie die Größe in Kilobyte angeben, die Sie für das TCP/IP-Schiebefenster für Ihren Clientknoten verwenden wollen.

Der sendende Host kann keine mehr Daten senden, bis er eine Empfangsbestätigung und eine Aktualisierung des TCP-Empfangsfensters empfängt. Jedes TCP-Paket enthält das in der Verbindung angegebene TCP-Empfangsfenster. Ein größeres Fenster ermöglicht dem Sender, weiterhin Daten zu senden, und verbessert möglicherweise die Leistung.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Übertragung** im Feld **Fenstergröße** im Profileditor definieren.

Syntax

►—TCPWindow size— —Fenstergröße—►

Parameter

Fenstergröße

Gibt die gewünschte Größe (in Kilobyte) für das TCP/IP-Schiebefenster des Clientknotens an. Der Wertebereich ist 0 bis 2048. Der Wert 0 ermöglicht dem Client die Verwendung der standardmäßigen TCP-Fenstergröße des Betriebssystems. Werte von 1 bis 2048 zeigen an, dass die Fenstergröße im Bereich von 1 KB bis 2 MB liegt. Wenn Sie einen Wert kleiner als 1 angeben, nimmt die

TCP-Fenstergröße standardmäßig den Wert 1 an. Wenn Sie einen Wert größer als 2048 angeben, nimmt die TCP-Fenstergröße standardmäßig den Wert 2048 an.

Für Clients für Sichern/Archivieren ist der Standardwert für diesen Parameter 63 KB.

Für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ist der Standardwert für diesen Parameter 512 KB.

Anmerkungen:

- Das TCP-Fenster fungiert als Puffer im Netzwerk. Es bezieht sich nicht auf die Option `tcpbuffsize` oder auf die im Client- oder Serverspeicher zugeordneten Sende- und Empfangspuffer.
- Eine Fenstergröße, die größer als der Pufferspeicherbereich auf dem Netzadapter ist, kann unter Umständen den Durchsatz verschlechtern, da Pakete, die auf dem Adapter verloren gingen, erneut gesendet werden müssen.
- Je nach den Betriebssystemeinstellungen für die Übertragung akzeptiert das System unter Umständen nicht alle Werte des Wertebereichs.
- Die Option `tcpwindowsize` überschreibt die Standardgröße der Sende- und Empfangsfenster für TCP/IP-Sitzungen des Betriebssystems.

Beispiele

Optionsdatei:

```
tcpwindowsize 63
```

Befehlszeile:

```
-tcpw=63
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Timeformat

Mit der Option `timeformat` wird das Format angegeben, in dem die Systemzeit angezeigt oder eingegeben werden soll.

Der Client für Sichern/Archivieren und der Verwaltungsclient erhalten standardmäßig Formatinformationen aus der Ländereinstellungsdefinition, die beim Aufruf des Clients aktiv ist. Ausführliche Informationen zur Definition der länderspezifischen Angaben können der Dokumentation auf dem lokalen System entnommen werden.

Anmerkung: Die Option `timeformat` betrifft nicht den Web-Client. Der Web-Client verwendet das Zeitformat der Ländereinstellung, die im Browser aktiv ist. Ist im Browser eine Ländereinstellung aktiv, die der Client nicht unterstützt, verwendet der Web-Client das Zeitformat für amerikanisches Englisch.

Die Option `timeformat` können Sie in folgenden Befehlen verwenden:

- **delete archive**
- **delete backup**
- **expire**
- **query archive**
- **query backup**
- **query filespace**
- **query image**

- **query nas**
- **restore**
- **restore image**
- **restore nas**
- **retrieve**
- **set event**

Wenn Sie die Option `timeformat` mit einem Befehl eingeben, muss diese Option vor den Optionen `fromtime`, `pittime` und `totime` stehen.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (`dsm.opt`) ein. Sie können diese Option auf der Registerkarte **Regionale Einstellungen** im Feld **Zeitformat** im Profileditor definieren.

Syntax

►►—`TIMEformat`— —*Formatnummer*—►►

Parameter

Formatnummer

Zeigt die Zeit in einem der hier aufgeführten Formate an. Wählen Sie die `Formatnummer` aus, die dem zu verwendenden Format entspricht. Wenn Sie die Option `timeformat` in einem Befehl eingeben, muss sie vor den Optionen `fromtime`, `pittime` und `totime` stehen.

- 0** Das durch die Ländereinstellung definierte Zeitformat verwenden (gilt nicht für Mac OS X). Dieser Wert ist der Standardwert, wenn das durch die Ländereinstellung angegebene Format aus Ziffern, Trennzeichen und, falls anwendbar, der Zeichenfolge AM oder PM besteht.
- 1** 23:00:00
Dies ist der Standardwert, wenn das durch die Ländereinstellung angegebene Format nicht aus Ziffern, Trennzeichen und, falls anwendbar, der Zeichenfolge AM oder PM besteht.
- 2** 23,00,00
- 3** 23.00.00
- 4** 12:00:00 A/P
- 5** A/P 12:00:00

Beispiele

Optionsdatei:

`timeformat 4`

Befehlszeile:

`-time=3`

Diese Option ist in der Anfangsbefehlszeile und im interaktiven Modus gültig. Wird die Option im interaktiven Modus eingegeben, ist nur der Befehl betroffen, mit dem sie eingegeben wird. Wenn dieser Befehl beendet ist, wird der Wert auf den Wert zu Beginn der interaktiven Sitzung zurückgesetzt. Dies ist der Wert aus der Datei `dsm.opt`, sofern er nicht durch die Anfangsbefehlszeile oder eine vom Server erzwungene Option überschrieben wurde.

Weitere Hinweise zur Angabe von Datums- und Zeitformaten

Das Datums- oder Zeitformat, das Sie mit dieser Option angeben, muss verwendet werden, wenn Optionen verwendet werden, deren Eingabe aus Datums- und Zeitangaben besteht. Beispiele sind: `totime`, `fromtime`, `today`, `fromdate` und `pittime`.

Wenn Sie beispielsweise die Option `timeformat` als `TIMEFORMAT 4` angeben, muss der Wert, den Sie für die Option `fromtime` oder `totime` angeben, als Zeit angegeben werden, wie z. B. `12:24:00pm`. Die Angabe `13:24:00` wäre nicht gültig, da `TIMEFORMAT 4` als Angabe für die Stunde eine ganze Zahl, die kleiner-gleich 12 ist, erfordert. Wenn in einer Option für die Stunde Werte bis zu 24 angegeben und Kommas als Trennzeichen verwendet werden sollen, müssen Sie `TIMEFORMAT 2` angeben.

Datums- und Zeitformate in der Konfigurationsdatei für die Systemländereinstellung konfigurieren

Sie können Datums- und Zeitformate angeben, indem Sie diese in der Ländereinstellungsdatei des Systems konfigurieren. Wenn Sie Datums- und Zeitformate in der Ländereinstellungsdatei angeben, müssen diese mithilfe einer Untermenge von Formatkennungen definiert werden, die Zahlen erstellen und von der Funktion `strftime()` der Programmiersprache C unterstützt werden. Sie können Datums- und Zeitformate in den Konfigurationseinstellungen für Ihre Ländereinstellung mithilfe der folgenden Kennungen definieren.

Datumskennungen

- `%Y` - das Jahr, angegeben mit 4 Ziffern, z. B. 2011
- `%y` - das Jahr, Angabe nur der letzten beiden Ziffern, z. B. 11 (nicht 2011)
- `%m` - der Monat, angegeben als Dezimalzahl (1-12)
- `%d` - der Tag des Monats (1-31)

In den Datumskennungen können Sie nur eine einzige Jahreskennung angeben. Sie dürfen `%Y` und `%y` nicht gleichzeitig angeben. Der Modifikator `E` (Großbuchstabe `E`) kann vor Datumskennungen stehen, um das Alternativformat der Ländereinstellung für das Jahr, den Monat oder den Tag zu erstellen. Wenn kein Alternativformat vorhanden ist, wird der Modifikator `E` ignoriert. Trennen Sie die Kennungen durch ein einzelnes 7-Bit-ASCII-Zeichen voneinander. Häufig verwendete Trennzeichen umfassen Doppelpunkte (`:`), Kommas (`,`), Punkte (`.`), Bindestriche (`-`) und Schrägstriche (`/`). Sie dürfen keine Mehrbytezeichen als Trennzeichen verwenden.

Zeitkennungen

- `%H` - die Stunde, angegeben im 24-Stunden-Format (00-23)
- `%I` - die Stunde, angegeben im 12-Stunden-Format (00-12)
- `%M` - die Minuten nach der Stunde (00-59)
- `%S` - die Sekunden nach der Minute (00-59)
- `%p` - fügt den Anzeiger AM (vor 12 Uhr mittags) oder PM (nach 12 Uhr mittags) ein.

In den Zeitkennungen können Sie nur eine einzige Stundenkennung angeben. Sie dürfen %I und %H nicht gleichzeitig angeben.

Der Modifikator O (Großbuchstabe O) kann vor Zeitkennungen stehen, um das Alternativformat der Ländereinstellung für die Stunde, die Minuten oder die Sekunden zu erstellen. Der Modifikator O darf nicht vor der Kennung %p stehen. Trennen Sie die Kennungen durch ein einzelnes 7-Bit-ASCII-Zeichen voneinander. Häufig verwendete Trennzeichen umfassen Doppelpunkte (:), Kommas (,) oder Punkte (.). Sie dürfen keine Mehrbytezeichen als Trennzeichen verwenden. Zwischen der Kennung %p und dem Trennzeichen, das vor oder hinter der Kennung steht, dürfen Sie kein Trennzeichen angeben.

Beispiele für in den Ländereinstellungen konfigurierte Zeitformate

Um ein bestimmtes Zeitformat zu definieren, editieren Sie die Konfigurationsdatei für die Ländereinstellung und ändern Sie die Zeile t_fmt gemäß den Anforderungen. Das ausgewählte Zeitformat gilt sowohl für die Ausgabe als auch für die Eingabe. Nachdem die Konfigurationsdatei für die Ländereinstellung editiert wurde, muss der Befehl localedef ausgeführt werden, um die endgültige Ländereinstellungsdatei zu erstellen.

Tabelle 78. Mustereinstellungen für das Zeitformat in der Konfigurationsdatei für die Ländereinstellung (Zeile t_fmt)

Beispiel	Ergebnis
"%H:%M:%S"	Zeigt die Zeit im Format hh:mm:ss an; hh liegt im Bereich von 0 bis 23.
"%H,%M,%S"	Zeigt die Zeit im Format hh,mm,ss an; hh liegt im Bereich von 0 bis 23.
"%I,%M,13p"	Zeigt die Zeit im Format hh,mm,ssA/P an, wobei hh (Stunde) den Bereich 1 bis 12 aufweist und A/P die Abkürzung für ante-meridian (vormittags, AM in Englisch) oder post-meridian (nachmittags, PM in Englisch) ist.

Beispiele für in den Ländereinstellungen konfigurierte Datumsformate

Um ein bestimmtes Datumsformat zu definieren, editieren Sie die Konfigurationsdatei und ändern Sie die Zeile d_fmt gemäß Ihren Anforderungen. Das ausgewählte Datumsformat gilt sowohl für die Ausgabe als auch für die Eingabe.

Tabelle 79. Mustereinstellungen für das Datumsformat in der Konfigurationsdatei für die Ländereinstellung (Zeile d_fmt)

Beispiel	Ergebnis
"%m/%d/%y"	Zeigt das Datum im Format MM/TT/JJ an.
"%d.%m.%Y"	Zeigt das Datum im Format TT.MM.JJJJ an.

Toc

Verwenden Sie die Option toc mit dem Befehl backup nas oder der Option include.fs.nas, um anzugeben, ob der Client für Sichern/Archivieren Inhaltsverzeichnisangaben (TOC) für jede Dateisystemsicherung speichern soll.

Sie sollten bei der Entscheidung, ob die Inhaltsverzeichnisangaben (TOC-Angaben) gesichert werden sollen, Folgendes berücksichtigen:

- Wenn Sie TOC-Angaben sichern, können Sie den Serverbefehl `QUERY TOC` verwenden, um den Inhalt einer Dateisystemsicherung festzustellen, sowie den Serverbefehl `RESTORE NODE`, um einzelne Dateien oder Verzeichnisstrukturen zurückzuschreiben.
- Sie können auch die GUI des Windows-Clients für Sichern/Archivieren verwenden, um die gesamte Baumstruktur des Dateisystems zu untersuchen und zurückzuschreibende Dateien und Verzeichnisse auszuwählen.
- Die Erstellung eines Inhaltsverzeichnisses erfordert, dass Sie das Attribut `TOCDESTINATION` in der Sicherungskopiengruppe für die Verwaltungsklasse definieren, an die dieses Sicherungsimage gebunden wird. Beachten Sie, dass die TOC-Erstellung während der Sicherungsoperation eine zusätzliche Verarbeitung, zusätzliche Netzressourcen, zusätzlichen Speicherpoolspeicher und möglicherweise einen zusätzlichen Mountpunkt erfordert.
- Wenn Sie keine TOC-Angaben sichern, können Sie über den Serverbefehl `RESTORE NODE` dennoch einzelne Dateien und Verzeichnisstrukturen zurückschreiben, wenn Sie den vollständig qualifizierten Namen jeder Datei bzw. jedes Verzeichnisses und das Image kennen, in dem das Objekt gesichert wurde.

Unterstützte Clients

Diese Option ist nur für AIX- und Solaris-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie die Anweisung `include.fs.nas`, die den Wert `toc` enthält, in die Datei `dsm.sys` innerhalb einer Serverzeilengruppe ein.

Syntax



Parameter

Yes

Gibt an, dass der Client während einer NAS-Dateisystemimagesicherung TOC-Angaben speichert. Die Sicherung schlägt jedoch fehl, wenn während der Erstellung des Inhaltsverzeichnisses ein Fehler auftritt.

No Gibt an, dass der Client während einer NAS-Dateisystemimagesicherung keine TOC-Angaben speichert.

Preferred

Gibt an, dass der Client während einer NAS-Dateisystemimagesicherung TOC-Angaben speichert. Die Sicherung schlägt nicht fehl, wenn während der Erstellung des Inhaltsverzeichnisses ein Fehler auftritt. Dies ist der Standardwert.

Anmerkung: Ist die Option `mode` auf `differential` gesetzt und setzen Sie die Option `toc` auf `preferred` oder `yes`, ohne dass das letzte vollständige Image über ein Inhaltsverzeichnis (TOC) verfügt, führt der Client eine vollständige Imagesicherung aus und erstellt ein TOC.

Beispiele

Optionsdatei:

```
include.fs.nas netappsj/vol/vol0 homemgmtclass toc=yes
```

Befehlszeile:

```
backup nas -nasnodename=netappsj /vol/vol0 -toc=yes
```

Todate

Mit der Option `todate` können Sie in Verbindung mit der Option `totime` ein Enddatum und eine Endzeit angeben, bis zu der Sie während einer Zurückschreibungs-, Abruf- oder Abfrageoperation nach Sicherungen oder Archivierungen suchen wollen.

Mit den Optionen `todate` und `totime` kann in Verbindung mit den Optionen `fromtime` und `fromdate` eine Liste der in einem bestimmten Zeitraum gesicherten oder archivierten Dateien angefordert werden. Es kann beispielsweise eine Liste mit Dateien angefordert werden, die zwischen 6:00 Uhr am 1. Juli 2002 und 23:59 Uhr am 30. Juli 2002 gesichert wurden.

Die Option `todate` ist in den folgenden Befehlen zu verwenden:

- **delete backup**
- **query archive**
- **query backup**
- **restore**
- **restore group**
- **retrieve**

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

►► —TODate = — —Datum—————►►

Parameter

Datum

Gibt ein Enddatum an. Das Datum muss in dem mit der Option `dateformat` ausgewählten Format eingegeben werden.

Wenn `dateformat` in einem Befehl angegeben wird, muss diese Option vor den Optionen `fromdate`, `pitdate` und `todate` stehen.

Beispiele

Befehlszeile:

```
dsmc restore "/Users/agordon/Documents/*" -todate=12/11/2003
```

Befehlszeile:

```
dsmc restore "/home/user1/*" -todate=12/11/2003
```

Totime

Mit der Option `totime` können Sie in Verbindung mit der Option `todate` ein Enddatum und eine Endzeit angeben, bis zu der Sie während einer Zurückschreibungs-, Abruf- oder Abfrageoperation nach Sicherungen oder Archivierungen suchen wollen. Der Client für Sichern/Archivieren ignoriert diese Option, wenn Sie die Option `todate` nicht angeben.

Mit den Optionen `totime` und `todate` kann in Verbindung mit den Optionen `fromtime` und `fromdate` eine Liste der in einem bestimmten Zeitraum gesicherten Dateien angefordert werden. Beispielsweise können Sie eine Liste mit Dateien anfordern, die zwischen 6:00 Uhr am 1. Juli 2003 und 23:59 Uhr am 30. Juli 2003 gesichert wurden.

Die Option `totime` ist in den folgenden Befehlen zu verwenden:

- **delete backup**
- **query archive**
- **query backup**
- **restore**
- **restore group**
- **retrieve**

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

►► —TOMTime = — —Zeit— ◀◀

Parameter

Zeit

Gibt eine Endzeit an. Wenn keine Zeit angegeben wird, lautet der Standardwert 23:59:59. Die Zeit muss in dem mit der Option `timeformat` ausgewählten Format angegeben werden.

Wenn die Option `timeformat` in einem Befehl angegeben wird, muss sie vor den Optionen `fromtime`, `pittime` und `totime` stehen.

Beispiele

Befehlszeile:

```
dsmc restore "/Users/van/Documents/myfiles/*" -todate=09/17/2003  
-totime=23:00:00
```

Befehlszeile:

```
dsmc restore "/home/user1/*" -todate=09/17/2003 -totime=23:00:00
```

Txnbytelimit

Mit der Option `txnbytelimit` wird die Anzahl Kilobyte angegeben, die das Clientprogramm puffert, bevor eine Transaktion an den Server gesendet wird.

Eine *Transaktion* ist die Arbeitseinheit, die zwischen dem Client und dem Server ausgetauscht wird. Eine Transaktion kann mehrere Dateien oder Verzeichnisse enthalten. Diese werden als *Transaktionsgruppe* bezeichnet.

Mit der Option `txnbytelimit` können Sie steuern, wie viele Daten zwischen Client und Server gesendet werden, bevor der Server die Daten und Änderungen in der Serverdatenbank festschreibt. Die Steuerung des gesendeten Datenvolumens wirkt sich auf die Geschwindigkeit aus, mit der der Client die Transaktionen ausführt. Die gesendete Datenmenge gilt, wenn Dateien während der Sicherung zusammengefasst werden oder wenn Dateien während einer Zurückschreibung vom Server empfangen werden.

Wenn die in `txngroupmax` angegebene Anzahl erreicht ist, sendet der Client die Dateien an den Server, auch wenn der Bytegrenzwert für die Transaktion nicht erreicht ist.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Allgemein** im Feld **Transaktionspuffergröße** des Profileditors definieren.

Syntax

►—TXNBytelimit— —*Nummer*—►

Parameter

Zahl

Gibt die Anzahl Kilobyte an, die das Clientprogramm an den Server sendet, bevor die Transaktion festgeschrieben wird. Der Wertebereich ist 300 bis 34359738368 (32 GB). Der Standardwert ist 25600 KB. Die Anzahl kann als Ganzzahl oder als Ganzzahl mit einem der folgenden Qualifikationsmerkmale für die Einheit angegeben werden:

- K oder k (Kilobyte)
- M oder m (Megabyte)
- G oder g (Gigabyte)

Wird kein Qualifikationsmerkmal für die Einheit angegeben, wird Kilobyte für die Ganzzahl verwendet.

Einschränkung: Die Option `txnbytelimit` unterstützt keine Dezimalzahlen und nur ein Buchstabe für die Einheit ist zulässig. Beispiele: K, M oder G.

Beispiele

Optionsdatei:

```
txnb 25600
txnb 2097152
txnb 2097152k
txnb 2048m
```

```
txnb 2g
```

```
txnb 32G
```

Befehlszeile:

```
-txnb=25600
```

```
-txnb=16G
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Type

Verwenden Sie die Option **type** im Befehl **query node**, um den Typ des abzufragenden Knotens anzugeben. Verwenden Sie diese Option im Befehl **set event**, um eine Löschsperre zu aktivieren oder freizugeben bzw. um den Aufbewahrungszeitraum zu starten.

Unterstützte Clients

Diese Option ist auch für den Befehl **set password** mit dem Typ TSM auf AIX-Clients gültig.

Diese Option ist nur für AIX- und Solaris-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax



Parameter

nas

Gibt alle auf dem Server registrierten NAS-Knoten an.

server

Gibt Clientknoten an, die andere IBM Spectrum Protect-Server sind.

client

Gibt Clientknoten an, die Clients für Sichern/Archivieren sind.

Beispiele

Befehlszeile:

```
query node -type=nas
```

Updatectime

Überprüfen Sie mithilfe der Option **updatectime** das Attribut für die Änderungszeit (**ctime**) während einer Teilsicherungsoperation.

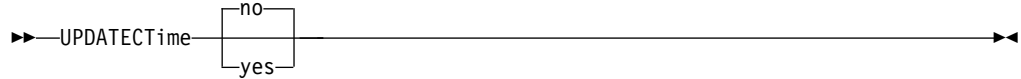
Unterstützte Clients

Diese Option ist nur für AIX- und Linux-Clients in GPFS-Dateisystemen gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein.

Syntax



Parameter

no Der Client für Sichern/Archivieren überprüft während einer Sicherungsoperation nicht das Attribut für die Änderungszeit (ctime). Dies ist der Standardwert.

yes

Der Client für Sichern/Archivieren überprüft während einer Sicherungsoperation das Attribut für die Änderungszeit (ctime). Wenn sich das Attribut ctime seit der letzten Sicherungsoperation geändert hat, wird das Attribut ctime auf dem IBM Spectrum Protect-Server aktualisiert. Das Objekt wird nur gesichert, wenn es über ACLs oder erweiterte Attribute verfügt. Der Client überprüft Dateien und Verzeichnisse.

Beispiele

Optionsdatei:

updatect yes

Befehlszeile:

dsmc incr /proj/gpfs/test/ -updatectime=yes

Useexistingbase

Die Option useexistingbase wird verwendet, wenn Sie Momentaufnahmen sichern, die sich auf NetApp-Dateiserverdatenträgern befinden. Die Option useexistingbase gibt an, dass die jüngste Momentaufnahme, die sich auf dem zu sichernden Datenträger befindet, als Basismomentaufnahme während einer Momentaufnahmedifferenzsicherung verwendet werden soll.

Wenn diese Option nicht angegeben wird, wird eine neue Momentaufnahme auf dem Datenträger erstellt, der gesichert wird. Da Zielfeilserverserverdatenträger schreibgeschützt sind, muss useexistingbase bei der Ausführung von Momentaufnahmedifferenzsicherungen von Zielfeilserverserverdatenträgern angegeben werden. Wenn useexistingbase nicht angegeben wird, schlagen Momentaufnahmedifferenzsicherungen eines Zielfeilserverserverdatenträgers fehl, weil die neue Momentaufnahme auf dem schreibgeschützten Datenträger nicht erstellt werden kann.

Verwenden Sie bei der Sicherung von Zielfeilserverserverdatenträgern sowohl die Option useexistingbase als auch die Option diffsnapshot=latest, um sicherzustellen, dass während der Datenträgersicherung die neuesten Basis- und Differenzmomentaufnahmen verwendet werden.

Unterstützte Clients

Diese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Optionsdatei

Diese Option ist nur in der Befehlszeile gültig.

Syntax

►►—USEEXISTINGBase—◄◄

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Optionsdatei:

Nicht zutreffend.

Befehlszeile:

```
dsmc incr \\DRFiler\UserDataVol_Mirror_Share -snapdiff
-useexistingbase -basenameshotname="nightly.?"
```

Zugehörige Informationen

Basesnapshotname

User replication failover

Die Option `usereplicationfailover` gibt an, ob die automatisierte Clientübernahme auf einem Clientknoten stattfindet.

Mit dieser Option können Sie die Übernahme eines Clientknotens aktivieren oder verhindern, dass eine Übernahme eines Clientknotens auf dem Sekundärserver stattfindet. Diese Option setzt die Konfiguration außer Kraft, die durch die Einstellungen des IBM Spectrum Protect-Serveradministrators auf dem Primärserver angegeben ist.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in eine Serverzeilengruppe in der Datei `dsm.sys` ein.

Syntax

```

graph LR
    Start(( )) --> UserReplicationFailover[USERREPLICATIONFailover]
    UserReplicationFailover -- Yes --> End(( ))
    UserReplicationFailover -- No --> End

```

Parameter

Yes

Gibt an, dass eine automatische Übernahme des Clients auf dem Sekundärserver stattfinden soll, falls der Primärserver nicht verfügbar ist. Der Client ver-

wendet die durch den Primärserver bereitgestellte Konfiguration, um eine Verbindung zum Sekundärserver herzustellen. Dies ist der Standardwert.

No Gibt an, dass keine automatische Übernahme des Clients auf dem Sekundärserver stattfindet.

Beispiele

Optionsdatei:

USEREPLICATIONFailover no

Befehlszeile:

Nicht zutreffend.

Zugehörige Konzepte:

„Konfiguration und Verwendung der automatisierten Clientübernahme“ auf Seite 98

Zugehörige Tasks:

„Client für automatisierte Übernahme konfigurieren“ auf Seite 102

Users (veraltet)

Diese Option ist veraltet.

V2archive

Verwenden Sie die Option `v2archive` im Befehl **archive**, um anzugeben, dass nur Dateien auf dem Server archiviert werden sollen.

Der Client für Sichern/Archivieren verarbeitet keine Verzeichnisse, die in dem Pfad der Quelldateispezifikation vorhanden sind.

Diese Option unterscheidet sich von der Option `filesonly` dadurch, dass bei der Option `filesonly` die Verzeichnisse, die im Pfad der Quelldateispezifikation bestehen, archiviert werden.

Die Optionen `v2archive` und `dirsonly` schließen sich gegenseitig aus und es wird eine Fehlermeldung angezeigt, wenn Sie beide Optionen zusammen im Befehl **archive** verwenden.

Wenn Sie diese Option verwenden, sollten Sie Folgendes berücksichtigen:

- Es kommt unter Umständen zu Leistungsproblemen, wenn große Datenmengen abgerufen werden, die mit dieser Option archiviert wurden.
- Sie sollten diese Option nur verwenden, wenn Sie über die Verfallsleistung auf einem Server besorgt sind, der bereits extrem große Mengen an archivierten Daten enthält.
- Gibt es mehrere Dateien mit demselben Namen für die Option `v2archive`, werden die Dateien mehrfach mit ihrer Verzeichnisstruktur archiviert. Die Option `v2archive` archiviert nur die Dateien.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

►—V2archive—◄

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Dieser Befehl:

```
dsmc archive "/Users/user2/Documents/*" -v2archive -su=y.
```

Archiviert diese Dateien:

```
/Users/user2/Documents/file1  
/Users/user2/Documents/file2  
/Users/user2/Documents/file3  
/Users/user2/Documents/dir2/file4  
/Users/user2/Documents/dir2/file5
```

Anmerkung: Der Client archiviert /Users/user2/Documents und /Users/user2/Documents/dir2 nicht.

Dieser Befehl:

```
dsmc archive "/home/relx/dir1/*" -v2archive -su=y.
```

Archiviert diese Dateien:

```
/home/relx/dir1/file1  
/home/relx/dir1/file2  
/home/relx/dir1/file3  
/home/relx/dir1/dir2/file4  
/home/relx/dir1/dir2/file5
```

Anmerkung: Der Client archiviert /home/relx/dir1 und /home/relx/dir1/dir2 nicht.

Verbose

Mit der Option **verbose** können Sie angeben, dass Sie detaillierte Verarbeitungsinformationen auf Ihrem Bildschirm anzeigen wollen. Dies ist der Standardwert.

Bei der Ausführung des Befehls **incremental**, **selective** oder **archive** werden Informationen zu allen Dateien angezeigt, die gesichert werden. Verwenden Sie die Option **quiet**, wenn diese Informationen nicht angezeigt werden sollen.

Das folgende Verhalten gilt, wenn die Optionen **verbose** und **quiet** verwendet werden:

- Wenn der Server entweder die Option **quiet** oder **verbose** in der Clientoptionsgruppe des Servers angibt, überschreiben die Servereinstellungen die Clientwerte, auch wenn auf dem Server für **force** der Wert *no* definiert ist.
- Wenn Sie **quiet** in Ihrer Datei `dsm.opt` und **-verbose** in der Befehlszeile angeben, hat **-verbose** Vorrang.
- Wenn Sie sowohl **-quiet** als auch **-verbose** in demselben Befehl angeben, hat die letzte Option, die bei der Optionsverarbeitung festgestellt wird, Vorrang. Wenn Sie **-quiet -verbose** angeben, hat **-verbose** Vorrang. Wenn Sie **-verbose -quiet** angeben, hat **-quiet** Vorrang.

Die Informationen werden im Fenster 'Schedulerstatus' auf Ihrem Bildschirm angezeigt. Diese Option ist nur gültig, wenn der Scheduler aktiv ist und der Client geplante Arbeit ausführt.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte **Befehlszeile** über das Kontrollkästchen **Keine Verarbeitungsdaten auf dem Bildschirm anzeigen** im Profileditor definieren.

Syntax

►►—Verbose—►►

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Optionsdatei:

verbose

Befehlszeile:

-verbose

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Verifyimage

Verwenden Sie die Option `verifyimage` im Befehl **restore image**, um anzugeben, dass die Feststellung von defekten Sektoren auf dem Zieldatenträger aktiviert werden soll.

Werden defekte Sektoren auf dem Zieldatenträger festgestellt, gibt der Client für Sichern/Archivieren eine Warnung auf der Konsole und im Fehlerprotokoll aus.

Unterstützte Clients

Diese Option ist nur für AIX-, Oracle Solaris- und alle Linux-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

►►—VERIFYImage—►►

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
dsmc restore image /usr -verifyimage
```

Virtualfsname

Verwenden Sie die Option **virtualfsname** im Befehl **backup group**, um den Namen des virtuellen Dateibereichs für die Gruppe anzugeben, mit dem die Operation ausgeführt werden soll. Die Angabe für **virtualfsname** darf nicht mit einem vorhandenen Dateibereichsnamen übereinstimmen.

Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients außer Mac OS X gültig.

Syntax

►—VIRTUALfsname =— —*Dateibereichsname*—►

Parameter

Dateibereichsname

Gibt den Namen des Containers für die Gruppe an, mit dem die Operation ausgeführt werden soll.

Beispiele

Befehlszeile:

```
backup group -filelist=/Users/van/Documents/filelist1 -groupname=group1  
-virtualfsname=/virtfs -mode=full  
backup group -filelist=/home/dir1/filelist1 -groupname=group1  
-virtualfsname=/virtfs -mode=full
```

Virtualmountpoint

Die Option **virtualmountpoint** definiert einen virtuellen Mountpunkt für ein Dateisystem, wenn Dateien für die Sicherung berücksichtigt werden sollen, die mit einem bestimmten Verzeichnis innerhalb dieses Dateisystems beginnen.

Die Verwendung der Option **virtualmountpoint** zum Angeben eines Verzeichnisses innerhalb eines Dateisystems ermöglicht einen direkten Pfad zu den Dateien, die gesichert werden sollen, wodurch sich die Verarbeitungszeit verkürzt. Das Definieren eines virtuellen Mountpunktes innerhalb eines Dateisystems ist effizienter als das Definieren dieses Dateisystems mit Hilfe der Option **domain** und das anschließende Ausschließen der Dateien, die nicht gesichert werden sollen, mit der Option **exclude** in der Einschluss-/Ausschlussoptionsliste.

Mit der Option **virtualmountpoint** können virtuelle Mountpunkte für mehrere Dateisysteme, für lokale und ferne Dateisysteme und mehrere virtuelle Mountpunkte innerhalb desselben Dateisystems definiert werden. Virtuelle Mountpunkte können in einem Dateisystem, das durch ein automatisches Mountprogramm bearbeitet wird, nicht verwendet werden.

Sie können die Option **virtualmountpoint** verwenden, um nicht unterstützte Dateisysteme mit bestimmten Einschränkungen zu sichern. Informationen zur Verwen-

dition von `virtualmountpoint` mit nicht unterstützten Dateisystemen befinden sich in „Dateisystem- und ACL-Unterstützung“ auf Seite 174.

Anmerkung: Wenn es sich bei dem Verzeichnis, das als virtueller Mountpunkt angegeben werden soll, um eine symbolische Verbindung handelt, muss für die Option `followsymbolic` der Wert `Yes` definiert werden. Wenn für diese Option `no` (der Standardwert) definiert wird, ist die Verwendung einer symbolischen Verbindung als virtueller Mountpunkt nicht zulässig. Zudem gilt: Wenn Sie ein Dateisystem sichern, dann einen virtuellen Mountpunkt hinzufügen und anschließend eine weitere Teilsicherung für das Dateisystem ausführen, verfallen die Dateien und Verzeichnisse in dem als virtueller Mountpunkt definierten Verzeichnis, da sie logisch in dem als virtueller Mountpunkt definierten Verzeichnis und nicht im Dateisystem enthalten sind.

Nach der Definition eines virtuellen Mountpunkts können Sie den Pfad und Verzeichnisnamen mit der Option `domain` entweder in der Clientoptionsdatei oder im Befehl **incremental** angeben, damit er bei Teilsicherungen berücksichtigt wird. Wenn Sie mit der Option `virtualmountpoint` eine Sicherung oder Archivierung ausführen, listet der Befehl **query filespace** in seiner Antwort den virtuellen Mountpunkt zusammen mit den anderen Dateisystemen auf. Im Allgemeinen werden Verzeichnisse, die Sie als virtuelle Mountpunkte definieren, als tatsächliche Dateisysteme behandelt, und sie erfordern, dass die Option `virtualmountpoint` in der Datei `dsm.sys` angegeben ist, damit die Dateien zurückgeschrieben oder abgerufen werden können.

Anmerkung: Wenn Sie eine Option `virtualmountpoint` angeben, wird der von dieser angegebene Pfad der Standardsicherungsdomäne (domain all-local) hinzugefügt. Der `virtualmountpoint`-Pfad wird immer als lokaler "Mountpunkt" angesehen, unabhängig vom Typ des realen Dateisystems, auf das er verweist.

Unterstützte Clients

Diese Option ist für alle UNIX-Clients außer Mac OS X gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Syntax



Parameter

Verzeichnis

Gibt den Pfad und den Verzeichnisnamen für das Verzeichnis an, das als virtueller Mountpunkt für ein Dateisystem verwendet werden soll. Im Pfad und im Verzeichnisnamen dürfen keine Platzhalterzeichen verwendet werden.

Definieren Sie nur einen virtuellen Mountpunkt für jede Option `virtualmount-point`, die Sie in Ihre Clientsystemoptionsdatei einfügen. Die Option

virtualmountpoint können Sie nach Bedarf so oft angeben, dass alle gewünschten virtuellen Mountpunkte definiert werden.

Beispiele

Optionsdatei:

```
virtualmountpoint /afs/xyzcorp.com/home/ellen  
virtualmountpoint /afs/xyzcorp.com/home/ellen/test/data
```

Befehlszeile:

Nicht zutreffend.

Virtualnodename

Die Option `virtualnodename` gibt den Knotennamen Ihrer Workstation an, wenn Sie Dateien auf einer anderen Workstation zurückschreiben oder abrufen wollen.

Wenn Sie die Option `virtualnodename` in Ihrer Clientoptionsdatei oder in einem Befehl verwenden, gilt Folgendes:

- Sie müssen den Namen angeben, den Sie mit der Option `nodename` in Ihrer Clientensystemoptionsdatei (`dsm.sys`) angegeben haben. Dieser Name sollte sich von dem Namen unterscheiden, den der Befehl **hostname** auf Ihrer Workstation zurückgibt.
- Der Client fordert Sie zur Eingabe des Kennworts auf, das dem angegebenen Knoten zugeordnet ist, falls ein Kennwort erforderlich ist (auch wenn die Option `passwordaccess` auf `generate` gesetzt ist). Wenn Sie das korrekte Kennwort eingeben, haben Sie Zugriff auf alle Sicherungen und Archivierungen, die von dem angegebenen Knoten ausgingen.

Wenn eine Verbindung zu einem Server hergestellt wird, muss sich der Client beim Server identifizieren. Diese Anmeldeidentifikation wird wie folgt bestimmt:

- Sind die Optionen `nodename` und `virtualnodename` nicht angegeben und wird kein virtueller Knotenname in der Befehlszeile angegeben, gibt der Befehl **hostname** den Namen der Standardanmelde-ID zurück.
- Ist die Option `nodename` angegeben, überschreibt der mit der Option `nodename` angegebene Name den Namen, der vom Befehl **hostname** zurückgegeben wird.
- Ist die Option `virtualnodename` angegeben oder wird ein virtueller Knotenname in der Befehlszeile angegeben, darf dieser Name nicht dem Namen entsprechen, den der Befehl **hostname** zurückgibt.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (`dsm.opt`) ein.

Syntax

►►—VIRTUALNodename— —Knotenname—————◄◄

Parameter

Knotenname

Gibt einen aus 1 bis 64 Zeichen bestehenden Namen an, der den Knoten identifiziert, für den IBM Spectrum Protect-Services angefordert werden sollen. Es gibt keinen Standardwert.

Beispiele

Optionsdatei:

```
virtualnodename cougar
```

Befehlszeile:

```
-virtualn=banshee
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.

Vmbackdir

Die Option `vmbackdir` gibt die temporäre Plattenposition an, an der der Client Steuerdateien speichert, die während VM-Gesamtsicherungs- und -Zurückschreibungsoperationen für virtuelle Maschinen erstellt werden.

Unterstützte Einheiten zum Versetzen von Daten



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Wenn ein Client auf einem Knoten der Einheit zum Versetzen von Daten eine VM-Gesamtsicherung einer virtuellen Maschine startet, erstellt der Client Metadaten in Dateien, die der gesicherten virtuellen Maschine und ihren Daten zugeordnet werden. Die Dateien, die die Metadaten enthalten, werden als *Steuerdateien* bezeichnet.

Bei VM-Gesamtsicherungsoperationen werden Metadaten auf einer Platte des Knotens der Einheit zum Versetzen von Daten gespeichert, bis die Sicherung beendet ist und sowohl die Daten der virtuellen Maschine als auch die Steuerdateien im Serverspeicher gespeichert werden. Bei einer vollständigen VM-Zurückschreibungsoperation werden die Steuerdateien vom Server kopiert und temporär auf der Platte der Einheit zum Versetzen von Daten gespeichert. Dort werden sie zur Zurückschreibung der virtuellen Maschine und ihrer Daten verwendet. Nach der Beendigung einer Sicherungs- oder Zurückschreibungsoperation werden die Steuerdateien nicht mehr benötigt und der Client löscht sie aus der temporären Plattenposition.

Das durch diese Option angegebene Verzeichnis muss sich auf einem Laufwerk befinden, das so viel freien Speicherbereich enthält, dass die Steuerinformationen aus einer vollständigen VM-Sicherung gespeichert werden können.

Diese Option ist für Linux- und Windows-Einheiten zum Versetzen von Daten gültig, die auf einem vStorage-Sicherungsserver installiert sind.

Optionsdatei

Definieren Sie diese Option in der Clientoptionsdatei oder geben Sie sie in die Befehlszeile als Option für den Befehl **backup vm** oder **restore vm** ein.

Syntax

►►—VBACKDir—Verzeichnis—►►

Parameter

Verzeichnis

Gibt den Pfad an, in dem die Steuerdateien auf dem Sicherungsserver gespeichert werden.

Der Standardwert ist /tmp/tsmvmbackup/fullvm/

Beispiele

Optionsdatei:

```
VBACKD /tmp/tsmvmbackup/
```

Befehlszeile:

```
dsmc backup vm -VBACKUPT=fullvm -VBACKD=/home/vmware/control_files
```

```
dsmc restore vm -VBACKUPT=fullvm -VBACKD=/home/mine/bkup_ctrl
```

Vmbackuplocation

Verwenden Sie die Option `vmbackuplocation` mit dem Befehl **backup vm** oder **restore vm**, um die Sicherungsposition für Sicherungs- und Zurückschreibungsoperationen für virtuelle Maschinen anzugeben.

Diese Option ist nur für virtuelle VMware-Maschinen gültig. Für diese Option benötigen Sie eine Lizenzvereinbarung für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Für Zurückschreibungsoperationen wird diese Option ignoriert, wenn die Option **vmrestoretype** auf `mountcleanup` oder `mountcleanupall` gesetzt ist.

Unterstützte Clients

Diese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Optionsdatei

Diese Option muss in der Befehlszeile eines Befehls **backup vm** oder **restore vm** angegeben werden. Sie können diese Option nicht in der Clientoptionsdatei angeben.

Syntax

►►—VBACKUPLoCation—

SERVER
LOCAL
BOTH

—►►

Parameter

SERVER

Gibt für Sicherungsoperationen an, dass virtuelle Maschinen auf dem IBM Spectrum Protect-Server gesichert werden.

Gibt für Zurückschreibungsoperationen an, dass virtuelle Maschinen vom IBM Spectrum Protect-Server zurückgeschrieben werden.

Dies ist der Standardwert.

LOCAL

Gibt für Sicherungsoperationen an, dass virtuelle Maschinen im Hardwarespeicher gesichert werden. Bei der Sicherung handelt es sich selbst dann um eine vollständige Imagemomentaufnahmen virtueller Maschinen, wenn eine Teilsicherung angegeben ist.

Um eine lokale Sicherung erstellen zu können, muss die virtuelle Maschine in einem VMware-Datenspeicher für virtuelle Datenträger (VVOL) gespeichert sein. Wenn sich eine virtuelle Platte der virtuellen Maschine nicht in einem VVOL-Datenspeicher befindet, ist die lokale Sicherung nicht zulässig.

Gibt für Zurückschreibungsoperationen an, dass virtuelle Maschinen aus Momentaufnahmen zurückgeschrieben werden, die im Hardwarespeicher gespeichert sind.

Bei der Zurückschreibung aus einer lokalen Momentaufnahme kann nur eine vorhandene virtuelle Maschine zurückgesetzt werden. Es ist nicht möglich, eine gelöschte virtuelle Maschine zurückzuschreiben oder eine virtuelle Maschine mit einem anderen Namen oder an eine andere Position zurückzuschreiben.

Eine lokale Zurückschreibung ist nicht gültig, wenn die folgenden Parameter im Befehl **restore vm** verwendet werden:

- **VMNAME**
- **DATACENTER**
- **HOST**
- **DATASTORE**
- **:vmdk**

Dieser Wert ist ebenfalls nicht gültig, wenn die Option **vmrestoretype** auf einen der folgenden Werte gesetzt ist. Wenn diese Werte definiert sind, wird eine Fehlermeldung angezeigt.

- **instantaccess**
- **instantrestore**
- **mount**

Da für lokale Momentaufnahmen keine Netzdatenversetzung erforderlich ist, können Sicherungs- und -zurückschreibungsoperationen schneller als Serversicherungs- und Zurückschreibungsoperationen ausgeführt werden.

BOTH

Gibt für Sicherungsoperationen an, dass virtuelle Maschinen sowohl auf dem IBM Spectrum Protect-Server als auch lokal gesichert werden. Bei der lokalen Sicherung handelt es sich immer um eine vollständige Imagemomentaufnahme der VMs, selbst wenn Teilsicherungen für den Server konfiguriert sind.

Gibt für Zurückschreibungsoperationen an, dass virtuelle Maschinen aus der neuesten aktiven Version zurückgeschrieben werden; dies ist unabhängig davon, ob es sich um eine lokale Sicherung oder eine Sicherung auf dem Server handelt. Wenn die Zeitmarke für beide aktive Sicherungen identisch ist, wird die lokale Sicherung für die Zurückschreibung verwendet.

Dieser Wert ist mit den oben für den Wert **LOCAL** aufgelisteten Parametern und Werten für die Option **vmrestoretype** nicht gültig.

Beispiele

Befehlszeile:

Servergesamtsicherung und lokale Sicherung für die virtuelle Maschine vm1 ausführen:

```
dsmc backup vm vm1 -vmbakuplocation=BOTH -vmbakuptype=Fullvm
```

Lokale Zurückschreibung für die virtuelle Maschine vm1 ausführen:

```
dsmc restore vm vm1 -vmbakuplocation=LOCAL
```

Vmbakupmailboxhistory

Die Option `vmbakupmailboxhistory` gibt an, ob die Mailbox-History automatisch mit der VM-Sicherung hochgeladen wird, wenn IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server auf einer virtuellen Maschine erkannt wird.

Unterstützte Clients

Diese Option ist auf Clients gültig, die als Einheit zum Versetzen von Daten für VMware-Gastmaschinensicherungen agieren.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein.

Syntax



Parameter

Yes

Die Mailbox-History wird automatisch mit der VM-Sicherung hochgeladen, wenn IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server auf einer virtuellen Maschine erkannt wird.

No Die Mailbox-History wird nicht automatisch mit der VM-Sicherung hochgeladen.

Beispiele


Optionsdatei:

```
vmbakupmailboxhistory yes
```

Vmbakuptype

Verwenden Sie die Option `vmbakuptype` mit dem Befehl **backup VM** oder **restore VM**, um den Typ der Sicherung oder Zurückschreibung der virtuellen Maschine anzugeben, der ausgeführt werden soll. Sie können diese Option auch in **query**

VM-Befehlen verwenden, um die Abfrageergebnisse zu filtern, sodass nur virtuelle Maschinen angezeigt werden, die mit einem bestimmten Sicherungstyp gesichert wurden. Beispiele finden Sie in der Beschreibung des Befehls **query VM**.

 Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Sie können eine vollständige VM-Sicherung für VMware angeben.

Unterstützte Clients

Diese Option ist für Linux-Einheiten zum Versetzen von Daten gültig, die auf einem vStorage-Sicherungsserver installiert sind. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Syntax

►►—VMBACKUPType Fullvm—►►

Parameter

Fullvm

Geben Sie diesen Wert an, um eine traditionelle VM-Gesamtsicherung einer virtuellen VMware-Maschine auszuführen. Dies ist der Standardsicherungstyp für Linux-Clients.

Beispiele

Optionsdatei:

```
VMBACKUPT full
```

Befehlszeile:

```
dsmc backup vm vm1 -VMBACKUPT=full -vmhost=virtctr  
-vmcuser=virtctr_admin -vmcpw=xxxxx
```

Führt eine vollständige VM-Sicherung der virtuellen Maschine vm1.example.com, die die VMware VirtualCenter-Maschine virtctr.example.com verwendet, auf dem IBM Spectrum Protect-Server unter Verwendung des Maschinennamens vm1 aus.

Vmhost

Verwenden Sie die Option **vmhost** im Befehl **backup VM**, **restore VM** oder **query VM**, um den Hostnamen des VMware VirtualCenter- oder ESX-Servers anzugeben, der gesichert, zurückgeschrieben oder abgefragt werden soll.

Verwenden Sie das VirtualCenter, falls es verfügbar ist. Wenn Sie keinen VirtualCenter-Server verwenden können und Sicherungen mehrerer Systeme auf mehreren ESX-Servern ausführen müssen, geben Sie diese Option nicht an, sondern geben Sie stattdessen die Option mit dem Befehl an, damit sie für jeden ESX-Server variiert werden kann.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Unterstützte Clients

Dieser Befehl ist für Clients gültig, die zur Ausführung einer Off-Host-Sicherung einer virtuellen VMware-Maschine konfiguriert sind. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt), in die Clientsystemoptionsdatei (dsm.sys) oder in die Befehlszeile ein.

Syntax

►►—VMCHost— —Hostname—►►

Parameter

Hostname

Gibt den Hostnamen des VMware VirtualCenter- oder ESX-Servers an, der gesichert, zurückgeschrieben oder abgefragt werden soll.

Beispiele

Optionsdatei:

VMCH vcenter.storage.usca.example.com

Befehlszeile:

-VMCH=esx1.storage.usca.example.com

Vmcpw

Verwenden Sie die Option vmcpw im Befehl **backup VM**, **restore VM** oder **query VM**, um das Kennwort für die VMware VirtualCenter- oder ESX-Benutzer-ID anzugeben, die mit der Option vmcuser angegeben wird.

Verwenden Sie das VirtualCenter, falls es verfügbar ist. Wenn Sie keinen VirtualCenter-Server verwenden können und Sicherungen mehrerer Systeme auf mehreren ESX-Servern ausführen müssen, geben Sie diese Option nicht an, sondern geben Sie stattdessen die Option mit dem Befehl an, damit sie für jeden ESX-Server variiert werden kann.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Unterstützte Clients

Diese Option ist nur auf unterstützten Linux-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind, der zum Sichern einer virtuellen VMware-Maschine verwendet wird.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) oder in die Befehlszeile ein.

1. Klicken Sie auf **Editieren > Clientvorgaben > VM-Sicherung**. Geben Sie in das Feld **Kennwort** das Kennwort ein, das gespeichert werden soll.
2. Klicken Sie auf **OK**.

Als Alternative zum Profileditor können Sie das Kennwort mit dem Befehl **set password** auch lokal speichern. Zum Beispiel:

```
dsmc SET PASSWORD -type=vm  
vcenter.us.ibm.com Administrator secret
```

Syntax

►—VMCPw— —Kennwortname—◄

Parameter

Kennwortname

Gibt das Kennwort für den VMware VirtualCenter- oder ESX-Server an, der gesichert, zurückgeschrieben oder abgefragt werden soll.

Beispiele

Optionsdatei:

VMCPw SECRET

Befehlszeile:

-VMCPw=SECRET

Zugehörige Verweise:

„Set Password“ auf Seite 820

Vmctlmc

Diese Option gibt die Verwaltungsklasse an, die beim Sichern von Steuerdateien für virtuelle Maschinen verwendet werden soll.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Standardmäßig sind die Steuerdateien für virtuelle Maschinen an die Standardverwaltungsklasse gebunden. Mit der Option **vmmc** kann eine andere Verwaltungsklasse angegeben werden, an die die Daten und Steuerdateien für virtuelle Maschinen gebunden werden. Die Option **vmctlmc** überschreibt die Standardverwaltungsklasse und die Option **vmmc** für die Steuerdateien virtueller Maschinen.

Unter bestimmten Bedingungen könnte es wünschenswert oder erforderlich sein, die Steuerdateien an eine andere Verwaltungsklasse als die Datendateien zu binden.

Die Option **vmctlmc** ist erforderlich, wenn Datendateien virtueller Maschinen auf Band gesichert werden. Steuerdateien für virtuelle Maschinen müssen in einem plattenbasierten Speicherpool gesichert werden, der nicht auf Band umgelagert wird. Der Speicherpool kann aus Datenträgern mit wahlfreiem Zugriff und sequen-

ziellen FILE-Datenträgern bestehen. Der Speicherpool kann außerdem ein deduplizierter Pool sein. Geben Sie mit der Option `vmctlmc` eine Verwaltungsklasse an, durch die Daten in einem solchen Speicherpool gespeichert werden.

Einschränkung: Die durch die Option `vmctlmc` angegebene Verwaltungsklasse gibt nur den Zielspeicherpool für die Steuerdateien virtueller Maschinen an. Die Aufbewahrung der Steuerdateien wird durch die Option `vmmc` festgelegt, falls angegeben, oder durch die Standardverwaltungs-klasse. Die Aufbewahrungsdauer der Steuerdateien von virtuellen Maschinen stimmt immer mit der Aufbewahrungsdauer der Datendateien von virtuellen Maschinen überein.

Unterstützte Clients

Diese Option ist für Clients gültig, die als Knoten der Einheit zum Versetzen von Daten agieren und virtuelle VMware-Maschinen schützen.

Die Option kann nur für Sicherungen virtueller Maschinen mit einem immer inkrementellen Sicherungsmodus verwendet werden.

Diese Option ist nur verfügbar, wenn Sie eine Lizenz für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware oder IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V besitzen.

Optionsdatei

Fügen Sie diese Option in die Systemoptionsdatei (`dsm.sys`) ein.

Syntax

►►—`VMCTLmc—Klassenname`—————►►

Parameter

Klassenname

Gibt eine Verwaltungsklasse an, die für die Sicherung der Steuerdateien für virtuelle Maschinen gilt. Wird diese Option nicht definiert, wird die in der Option `vmmc` angegebene Verwaltungsklasse verwendet. Wird diese Option nicht definiert und ist die Option `vmmc` nicht definiert, wird die Standardverwaltungs-klasse des Knotens verwendet.

Beispiele

Optionsdatei:

`vmctlmc diskonlymc`

Befehlszeile:

Nicht zutreffend.

Vmcuser

Verwenden Sie die Option `vmcuser` im Befehl **backup VM**, **restore VM** oder **query VM**, um den Benutzernamen des VMware VirtualCenter- oder ESX-Servers anzugeben, der gesichert, zurückgeschrieben oder abgefragt werden soll.

Verwenden Sie das VirtualCenter, falls es verfügbar ist. Wenn Sie keinen VirtualCenter-Server verwenden können und Sicherungen mehrerer Systeme auf mehre-

ren ESX-Servern ausführen müssen, geben Sie diese Option nicht an, sondern geben Sie stattdessen die Option mit dem Befehl an, damit sie für jeden ESX-Server variiert werden kann.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Unterstützte Clients

Diese Option ist für Clients gültig, die zur Ausführung einer Off-Host-Sicherung virtueller VMware-Maschinen konfiguriert sind. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt), in die Clientsystemoptionsdatei (dsm.sys) oder in die Befehlszeile ein.

Syntax

►►—VMCUser— —Benutzername—►►

Parameter

Benutzername

Gibt den Benutzernamen des VMware VirtualCenter- oder ESX-Servers an, der gesichert, zurückgeschrieben oder abgefragt werden soll.

Wird mit einem Virtual Center gearbeitet, ist eine Benutzer-ID mit Zugriff auf das Windows-System, auf dem sich das Virtual Center befindet, erforderlich. Diese Benutzer-ID muss entweder über Administratorberechtigungen oder über die Mindestberechtigungen verfügen, die in der Technote 1659544 angegeben sind.

Beispiele

Optionsdatei:

```
VMCUser administrator
```

Befehlszeile:

```
backup vm -VMCUser=domainname\administrator
```

Befehlszeile:

Beispiel für die Herstellung einer Verbindung zu einem ESX-Server:

```
backup vm -VMCUser=root
```

Vmdatastorethreshold

Verwenden Sie die Option `vmdatastorethreshold`, um den Prozentsatz für den Schwellenwert der Speicherbelegung für jeden VMware-Datenspeicher einer virtuellen Maschine zu definieren.

Wenn Sie diese Option angeben, wird die Speicherbelegung überprüft, bevor eine VM-Momentaufnahme erstellt wird. Ist der Schwellenwert überschritten, wird die

virtuelle Maschine nicht gesichert. Wenn diese Option definiert wird, können Fehler aufgrund fehlenden Speicherbereichs bei der Sicherung von virtuellen Maschinen verhindert werden.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Unterstützte Clients

Sie können diese Option für unterstützte Linux x86_64-Clients verwenden.

Optionsdatei

Sie können diese Option in der Clientsystemoptionsdatei (`dsm.sys`) oder mit dem Befehl **backup vm** in der Befehlszeile angeben. Sie können diese Option auf einem IBM Spectrum Protect-Server mit Version 7.1.5 oder höher auch in einer Clientoptionsgruppe angeben. Sie können diese Option nicht im Profileditor definieren.

Syntax

►►—VMDATASTOREThreshold—*Prozent*—————►►

Parameter

Prozent

Gibt den Schwellenwertprozentsatz für jeden VMware-Datenspeicher der virtuellen Maschine an, die gesichert werden soll. Sie können eine ganze Zahl von 0 bis 100 angeben. Der Standardwert ist 100. Wenn Sie diese Option nicht definieren, startet der Client eine Sicherung der virtuellen Maschine, ohne zuvor die vorhandene Speicherbelegung zu überprüfen.

Voraussetzungen:

- Stellen Sie sicher, dass der Schwellenwert nicht zu hoch ist, damit die Momentaufnahme nicht den gesamten verfügbaren Speicherbereich in den VMware-Datenspeichern belegt. Andernfalls ist in den VMware-Datenspeichern kein Speicherbereich mehr verfügbar und die Momentaufnahme wird nicht erstellt.
- Wenn Sie mehrere Clients verwenden, die als Einheiten zum Versetzen von Daten agieren, müssen Sie diese Option der Optionsdatei für jede Einheit zum Versetzen von Daten hinzufügen.
- Der Client überprüft die Datennutzung des VMware-Datenspeichers, der die VM-Plattenmomentaufnahmen enthält. Standardmäßig werden die Momentaufnahmen in dem Verzeichnis erstellt, in dem sich auch die übergeordnete Datei der virtuellen Platte (`.vmdk`) befindet.

Wenn Sie die Momentaufnahmeposition in ein neues Verzeichnis in demselben Datenspeicher oder in einem anderen Datenspeicher mit der Option `workingDir` in der VM-Konfigurationsdatei ändern, müssen Sie sicherstellen, dass der Pfad des Arbeitsverzeichnisses korrekt ist. Ist der Pfad nicht korrekt, kann der Client möglicherweise die Datennutzung des falschen Datenspeichers überprüfen.

Wenn Sie die Option `EXCLUDE.VMDISK` verwenden, um eine oder mehrere Platten von einer Sicherung auszuschließen, wird dennoch die Schwellenwertüber-

prüfung auf diesen Platten ausgeführt. Diese Platten werden zwar nicht gesichert; jedoch erstellt VMware dennoch eine Momentaufnahme dieser Platten.

Unabhängige Platten werden während der Verarbeitung der Speicherbereichsüberprüfung nicht überprüft, da eine Momentaufnahme dieser Platten keinen Speicherbereich in einem VMware-Datenspeicher belegt.

Beispiel 1

Die virtuelle Maschine vm1 erstreckt sich über datastore1 und datastore2. Setzen Sie die Option `vmdatastorethreshold` auf 90, um sicherzustellen, dass beide VMware-Datenspeicher maximal zu 90 % belegt sind, wenn die virtuelle Maschine gesichert wird.

Optionsdatei:

```
vmdatastorethreshold 90
```

Befehlszeile:

```
dsmc backup vm vm1 -vmdatastorethreshold=90
```

Beispiel 2

Der Schwellenwert des Datenspeichers datastore2 wird auf 85 gesetzt. Der Schwellenwert des Datenspeichers wird während der Sicherung der virtuellen Maschine vm5 überschritten. Die folgende Fehlermeldung wird angezeigt:

```
ANS14200E Die virtuelle Maschine 'vm5' konnte nicht gesichert werden, da die  
Datennutzung des Datenspeichers 'datastore2' den Schwellenwert von  
85 Prozent für den Datenspeicher überschritten hat.
```

Erhöhen Sie den Wert der Option `vmdatastorethreshold` auf 95 und starten Sie die Sicherung erneut.

Optionsdatei:

```
vmdatastorethreshold 95
```

Befehlszeile:

```
dsmc backup vm vm5 -vmdatastorethreshold=95
```

Zugehörige Verweise:

„Backup VM“ auf Seite 710

Vmdefaultvportgroup

Mit dieser Option können Sie die Portgruppe angeben, die NICs (Netzschnittstellenkarten) während **restore vm**-Operationen für eine virtuelle Maschine verwenden sollen, die bei ihrer Sicherung mit einer verteilten virtuellen Portgruppe verbunden war, ohne dass der Zielhost der Zurückschreibungsoperation eine ähnliche verteilte virtuelle Portgruppe enthält.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Diese Option ist nicht für Sicherungs- oder Zurückschreibungsoperationen für virtuelle Microsoft-Hyper-V-Maschinen gültig.

Unterstützte Clients

Diese Option ist für Linux-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (`dsm.opt`) oder in die Clientsystemoptionsdatei (`dsm.sys`) ein oder geben Sie sie als Befehlszeilenparameter im Befehl **restore vm** an.

Syntax

►—VMDEFAULTDVPORTGROUP—*Portgruppenname*—►

Parameter

Portgruppenname

Gibt den Namen der Portgruppe an, der verwendet werden soll. Beim Portgruppennamen muss die Groß-/Kleinschreibung beachtet werden.

Beispiele

Optionsdatei:

```
VMDEFAULTDVPORTGROUP dvPortGroup
```

Befehlszeile:

```
dsmc restore vm vm123 -VMDEFAULTDVPORTGROUP=dvPortGroup
```

Zugehörige Verweise:

„Vmdefaultnetwork“ auf Seite 645

„Vmdefaultdvswitch“

Vmdefaultdvswitch

Mit dieser Option können Sie den verteilten virtuellen Switch (dvSwitch) angeben, der die Portgruppe enthält, die Sie mit der Option `vmdefaultdvportgroup` definieren. Die Option bleibt ohne Wirkung, wenn nicht auch die Option `vmdefaultdvportgroup` angegeben wird.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Unterstützte Clients

Diese Option ist für Linux-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (`dsm.opt`) oder in die Clientsystemoptionsdatei (`dsm.sys`) ein oder geben Sie sie als Befehlszeilenparameter im Befehl **restore vm** an.

Syntax

►►—VMDEFAULTDVSWITCH—*dvSwitch*—◄◄

Parameter

dvSwitch

Gibt den Namen des virtuellen Switch an, der verwendet werden soll. Beim Namen des virtuellen Switch muss die Groß-/Kleinschreibung beachtet werden.

Beispiele

Optionsdatei:

```
VMDEFAULTDVSWITCH dvSwitch
```

Befehlszeile:

```
dsmc restore vm vm123 -VMDEFAULTDVSWITCH=dvSwitch -VMDEFAULTDVPORTGROUP=dvPortGroup
```

Zugehörige Verweise:

„Vmdefaultdvportgroup“ auf Seite 643

Vmdefaultnetwork

Mit dieser Option können Sie ein Netz angeben, das NICs (Netzschnittstellenkarten) während einer **restore vm**-Operation für eine virtuelle Maschine verwenden sollen, die bei ihrer Sicherung mit einer verteilten virtuellen Portgruppe verbunden war, ohne dass für den Zielhost der Zurückschreibungsoperation verteilte Switch-Portgruppen konfiguriert sind.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Unterstützte Clients

Diese Option ist für Linux-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (`dsm.opt`) oder in die Clientsystemoptionsdatei (`dsm.sys`) ein oder geben Sie sie als Befehlszeilenparameter im Befehl **restore vm** an.

Syntax

►►—VMDEFAULTNETWORK—*VM-Netzname*—◄◄

Parameter

VM-Netzname

Gibt den Namen des Netzes der virtuellen Maschine an, der verwendet wer-

den soll. Beim Netznamen muss die Groß-/Kleinschreibung beachtet werden. Wenn der Name Leerzeichen enthält, muss er in Anführungszeichen eingeschlossen werden.

Beispiele

Optionsdatei:

```
VMDEFAULTNETWORK "VM Network"
```

Befehlszeile:

```
dsmc restore vm vm123 -VMDEFAULTNETWORK="VM Network"
```

Zugehörige Verweise:

„Vmdefaultdvportgroup“ auf Seite 643

„Vmdefaultdvswitch“ auf Seite 644

Vmenabletemplatebackups

Die Option `vmenabletemplatebackups` gibt an, ob der Client virtuelle VMware-Schablonenmaschinen sichert, wenn er virtuelle Maschinen auf einem vCenter-Server schützt. Virtuelle VMware-Schablonenmaschinen können nicht gesichert werden, wenn sie sich auf einem ESXi-Host befinden, weil ESXi Schablonen nicht unterstützt.

Wenn diese Option aktiviert ist, können Sie VMware-Schablonenmaschinen in vollständige VM-Sicherungsoperationen einschließen. Sie verwenden den vorhandenen Befehl **Backup VM** und die Option `DOMAIN.VMFULL`, um die virtuellen Maschinen anzugeben, die bei der Sicherungsoperation berücksichtigt werden sollen.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Teilsicherungen werden nicht unterstützt und Momentaufnahmen nicht erstellt; daher müssen Sie `MODE=IFFULL` verwenden. Mit `MODE=IFFULL` können Sie selbst dann eine neue Sicherung virtueller VMware-Schablonenmaschinen erzwingen, wenn diese sich seit der letzten Sicherung nicht geändert haben.

Wenn `vmenabletemplatebackups` aktiviert ist, wird jeder Sicherungsprozess, der mit `MODE=IFINCREMENTAL` eingeleitet wird, unter Verwendung von `MODE=IFFULL` verarbeitet. Virtuelle VMware-Schablonenmaschinen werden bei einer Sicherung nur berücksichtigt, wenn sie seit der letzten Sicherung geändert wurden.

Wenn diese Option aktiviert ist, müssen Sie sicherstellen, dass `vmvstortransport`-Optionen den Wert `NBDSSL` oder `NBD` enthalten. Wird nur der Transportmodus `SAN` oder `HOTADD` in Verbindung mit dieser aktivierten Option verwendet, schlagen Sicherungen der Schablonenmaschinen fehl.

Unterstützte Clients

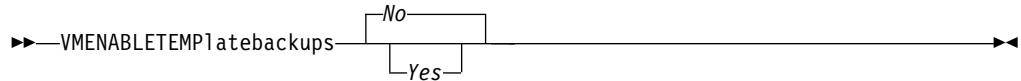
Diese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Optionsdatei

Sie können diese Option in der Befehlszeile, in der Clientsystemoptionsdatei (dsm.sys), in der Clientoptionsdatei (dsm.opt) oder auf dem Server in einer Clientoptionsgruppe definieren.

Sie können die Option auch im Profileditor auf der Registerkarte 'VM-Sicherung' definieren (wählen Sie die Option für die Sicherung von Schablonen virtueller Maschinen aus).

Syntax



Parameter

No Gibt an, dass virtuelle Schablonenmaschinen in vollständigen VM-Sicherungsoperationen nicht eingeschlossen werden. Dies ist die Standardeinstellung.

Yes

Gibt an, dass virtuelle Schablonenmaschinen in vollständigen VM-Sicherungsoperationen eingeschlossen werden.

Beispiele

Optionsdatei

```
vmenabletemplatebackups yes
```

Befehlszeile:

Eine virtuelle VMware-Schablonenmaschine sichern:

```
dsmc backup vm VM-Name -VMENABLETEMPLATEBACKUPS=YES
```

VM-Name ist der Name der Schablonenmaschine.

Befehlszeile:

Eine virtuelle VMware-Schablonenmaschine an dieselbe Position und mit demselben Namen zurückschreiben:

```
dsmc restore vm VM-Name -VMENABLETEMPLATEBACKUPS=YES
```

VM-Name ist der Name der Schablonenmaschine.

Befehlszeile:

Eine virtuelle Schablonenmaschine an eine neue Position zurückschreiben:

```
dsmc restore vm VM-Name -vmname=win7x64  
-datastore=datastore22 -host=supersht.labx.com  
-datacenter="Lab Center" -VMENABLETEMPLATEBACKUPS=YES
```

VM-Name ist der Name der Schablonenmaschine. „win7x64“ ist der neue Name der virtuellen Schablonenmaschine. Das neue Datacenter, der neue Host und der neue Datenspeicher sind ebenfalls enthalten.

Zugehörige Verweise:

„Backup VM“ auf Seite 710

„Restore VM“ auf Seite 791

„Domain.vmfull“ auf Seite 414

Vmlimitperdatastore

Die Option `vmlimitperdatastore` gibt die Anzahl virtueller Maschinen (VMs) und virtueller Platten in einem Datenspeicher an, die während einer optimierten Sicherungsoperation parallel verarbeitet werden können.

Bei einer optimierten Sicherungsoperation sind parallele Sicherungen auf der VM-Ebene, auf der Ebene der virtuellen Platte oder auf der Unterplattenebene aktiviert.

Die Option `vmlimitperdatastore` wird zusammen mit den Optionen `vmmaxparallel`, `vmmaxbackupsessions` und `vmlimitperhost` verwendet, um Sicherungsoperationen zu optimieren und das Ressourcenvolumen zu steuern, das durch die Sicherung auf einem Host in der vSphere-Infrastruktur erstellt werden kann. Passen Sie die Werte dieser Optionen an, um die Werte zu ermitteln, mit denen eine optimale Leistung für die Sicherungen in Ihrer Umgebung erzielt wird.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

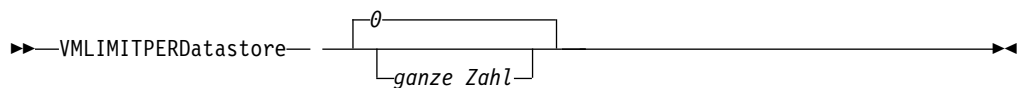
Unterstützte Clients

Diese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Optionsdatei

Diese Option ist in der Clientsystemoptionsdatei (`dsm.sys`), in der Clientoptionsdatei (`dsm.opt`) und in der Befehlszeile für **Backup VM** gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profilditor definiert werden.

Syntax



Parameter

ganze_Zahl

Gibt die maximale Anzahl VMs in einem beliebigen Datenspeicher an, die in eine optimierte Sicherungsoperation eingeschlossen werden. Sie können maximal 50 virtuelle Maschinen angeben. Der Standardwert ist 0 (null).

Die Angabe 0 bedeutet, dass die Anzahl der virtuellen Maschinen, die parallel aus einem Datenspeicher gesichert werden können, keine Rolle spielt. Stattdessen soll die maximale Anzahl virtueller Maschinen, die in eine Sicherung eingeschlossen werden sollen, mit dem für die Option `vmmaxparallel` angegebenen Wert begrenzt werden. Die Option `vmlimitperdatastore` wird auch dann umgesetzt, wenn VM-Daten in zwei oder mehr Datenspeichern vorhanden sind.

Beispiele

Optionsdatei

```
VMLIMITPERD 5
```

Befehlszeile:

```
dsmc backup vm -VMLIMITPERD=5
```

Zugehörige Verweise:

„Backup VM“ auf Seite 710

„Domain.vmfull“ auf Seite 414

„Vmmaxbackupsessions“ auf Seite 650

„Vmmaxparallel“ auf Seite 652

„Vmlimitperhost“

Zugehörige Informationen:

➡ Mehrere virtuelle Maschinen parallel sichern

Vmlimitperhost

Die Option `vmlimitperhost` gibt die Anzahl virtueller Maschinen (VMs) und virtueller Platten in einem Host an, die während einer optimierten Sicherungsoperation parallel verarbeitet werden können.

Bei einer optimierten Sicherungsoperation sind parallele Sicherungen auf der VM-Ebene, auf der Ebene der virtuellen Platte oder auf der Unterplattenebene aktiviert.

Die Option `vmlimitperhost` wird zusammen mit den Optionen `vmmaxparallel`, `vmmaxbackupsessions` und `vmlimitperdatastore` verwendet, um Sicherungsoperationen zu optimieren und das Ressourcenvolumen zu steuern, das durch die Sicherung auf einem Host in der vSphere-Infrastruktur erstellt werden kann. Passen Sie die Werte dieser Optionen an, um die Werte zu ermitteln, mit denen eine optimale Leistung für die Sicherungen in Ihrer Umgebung erzielt wird.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

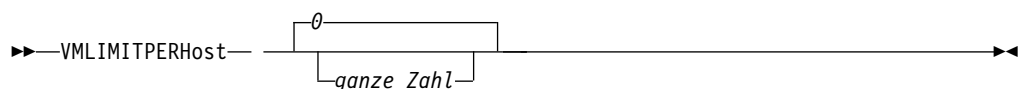
Unterstützte Clients

Diese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Optionsdatei

Diese Option ist in der Clientsystemoptionsdatei (`dsm.sys`), in der Clientoptionsdatei (`dsm.opt`) und in der Befehlszeile für **Backup VM** gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profilditor definiert werden.

Syntax



Parameter

ganze_Zahl

Gibt die maximale Anzahl VMs auf einem beliebigen ESX-Server an, die in

eine optimierte Sicherungsoperation eingeschlossen werden können. Sie können maximal 50 virtuelle Maschinen angeben. Der Standardwert ist 0 (null).

Die Angabe 0 bedeutet, dass die Anzahl der virtuellen Maschinen, die parallel auf einem ESX-Server gesichert werden können, keine Rolle spielt. Stattdessen soll die maximale Anzahl virtueller Maschinen, die in eine Sicherung eingeschlossen werden sollen, mit dem für die Option `vmmaxparallel` angegebenen Wert begrenzt werden.

Beispiele

Optionsdatei

`VMLIMITPERH 5`

Befehlszeile:

`dsmc backup vm -VMLIMITPERH=5`

Zugehörige Verweise:

„**Backup VM**“ auf Seite 710

„`Domain.vmfull`“ auf Seite 414

„`Vmmaxparallel`“ auf Seite 652

„`Vmlimitperhost`“ auf Seite 649

Zugehörige Informationen:

 Mehrere virtuelle Maschinen parallel sichern

Vmmaxbackupsessions

Die Option `vmmaxbackupsessions` gibt die maximale Anzahl IBM Spectrum Protect-Serversitzungen zum Versetzen von VM-Daten auf den Server an, die in eine optimierte Sicherungsoperation eingeschlossen werden können.

Bei einer optimierten Sicherungsoperation sind parallele Sicherungen auf der VM-Ebene, auf der Ebene der virtuellen Platte oder auf der Unterplattenebene aktiviert.

Die Option `vmmaxbackupsessions` wird zusammen mit den Optionen `vmmaxparallel`, `vmlimitperdatastore` und `vmlimitperhost` verwendet, um Sicherungsoperationen zu optimieren und das Ressourcenvolumen zu steuern, das durch die Sicherung auf einem Host in der vSphere-Infrastruktur erstellt werden kann. Passen Sie die Werte dieser Optionen an, um die Werte zu ermitteln, mit denen eine optimale Leistung für die Sicherungen in Ihrer Umgebung erzielt wird.

Unterstützte Clients



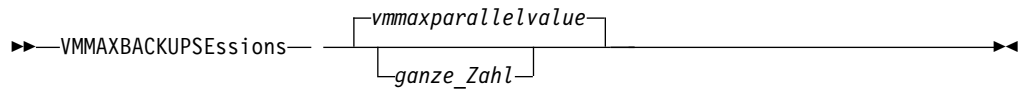
Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Diese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Optionsdatei

Diese Option ist in der Clientsystemoptionsdatei (`dsm.sys`), in der Clientoptionsdatei (`dsm.opt`) und in der Befehlszeile für **Backup VM** gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profilditor definiert werden.

Syntax



Parameter

ganze_Zahl

Gibt die maximale Anzahl IBM Spectrum Protect-Serversitzungen an, die während der Sicherungsoperation erstellt werden können.

Lesen Sie die folgenden Informationen zur Verwendung der Option `vmxbackupsessions` zusammen mit der Option `vmxparallel` oder dem Serverparameter `maxnummp`:

vmxparallel

Die Option `vmxparallel` gibt die maximale Anzahl virtueller Maschinen an, die gleichzeitig auf dem IBM Spectrum Protect-Server gesichert werden können. Der Wert für die Option `vmxbackupsessions` muss größer-gleich dem Wert für die Option `vmxparallel` sein.

Wenn der Wert kleiner als der Wert für die Option `vmxparallel` ist, wird die folgende Nachricht zurückgegeben und der Wert in denselben Wert wie für die Option `vmxparallel` geändert:

ANS9995W Der Wert der Option VMXBACKUPSESSIONS ist 'Zahlenwert'. Dieser Wert muss größer-gleich dem Wert der Option VMXPARALLEL sein, der 'Zahlenwert' lautet. Der Wert wird auf den Wert der Option VMXPARALLEL gesetzt.

maxnummp

Der Serverparameter `maxnummp` gibt die maximale Anzahl Mountpunkte an, die ein Knoten auf dem Server verwenden darf, wenn das Kopienziel des Speicherpools FILE oder TAPE lautet. Der Parameter `maxnummp` muss größer-gleich der Einstellung für die Optionen `vmxparallel` und `vmxbackupsessions` sein. Wenn mehrere Instanzen des Clients Dateien sichern oder wenn ein einziger Client parallele Sicherungen ausführt, sind unter Umständen mehr Mountpunkte erforderlich.

Wenn der Wert für `vmxparallel` oder `vmxbackupsessions` den Wert für `maxnummp` überschreitet, werden Nachricht ANS0266I und andere Nachrichten angezeigt. Abhängig von der Nachricht verringert der Client den Wert für die Option `vmxparallel` auf die Anzahl, die durch den Parameter `maxnummp` angegeben ist, oder verhindert das Öffnen weiterer Sitzungen für die angegebene VM. In jeder dieser Situationen wird die Sicherungsoperation fortgesetzt.

Werden weitere Fehler ANS0266I gefunden, verringert der Client den Wert für `vmxparallel` um 1 und versucht, die Sicherung fortzusetzen. Wenn der Wert für `vmxparallel` auf 1 verringert wird und der Client weitere Fehler ANS0266I empfängt, beendet der Client die Sicherung und gibt den folgenden Fehler aus:

ANS5228E Eine VM-Sicherungsoperation ist fehlgeschlagen, weil VMXPARALLEL auf 1 reduziert wurde und der Client noch immer keinen Servermountpunkt abrufen kann.

Wenden Sie sich an Ihren Serveradministrator, wenn der aktuelle Wert für `maxnummp` erhöht werden soll, damit Ihr Knoten weitere parallele Sicherungssitzungen unterstützen kann.

Sie können maximal 100 Sitzungen angeben. Der Standardwert ist der für die Option `vmmaxparallel` festgelegte Wert.

Beispiele

Optionsdatei

`VMMAXBACKUPS 10`

Befehlszeile:

`dsmc backup vm -VMMAXBACKUPS=10`

Zugehörige Verweise:

„Backup VM“ auf Seite 710

„Domain.vmfull“ auf Seite 414

„Vmmaxparallel“

„Vmlimitperdatastore“ auf Seite 648

„Vmlimitperhost“ auf Seite 649

Zugehörige Informationen:

 Mehrere virtuelle Maschinen parallel sichern

Vmmaxparallel

Die Option `vmmaxparallel` dient zum Konfigurieren optimierter Sicherungen mehrerer virtueller Maschinen mithilfe einer einzigen Instanz des Clients für Sichern/Archivieren. Diese Option gibt die maximale Anzahl virtueller Maschinen an, die gleichzeitig auf dem IBM Spectrum Protect-Server gesichert werden können.

Bei einer optimierten Sicherungsoperation sind parallele Sicherungen auf der VM-Ebene, auf der Ebene der virtuellen Platte oder auf der Unterplattenebene aktiviert.

Die Option `vmmaxparallel` wird zusammen mit den Optionen `vmmaxbackupsessions`, `vmlimitperhost` und `vmlimitperdatastore` verwendet, um Sicherungsoperationen zu optimieren und das Ressourcenvolumen zu steuern, das durch die Sicherung auf einem Host in der vSphere-Infrastruktur erstellt werden kann. Passen Sie die Werte dieser Optionen an, um die Werte zu ermitteln, mit denen eine optimale Leistung für die Sicherungen in Ihrer Umgebung erzielt wird.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

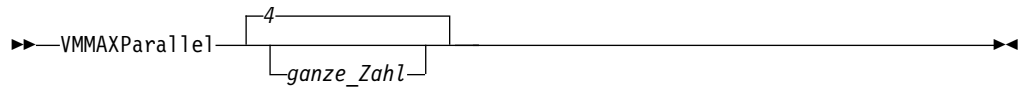
Unterstützte Clients

Diese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Optionsdatei

Diese Option ist in der Clientsystemoptionsdatei (`dsm.sys`) und in der Befehlszeile für den Befehl **Backup VM** gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profileditor definiert werden.

Syntax



Parameter

ganze Zahl

Gibt die maximale Anzahl virtueller Maschinen an, die während einer optimierten Sicherungsoperation gleichzeitig gesichert werden können. Der Standardwert ist 4. Der Maximalwert ist 50.

Tipp: Wenn Sie die clientseitige Datenduplizierung verwenden, wird eine Datenduplizierungssitzung für jede VM gestartet. Diese Datenduplizierungssitzungen werden bei `vmaxparallel` nicht mitgezählt. Lesen Sie die folgenden Informationen zur Verwendung der Option `vmaxparallel` zusammen mit der Option `vmaxbackupsessions` oder dem Serverparameter `maxnummp`:

vmaxbackupsessions

Die Option `vmaxbackupsessions` gibt die maximale Anzahl Sitzungen zum Versetzen von Daten virtueller Maschinen auf den Server an, die in eine optimierte Sicherungsoperation eingeschlossen werden können. Der Wert für die Option `vmaxbackupsessions` muss größer-gleich dem Wert für die Option `vmaxparallel` sein.

maxnummp

Der Serverparameter `maxnummp` gibt die maximale Anzahl Mountpunkte an, die ein Knoten auf dem Server verwenden darf, wenn das Kopienziel des Speicherpools `FILE` oder `TAPE` lautet. Der Parameter `maxnummp` muss größer-gleich der Einstellung für die Optionen `vmaxparallel` und `vmaxbackupsessions` sein. Wenn mehrere Instanzen des Clients Dateien sichern oder wenn ein einziger Client parallele Sicherungen ausführt, sind unter Umständen mehr Mountpunkte erforderlich.

Wenn der Wert für `vmaxparallel` oder `vmaxbackupsessions` den Wert für `maxnummp` überschreitet, werden Nachricht `ANS0266I` und andere Nachrichten angezeigt. Abhängig von der Nachricht verringert der Client den Wert für die Option `vmaxparallel` auf die Anzahl, die durch den Parameter `maxnummp` angegeben ist, oder verhindert das Öffnen weiterer Sitzungen für die angegebene VM. In jeder dieser Situationen wird die Sicherungsoperation fortgesetzt.

Werden weitere Fehler `ANS0266I` gefunden, verringert der Client den Wert für `vmaxparallel` um 1 und versucht, die Sicherung fortzusetzen. Wenn der Wert für `vmaxparallel` auf 1 verringert wird und der Client weitere Fehler `ANS0266I` empfängt, beendet der Client die Sicherung und gibt den folgenden Fehler aus:

`ANS5228E` Eine VM-Sicherungsoperation ist fehlgeschlagen, weil `VMAXPARALLEL` auf 1 reduziert wurde und der Client noch immer keinen Servermountpunkt abrufen kann.

Wenden Sie sich an Ihren Serveradministrator, wenn der aktuelle Wert für `maxnummp` erhöht werden soll, damit Ihr Knoten weitere parallele Sicherungssitzungen unterstützen kann.

Beispiele

Optionsdatei

VMMAXP 10

Zugehörige Verweise:

„Backup VM“ auf Seite 710

„Domain.vmfull“ auf Seite 414

„Vmlimitperhost“ auf Seite 649

„Vmlimitperdatastore“ auf Seite 648

Zugehörige Informationen:

➡ Mehrere virtuelle Maschinen parallel sichern

Vmmaxrestoresessions

Die Option `vmmaxrestoresessions` definiert die Gesamtzahl der Sitzungen, die für die optimierte Zurückschreibungsoperation des IBM Spectrum Protect-Servers zugeordnet werden.

Bei einer optimierten Zurückschreibungsoperation sind parallele Zurückschreibungen auf der Unterplattenebene einer virtuellen Platte aktiviert.

Anmerkung: Mindestens eine Sitzung muss für jede zurückzuschreibende Platte zugeordnet werden.

Anmerkung: Ist der Wert von `vmmaxrestoresessions` kleiner als das Produkt aus dem Wert von `vmmaxstoreparalleldisks` und dem Wert von `vmmaxstoreparallelvms`, wird der Wert während der Ausführungszeit automatisch auf das Produkt aus dem Wert von `vmmaxstoreparalleldisks` und dem Wert von `vmmaxstoreparallelvms` angepasst.

Unterstützte Clients

Diese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

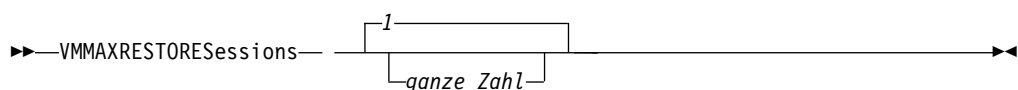


Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Optionsdatei

Diese Option ist in der Clientsystemoptionsdatei (`dsm.sys`), in der Clientoptionsdatei (`dsm.opt`) und in der Befehlszeile für **Restore VM** gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profilditor definiert werden.

Syntax



Parameter

ganze_Zahl

Gibt die Anzahl IBM Spectrum Protect-Serversitzungen an, die während der Zurückschreibungsoperation erstellt werden. Der Standardwert ist 1. Der maximale Wert ist 100.

Beispiele

Optionsdatei

VMMAXRESTORES 5

Befehlszeile:

dsmc restore vm webserver1 -VMMAXRESTORES=5

Anmerkung: Dieses Befehlszeilenbeispiel für diese Option ist sowohl in unterstützten Windows-Clients als auch in unterstützten Linux-Clients gültig.

Zugehörige Verweise:

„Restore VM“ auf Seite 791

Vmmaxrestoreparalleldisks

Die Option `vmmaxrestoreparalleldisks` ermöglicht einem IBM Spectrum Protect-Client die gleichzeitige Zurückschreibung mehrerer spezieller virtueller Platten pro virtueller Maschine.

Sie können die Anzahl zu öffnender Plattensitzungen bis zu einem Maximalwert von 10 Sitzungen angeben. Sitzungen werden pro Platte auf der Basis des Transporttyps aus der Option `vmvstortransport` zugeordnet. Die Zuordnung verfügbarer Sitzungen erfolgt gemäß der mit `vmmaxrestoreparalleldisks` angegebenen Anzahl Plattensitzungen; dabei wird die Anzahl Sitzungen pro Platte auf die nächste ganze Zahl abgerundet.

Unterstützte Clients

Diese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Anmerkung:

Sie müssen sicherstellen, dass die Gesamtzahl der Zurückschreibungsoperationen aus allen Quellen auf denselben ESXi-Host nicht größer als 26 ist. Aufgrund eines Problems beim ESXi-Host kann die Operation fehlschlagen, wenn diese Anzahl der parallelen Zurückschreibungen überschritten wird. Wenn beispielsweise 3 verschiedene Zurückschreibungsinstanzen auf denselben ESXi-Host vorhanden sind und für jede dieser Instanzen `VMMAXRESTOREPARALLELDISKS 10` angegeben wurde, können die Zurückschreibungen fehlschlagen, weil die Gesamtzahl der Verbindungen 30 beträgt.

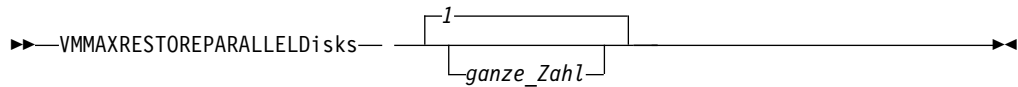


Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Optionsdatei

Diese Option ist in der Clientsystemoptionsdatei (`dsm.sys`) und in der Befehlszeile für **Restore VM** gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profileditor definiert werden.

Syntax



Parameter

ganze_Zahl

Gibt die Anzahl virtueller Festplatten an, die gleichzeitig zurückgeschrieben werden können. Der Standardwert ist 1. Der Maximalwert ist 10.

Beispiele

Task Maximal 2 simultane Zurückschreibungsoperationen für virtuelle Platten in der Zurückschreibungsoperation der virtuellen Maschine **vm1** festlegen:

```
dsmc restore vm vm1 -vmmaxrestoreparalleldisks=2 -vmmaxrestoresessions=8
```

Damit werden 4 simultane Zurückschreibungssitzungen pro virtuelle Platte zugeordnet.

Zugehörige Verweise:

„Restore VM“ auf Seite 791

Vmmaxrestoreparallelvms

Mit der Option `vmmaxrestoreparallelvms` wird die Anzahl der virtuellen Maschinen gesteuert, die ein IBM Spectrum Protect-Client gleichzeitig zurückschreiben kann.

Verwenden Sie diese Option, um die Zurückschreibungsleistung durch eine Erhöhung der Anzahl gleichzeitig zurückzuschreibender virtueller Maschinen zu verbessern.

Sie können die Anzahl der gleichzeitig zurückzuschreibenden virtuellen Maschinen bis zu einem Maximalwert von 10 angeben. Der Standardwert ist 1.

Unterstützte Clients

Diese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

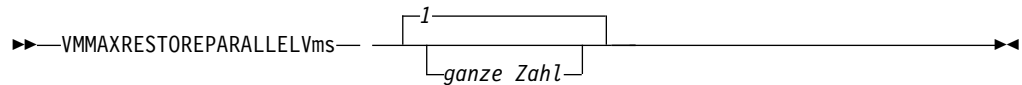


Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Optionsdatei

Diese Option ist in der Clientsystemoptionsdatei (`dsm.sys`) und in der Befehlszeile für **Restore VM** gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profileditor definiert werden.

Syntax



Parameter

ganze Zahl

Gibt die maximale Anzahl virtueller Maschinen an, die gleichzeitig zurückschrieben werden können. Der Standardwert ist 1. Der maximale Wert ist 10.

Anmerkung: Wenn Sie die Option `Vmmaxrestoresessions` zur Begrenzung der Anzahl Zurückschreibungssitzungen verwenden, darf die Anzahl Sitzungen die Anzahl virtueller Maschinen nicht unterschreiten. Dadurch ist gewährleistet, dass mindestens eine Sitzung pro virtuelle Maschine verfügbar ist.

Anmerkung: Wenn Sie die Option `Vmmaxparalleldisks` zum gleichzeitigen Zurückschreiben mehrerer virtueller Platte verwenden, darf die Anzahl virtueller Platten die Anzahl Sitzungen nicht überschreiten.

Beispiele

Task

Maximal 5 gleichzeitige Zurückschreibungen virtueller Maschinen für die Maschinen **vm1, vm2, vm3, vm4 und vm5** festlegen:

```
dsmc restore vm1,vm2,vm3,vm4,vm5 -VMMAXRESTOREPARALLELVms=5  
VMMAXRESTORESessions=10 -VMMAXRESTOREPARALLELDisks=2
```

Hierdurch werden 5 gleichzeitige Zurückschreibungen virtueller Maschinen, die jeweils bis zu 2 virtuelle Platten in Parallelverarbeitung pro virtuelle Maschine zurückschreiben können, und 2 Sitzungen pro virtuelle Maschine zugeordnet.

Task Maximal 2 gleichzeitige Zurückschreibungen virtueller Maschinen für die Maschinen **vm1 und vm2** festlegen:

```
dsmc restore vm1,vm2 -VMMAXRESTOREPARALLELVms=2  
VMMAXRESTORESessions=10 -VMMAXRESTOREPARALLELDisks=1
```

Hierdurch werden 2 gleichzeitige Zurückschreibungen virtueller Maschinen mit jeweils mindestens einer Platte pro virtuelle Maschine und 5 Sitzungen pro virtuelle Maschine zugeordnet.

Task Maximal 2 gleichzeitige Zurückschreibungen virtueller Maschinen für die Maschinen **vm1, vm2, vm3 und vm4** festlegen:

```
dsmc restore vm1,vm2,vm3,vm4 -VMMAXRESTOREPARALLELVms=2  
VMMAXRESTORESessions=16 -VMMAXRESTOREPARALLELDisks=2
```

Hierdurch werden 2 gleichzeitige Zurückschreibungen virtueller Maschinen mit jeweils 2 Platten pro virtuelle Maschine und 8 Sitzungen pro virtuelle Maschine zugeordnet.

Zugehörige Verweise:

„Restore VM“ auf Seite 791

„Vmmaxrestoresessions“ auf Seite 654

„Vmmaxrestoreparalleldisks“ auf Seite 655

Vmmaxvirtualdisks

Die Option `vmmaxvirtualdisks` gibt die maximale Größe von Platten virtueller VMware-Maschinen (VMDK) an, die bei einer Sicherungsoperation eingeschlossen werden sollen. Die Option `vmmaxvirtualdisks` gibt die maximale Größe von Platten virtueller Maschinen an, die bei einer Sicherungsoperation eingeschlossen werden sollen.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Verwenden Sie die Option `vmmaxvirtualdisks` mit der Option `mskipmaxvirtualdisks`, um anzugeben, wie die Einheit zum Versetzen von Daten während einer Sicherungsoperation große Platten virtueller Maschinen (VM-Platten) verarbeitet:

- Definieren Sie die Option `vmmaxvirtualdisks`, um die maximale Größe von VM-Platten anzugeben, die eingeschlossen werden sollen.
- Definieren Sie die Option `mskipmaxvirtualdisks`, um anzugeben, dass die VM-Platten, die die maximale Größe nicht überschreiten, gesichert (und die übrigen VM-Platten ausgeschlossen) werden sollen oder dass die Operation fehlschlagen soll.

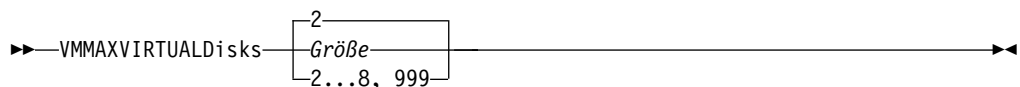
Unterstützte Clients

Diese Option ist für 64-Bit-Linux-Clients gültig, die als Einheiten zum Versetzen von Daten für das Sichern virtueller VMware-Maschinen konfiguriert sind.

Optionsdatei

Definieren Sie die Option `vmmaxvirtualdisks` in der Clientsystemoptionsdatei (`dsm.sys`). Sie können diese Option auch als Befehlszeilenparameter im Befehl **backup vm** angeben.

Syntax



Parameter

Größe

Gibt die maximale Größe der VM-Platten in Terabyte (TB) an, die in eine Sicherungsoperation eingeschlossen werden sollen. Der Bereich ist eine ganze Zahl von 2 bis 8; der Standardwert ist 2. Der Maximalwert ist 8 TB (äquivalent zu 8192 GB).

Geben Sie 999 an, um sicherzustellen, dass die Größe der VM-Platten, die bei Sicherungsoperationen eingeschlossen sind, immer die maximale Größe ist. Dieser Wert ist die einfachste Methode, um sicherzustellen, dass immer der Maximalwert definiert ist. Mit diesem Wert entfällt die kontinuierliche Änderung der Optionsdatei.

Wenn Sie außerdem die Option `mskipmaxvirtualdisks yes` angeben, werden VM-Platten, die der angegebenen maximalen Größe entsprechen oder kleiner sind, gesichert, während VM-Platten, die größer als die angegebene maximale Größe sind, ausgeschlossen werden.

Wenn Sie außerdem die Option `vmskipmaxvirtualdisks no` angeben, schlagen Sicherungsoperationen fehl, wenn die Größe einer VM-Platte die angegebene maximale Größe überschreitet.

Beispiele

Optionsdatei:

```
vmmxvirtualdisks 3
```

Befehlszeile:

VM-Platten sichern, die maximal 5 TB groß sind, und VM-Platten abschließen, die größer als 5 TB sind:

```
backup vm VM1 -vmmxvirtualdisks=5 -vmskipmaxvirtualdisks=yes
```

VM-Platten sichern, die maximal 3 TB groß sind, und die Sicherung fehlschlagen lassen, wenn eine VM-Platte größer als 3 TB ist:

```
backup vm VM1 -vmmxvirtualdisks=3 -vmskipmaxvirtualdisks=no
```

VM-Platten sichern, die maximal 8 TB groß sind, und VM-Platten abschließen, die größer als 8 TB sind:

```
backup vm VM1 -vmmxvirtualdisks=8 -vmskipmaxvirtualdisks=yes
```

Oder:

```
backup vm VM1 -vmmxvirtualdisks=999 -vmskipmaxvirtualdisks=yes
```

Vmmc

Verwenden Sie die Option `vmmc`, um die Sicherungen virtueller Maschinen mit einer anderen Verwaltungsklasse als der Standardverwaltungsklasse zu speichern. Für Sicherungen virtueller VMware-Maschinen ist die Option `vmmc` nur gültig, wenn die Option `vmbackuptype=fullvm` festgelegt ist.

Unterstützte Clients



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Diese Option ist für Clients gültig, die für die Sicherung virtueller VMware-Maschinen konfiguriert sind. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei `dsm.opt`, in die Clientssystemoptionsdatei `dsm.sys` oder in die Befehlszeile ein.

Syntax

►—VMMC—*Name der Verwaltungsklasse*—►

Parameter

Name der Verwaltungsklasse

Gibt eine Verwaltungsklasse an, die für die Sicherung von Daten virtueller Maschinen angewendet wird. Wird diese Option nicht definiert, wird die Standardverwaltungsklasse des Knotens verwendet.

Beispiele

Task: Eine Sicherung der virtuellen Maschine mit dem Namen `myVirtualMachine` ausführen und die Sicherung gemäß der Verwaltungsklasse mit dem Namen `myManagementClass` speichern.

```
dsmc backup vm "myVirtualMachine" -vmc=myManagementClass
```

Vmnoprmdisks

Diese Option ermöglicht dem Client die Zurückschreibung von Konfigurationsdaten für die pRDM-Datenträger, die einer virtuellen VMware-Maschine zugeordnet sind, auch wenn die LUNs, die den Datenträgern zugeordnet wurden, nicht gefunden werden. Da pRDM-Datenträger in einer VM-Momentaufnahme nicht enthalten sind, können nur die Konfigurationsdaten und nicht die Daten zurückgeschrieben werden, die sich auf den Datenträgern befanden.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Diese Option ist für Sicherungen von virtuellen Microsoft-Hyper-V-Maschinen nicht gültig.

Unterstützte Clients

Diese Option ist für Windows- und Linux-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (`dsm.opt`) oder in die Clientsystemoptionsdatei (`dsm.sys`) ein oder geben Sie sie als Befehlszeilenparameter im Befehl **restore vm** an.

Syntax



Parameter

YES

Geben Sie diesen Wert an, wenn Sie eine virtuelle Maschine zurückschreiben müssen, die mit der Angabe `-vmprocesswithprdm=yes` gesichert wurde, und die ursprünglichen LUNs, die durch die RDM-Datei zugeordnet wurden, nicht lokalisiert werden können. Diese Einstellung hat zur Folge, dass der Client Versuche, die fehlenden, von den pRDM-Datenträgern verwendeten LUNs zu finden, überspringt und die ihnen zugeordneten Konfigurationsinformationen (Plattenkennsätze) zurückschreibt. Die pRDM-Datenträger werden als mit Thin-Provisioning definierte VMFS VMDKs zurückgeschrieben. Anschließend können Sie mit dem vSphere-Client die erforderlichen pRDM-Zuordnungen erstellen.

NO Bei Angabe von `-vmnoprmdisk=no` schlagen Zurückschreibungsoperationen für virtuelle Maschinen, die mit `-processvmwithprdm=yes` gesichert wurden, fehl,

wenn die ursprünglichen LUNs, die durch die RDM-Datei zugeordnet wurden, nicht lokalisiert werden können. Dies ist der Standardwert.

Beispiele

Optionsdatei:

```
VMNOPRDMDISKS YES
```

Befehlszeile:

```
dsmc restore vm vm123 -vmnoprmdisks=yes
```

Vmnovrmdisks

Diese Option ermöglicht dem Client die Zurückschreibung von Konfigurationsdaten und Daten für die vRDM-Datenträger, die einer virtuellen VMware-Maschine zugeordnet sind, auch wenn die LUNs, die den Datenträgern zugeordnet wurden, nicht gefunden werden.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Diese Option ist für Sicherungen von virtuellen Microsoft-Hyper-V-Maschinen nicht gültig.

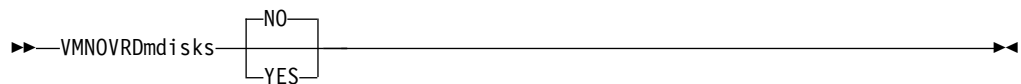
Unterstützte Clients

Diese Option ist für Windows- und Linux-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (`dsm.opt`) oder in die Clientsystemoptionsdatei (`dsm.sys`) ein oder geben Sie sie als Befehlszeilenparameter im Befehl **restore vm** an.

Syntax



Parameter

YES

Geben Sie diesen Wert an, wenn Sie eine virtuelle Maschine zurückschreiben müssen, die gesichert wurde, und die ursprünglichen LUNs, die durch die RDM-Datei zugeordnet wurden, nicht lokalisiert werden können. Diese Einstellung hat zur Folge, dass der Client Versuche, die fehlenden, von den vRDM-Datenträgern verwendeten LUNs zu finden, überspringt und die Konfigurationsinformationen (Plattenkennsätze) sowie die gesicherten Daten zurückschreibt. Die vRDM-Datenträger werden als mit Thin-Provisioning definierte VMFS VMDKs zurückgeschrieben.

NO Bei Angabe von `-vmnovrmdisk=no` schlagen Zurückschreibungsoperationen für

virtuelle Maschinen mit vRDM-Datenträgern fehlt, wenn die ursprünglichen LUNs, die durch die RDM-Datei zugeordnet wurden, nicht lokalisiert werden können. Dies ist der Standardwert.

Beispiele

Optionsdatei:

```
VMNOVRMDISKS YES
```

Befehlszeile:

```
dsmc restore vm vm123 -vmnovrmdisks=yes
```

Vmpreferdagpassive

Die Option `vmpreferdagpassive` gibt an, ob eine aktive Kopie oder eine passive Kopie einer Datenbank gesichert werden soll, die zu einer Microsoft Exchange Server-Datenbankverfügbarkeitsgruppe (DAG) gehört.

Diese Option gilt für Microsoft Exchange Server-Workloads, die in virtuellen Gastmaschinen ausgeführt werden, die durch IBM Spectrum Protect for Virtual Environments geschützt werden.

Verwenden Sie die Option `vmpreferdagpassive` mit dem Befehl **backup vm**.

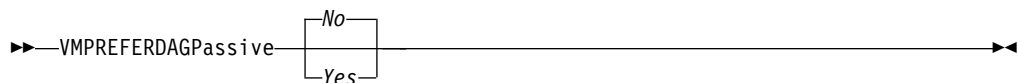
Unterstützte Clients

Diese Option ist auf Clients gültig, die als Einheit zum Versetzen von Daten für VMware-Gastmaschinensicherungen agieren.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (`dsm.sys`) innerhalb einer Serverzeilengruppe ein.

Syntax



Parameter

No Die Microsoft Exchange Server-Datenbank, unabhängig davon, ob es sich um eine aktive oder passive Kopie handelt, in einer Datenbankverfügbarkeitsgruppe (DAG) sichern. Dies ist der Standardwert.

Yes

Die Sicherung einer aktiven Datenbankkopie in einer Datenbankverfügbarkeitsgruppe (DAG) überspringen, wenn eine gültige passive Kopie auf einem anderen Server verfügbar ist. Ist keine gültige passive Kopie verfügbar, wird die aktive Datenbankkopie gesichert.

Beispiele

Optionsdatei:

```
vmpreferdagpassive yes
```

Vmprocessvmwithindependent

Verwenden Sie diese Option, um anzugeben, ob VMware-VMs (VM - virtuelle Maschine), die mit mindestens einer unabhängigen Platte bereitgestellt werden, gesichert werden. Standardmäßig werden VMs mit unabhängigen Platten nicht gesichert.

Unabhängige Platten können nicht gesichert werden, da sie Momentaufnahmen nicht unterstützen. Beachten Sie daher die folgenden Hinweise, bevor Sie die Option `vmprocessvmwithindependent` auf `yes` setzen:

- Nur normale Plattendatenträger werden gesichert. Die Daten auf unabhängigen Platten werden nicht gesichert.
- Die Konfigurationsinformationen für unabhängige Platten werden nicht gesichert. Unabhängige Platten müssen auf einer zurückgeschriebenen Maschine erneut erstellt werden.
- Wenn ein Datenträger über normale und unabhängige Platten verteilt wurde, kann nur der Teil der Datenträgerdaten zurückgeschrieben werden, der sich auf normalen Platten befindet. Folglich ist der Datenträger nach der Zurückschreibung der VM beschädigt, da die Stripes auf den unabhängigen Platten fehlen.
- Die Zurückschreibung auf Dateiebene wird für VMs unterstützt, die über normale und unabhängige Platten verfügen, wenn kein Datenträger über normale und unabhängige Platten verteilt ist. Nur Dateien auf den normalen Platten können zurückgeschrieben werden.
- Die Zurückschreibung auf Dateiebene wird nicht für VMs unterstützt, bei denen mindestens ein Datenträger über normale und unabhängige Platten verteilt ist. Verwenden Sie eine vollständige VM-Zurückschreibung für solche VMs.

Wenn die virtuelle Maschine mindestens einen RDM-Datenträger (Raw Device Mapping) enthält, der im Modus für physische Kompatibilität (pRDM) bereitgestellt wird, verwenden Sie die Option `vmprocessvmwithprdm`, um anzugeben, ob der Client die virtuelle Maschine sichert, wenn eine pRDM-Platte vorhanden ist.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Diese Option ist nur für VMware-Sicherungen gültig und gilt nicht für Microsoft Hyper-V-Sicherungen.

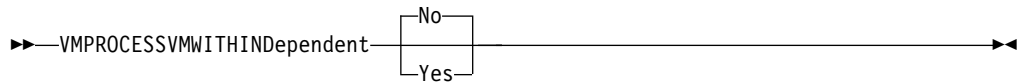
Unterstützte Clients

Diese Option ist für Windows- und Linux-Clients gültig, die als Einheit zum Versetzen von Daten für die VMware-Sicherung konfiguriert sind. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (`dsm.opt`), in die Clientssystemoptionsdatei (`dsm.sys`) oder in die Befehlszeile ein.

Syntax



Parameter

No Die Sicherung der VM schlägt fehl, wenn ein oder mehrere unabhängige Plattendatenträger erkannt werden. No ist der Standardwert.

Yes

Die Sicherung der VM wird fortgesetzt, wenn ein oder mehrere unabhängige Plattendatenträger erkannt werden. Lesen Sie die obigen Hinweise, bevor Sie Yes verwenden.

Beispiele

Optionsdatei:

```
VMPROCESSVMWITHINDEPENDENT Yes
```

Befehlszeile:

```
dsmc backup vm vmlocal -vmbackuptype=fullvm -vmprocessvmwithindependent=yes
```

Vmprocessvmwithprdm

Mit dieser Option können Sie steuern, ob vollständige VMware VM-Sicherungen verarbeitet werden, wenn die virtuelle Maschine über mindestens einen RDM-Datenträger (RDM = raw device mapping) verfügt, der im Modus für physische Kompatibilität (pRDM) bereitgestellt wird.

pRDM-Datenträger unterstützen keine Momentaufnahmen. Alle pRDM-Datenträger, die auf einer virtuellen Maschine gefunden werden, werden nicht als Teil der Sicherungsoperation verarbeitet. Bei der Zurückschreibung der virtuellen Maschine stellt der Client für Sichern/Archivieren die virtuelle Maschine wieder her und es werden nur die Datenträger zurückgeschrieben, die an Momentaufnahmeoperationen teilgenommen haben. Konfigurationsdaten und der Inhalt der pRDM-Datenträger werden in den auf dem IBM Spectrum Protect-Server gespeicherten Informationen nicht beibehalten. Benutzer müssen die pRDM-Datenträger auf der zurückgeschriebenen Maschine erneut erstellen.

Diese Option gilt nicht für virtuelle Maschinen, die über mindestens einen RDM-Datenträger verfügen, der im Modus für virtuelle Kompatibilität (vRDM) bereitgestellt wird. Da vRDM-Datenträger Momentaufnahmeoperationen unterstützen, werden sie in eine vollständige VMware VM-Sicherung eingeschlossen.

Enthält die virtuelle Maschine außerdem eine oder mehrere unabhängige Platten, verwenden Sie die Option `vmprocessvmwithindependent`, um zu steuern, ob der Client Dateien auf der virtuellen Maschine sichert, wenn eine unabhängige Platte vorhanden ist.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Diese Option ist nur für VMware-Sicherungen gültig und gilt nicht für Microsoft Hyper-V-Sicherungen.

Unterstützte Clients

Diese Option ist für Windows- und Linux-Clients gültig, die als VMware-Sicherungsserver konfiguriert sind. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt), in die Clientsystemoptionsdatei (dsm.sys) oder in die Befehlszeile ein.

Syntax



Parameter

No Die Sicherung der virtuellen Maschine schlägt fehl, wenn ein oder mehrere pRDM-Datenträger erkannt werden. No ist der Standardwert.

Yes

Virtuelle Maschinen, die einen oder mehrere RDM-Datenträger enthalten, die im Modus für physische Kompatibilität (pRDM) bereitgestellt werden, werden gesichert. Die pRDM-Datenträger werden jedoch nicht als Teil der VM-Sicherungsoperation verarbeitet.

Enthält die virtuelle Maschine außerdem eine oder mehrere unabhängige Platten, muss auch die Option `vmprocessvmwithindependentdisk` angegeben werden.

Beispiele

Optionsdatei:

```
VMPROCESSVMWITHPRDM Yes
```

Befehlszeile:

```
dsmc backup vm vmlocal -vmbackuptype=fullvm -vmprocessvmwithprdm=yes
```

Vmskipctlcompression

Mit der Option `vmskipctlcompression` können Sie bei VM-Sicherungen angeben, ob Steuerdateien (*.ctl) während einer VM-Sicherung komprimiert werden. Die Option hat keinen Einfluss auf die Komprimierung von Datendateien (*.dat).

Sie können Steuerdateien und Datendateien virtueller Maschinen nur dann komprimieren, wenn die Dateien in einem Speicherpool gespeichert sind, für den die clientseitige Deduplizierung aktiviert ist. Verwenden Sie die folgende Optionskonfiguration, um Datendateien zu komprimieren und Steuerdateien nicht zu komprimieren:

```
compression yes  
vmskipctlcompression yes
```

Sie müssen die Datendateien in einen Speicherpool übertragen, für den die clientseitige Deduplizierung aktiviert ist. Sie können die Steuerdateien in einen Speicherpool übertragen, für den die clientseitige Deduplizierung nicht aktiviert ist.

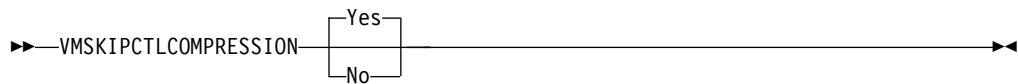
Für diese Option benötigen Sie eine Lizenz für die Verwendung von IBM Spectrum Protect for Virtual Environments.

Unterstützte Clients

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (`dsm.opt`) oder in die Befehlszeile ein.

Syntax



Parameter

Yes

Steuerdateien (*.ctl) während einer VM-Sicherung nicht komprimieren. Die Option hat keinen Einfluss auf die Komprimierung von Datendateien (*.dat).

No Steuerdateien (*.ctl) können während einer VM-Sicherung komprimiert werden. Ob Steuerdateien komprimiert werden, ist vom Wert der Option `compression` abhängig.

Vmskipmaxvirtualdisks

Die Option `vmskipmaxvirtualdisks` gibt an, wie Platten virtueller Maschinen (VM-Platten), die die maximale Plattengröße überschreiten, bei Sicherungsoperationen verarbeitet werden.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Verwenden Sie die Option `vmskipmaxvirtualdisks` mit der Option `vmmxvirtualdisks`, um anzugeben, wie die Einheit zum Versetzen von Daten große VM-Platten während einer Sicherungsoperation verarbeitet:

- Definieren Sie die Option `vmskipmaxvirtualdisks`, um anzugeben, dass die VM-Platten, die die maximale Größe nicht überschreiten, gesichert (und die übrigen VM-Platten ausgeschlossen) werden sollen oder dass die Operation fehlschlagen soll.
- Definieren Sie die Option `vmmxvirtualdisks`, um die maximale Größe von VM-Platten anzugeben, die eingeschlossen werden sollen.

In Data Protection for VMware Version 7.1.3 und früheren Versionen hatte die Option `vmskipmaxvirtualdisks` den Namen `vmskipmaxvmdks`. In Version 7.1.4 und höher ist `vmskipmaxvirtualdisks` der bevorzugte Optionsname. Der Client verarbeitet jedoch noch Sicherungsoperationen mit dem Namen `vmskipmaxvmdks`.

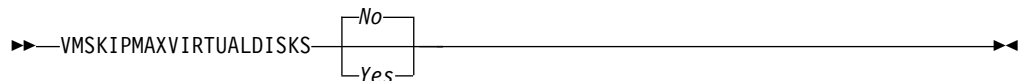
Unterstützte Clients

Diese Option ist für 64-Bit-Linux-Clients gültig, die als Einheiten zum Versetzen von Daten für das Sichern virtueller VMware-Maschinen konfiguriert sind.

Optionsdatei

Definieren Sie die Option `vmskipmaxvirtualdisks` in der Clientsystemoptionsdatei (`dsm.sys`). Sie können diese Option auch als Befehlszeilenparameter im Befehl **backup vm** angeben.

Syntax



Parameter

No Gibt an, dass Sicherungsoperationen fehlschlagen, wenn eine virtuelle Maschine mindestens eine VM-Platte enthält, die die maximale Größe überschreitet. Dies ist die Standardeinstellung.

Yes

Gibt an, dass bei Sicherungsoperationen VM-Platten eingeschlossen werden, die die maximale Größe nicht überschreiten, und VM-Platten ausgeschlossen werden, die die maximale Größe überschreiten.

Beispiele

Optionsdatei:

```
vmskipmaxvirtualdisks yes
```

Befehlszeile:

Angeben, dass eine Sicherungsoperation fehlschlagen soll, wenn eine VM-Platte größer als 2 TB ist:

```
backup vm VM1 -vmskipmaxvirtualdisks=no
```

Angeben, dass eine Sicherungsoperation fehlschlagen soll, wenn eine VM-Platte größer als 5 TB ist:

```
backup vm VM1 -vmskipmaxvirtualdisks=no -vmmaxvirtualdisks=5
```

VM-Platten sichern, die maximal 8 TB groß sind, und VM-Platten ausschließen, die größer als 8 TB sind:

```
backup vm VM1 -vmskipvirtualdisks=yes -vmmaxvirtualdisks=8
```

Vmskipmaxvmdks

Die Option `vmskipmaxvmdks` gibt an, wie die Sicherungsoperation Platten virtueller VMware-Maschinen (VMDKs) verarbeitet, die die maximale Plattengröße überschreiten.

In Version 7.1.4 und höher wird `vmskipmaxvmdks` in `vmskipmaxvirtualdisks` umbenannt. Der bevorzugte Name ist zwar `vmskipmaxvirtualdisks`; der Client verarbeitet jedoch noch Sicherungsoperationen mit dem Namen `vmskipmaxvmdks`.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Vmtagdatamover

Verwenden Sie die Option `vmtagdatamover`, um Tagging-Unterstützung auf dem Client für Sichern/Archivieren (Einheit zum Versetzen von Daten) zu aktivieren. Wenn diese Option aktiviert ist, verwaltet der Client Sicherungen virtueller Maschinen in VMware-Bestandsobjekten gemäß den Datenschutztags, die über die IBM Spectrum Protect vSphere-Client-Plug-in des vSphere-Web-Clients oder mithilfe von Tools wie VMware vSphere PowerCLI Version 5.5 R2 oder höher definiert werden.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Weitere Informationen zu Datenschutztags finden Sie in "Übersicht über das Datenschuttagging".

Die Einheit zum Versetzen von Daten verarbeitet Datenschutztags, wenn die Option `vmtagdatamover` auf `yes` gesetzt ist. Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind.

Voraussetzungen:

- Für die Einheit zum Versetzen von Daten:
 - Der VMware vCenter-Server muss über Version 6.0 Update 1 oder eine höhere Version verfügen.
 - Für das Konto, das für Sicherungs- oder Zurückschreibungsoperationen verwendet wird, sind zusätzliche Berechtigungen erforderlich. Die folgenden neuen vCenter-Berechtigungen sind für die Ausführung von Kategorie- und Tagging-Operationen erforderlich. Stellen Sie sicher, dass diese Benutzerberechtigungen auf dem Root-vCenter-Server definiert sind:
 - Inventory Service > vSphere-Tagging > vSphere-Tag zuweisen oder Zuweisung aufheben
 - Inventory Service > vSphere-Tagging > vSphere-Tag erstellen
 - Inventory Service > vSphere-Tagging > vSphere-Tag-Kategorie erstellen
 - Inventory Service > vSphere-Tagging > vSphere-Tag löschen
 - Inventory Service > vSphere-Tagging > vSphere-Tag-Kategorie löschen
 - Inventory Service > vSphere-Tagging > Feld "Verwendet von" für Tag ändern
 - Inventory Service > vSphere-Tagging > Feld "Verwendet von" für Kategorie ändern
 - Inventory Service > vSphere-Tagging > vSphere-Tag bearbeiten
 - Inventory Service > vSphere-Tagging > vSphere-Tag-Kategorie bearbeiten
- Weitere Informationen zum Definieren von vCenter-Berechtigungen für Sicherungs- und Zurückschreibungsoperationen finden Sie in der Technote 7047438.
- Damit die Data Protection for VMware vSphere-GUI mit Tagging-Unterstützung ordnungsgemäß funktioniert, müssen Sie sicherstellen, dass die folgenden Voraussetzungen während der Installation der GUI erfüllt sind:
 - Mindestens eine Einheit zum Versetzen von Daten und die Data Protection for VMware vSphere-GUI müssen auf demselben Server installiert werden. Dieser Knoten der Einheit zum Versetzen von Daten muss so konfiguriert werden, dass die Berechtigungsnachweise des vCenter-Servers gespeichert werden. Sie können die Berechtigungsnachweise speichern, indem der Konfigurationsassistent zum Speichern des Kennworts für den Knoten der Einheit

zum Versetzen von Daten ausgeführt wird oder der Befehl **dsmc set password** in der Befehlszeile der Einheit zum Versetzen von Daten verwendet wird.

Wenn Sie andere Einheiten zum Versetzen von Daten verwenden, die auf virtuellen Maschinen oder physischen Maschinen als zusätzliche Einheiten zum Versetzen von Daten ausgeführt werden, können Sie diese auf anderen Servern installieren. Für die Tagging-Unterstützung müssen alle diese Einheiten zum Versetzen von Daten auch mit der Option `vmtagdatamover=yes` konfiguriert werden. Diese zusätzlichen Einheiten zum Versetzen von Daten erfordern nicht die Installation der Data Protection for VMware vSphere-GUI auf demselben Server für ihre korrekte Funktionsweise als tag-basierte Einheiten zum Versetzen von Daten.

- Für Linux-Einheiten zum Versetzen von Daten müssen Sie das Installationsverzeichnis der Einheit zum Versetzen von Daten und die gemeinsam genutzte Java™-Bibliothek `libjvm.so` in der Umgebungsvariablen `LD_LIBRARY_PATH` angeben. Der Pfad zu `libjvm.so` wird für die Tagging-Unterstützung verwendet, wenn Sie die Option `vmtagdatamover` auf der Einheit zum Versetzen von Daten aktivieren. Anweisungen finden Sie in "Knoten der Einheit zum Versetzen von Daten in einer vSphere-Umgebung definieren".
- Unter Linux-Betriebssystemen muss die Data Protection for VMware vSphere-GUI mit dem Standardbenutzernamen (`tdpvmware`) installiert werden.
- Auf Knoten der Einheit zum Versetzen von Daten unter Linux muss die Standardkennwortdatei (`/etc/adsm/TSM.sth`) verwendet werden.

Unterstützte Clients

Diese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Optionsdatei

Sie können diese Option in der Clientsystemoptionsdatei (`dsm.sys`) oder in der Befehlszeile für den Befehl **backup vm** angeben. Sie können diese Option auch auf dem IBM Spectrum Protect-Server in einer Clientoptionsgruppe angeben. Sie können diese Option nicht im Profileditor definieren.

Syntax



Parameter

No Der Client ignoriert alle Datenschutzeinstellungen oder -tags, die dem VMware-Asset zugeordnet sind. Dies ist der Standardwert.

Yes

Der Client verwaltet Sicherungen auf der Basis der Datenschutzeinstellungen in der IBM Spectrum Protect vSphere-Client-Plug-in oder auf der Basis der Tagwerte, die dem VMware-Asset zugeordnet sind.

Wenn die Tagging-Unterstützung aktiviert ist, können einige Clientoptionen von den Datenschutzeinstellungen betroffen sein. Informationen zu den betroffenen Optionen finden Sie in "Unterstützte Datenschutztags".

Die folgenden Beispiele zeigen, in welcher Form Clientoptionen von Datenschuttags betroffen sein können:

- Wenn Sie mithilfe von Datenschutzeinstellungen oder -tags steuern, welche virtuellen VMware-Maschinen gesichert werden, überschneiden sich die Tagwerte möglicherweise mit der Einstellung für die Clientoption `domain.vmfull`. Während die Option `domain.vmfull` definiert, welche virtuellen Maschinen der Client schützt, überschreiben die Tags `Excluded` und `Included` den durch die Option `domain.vmfull` definierten Wert.

Beispielsweise gibt die folgende Anweisung in der Optionsdatei an, welche virtuellen Maschinen bei Gesamtsicherungsoperationen für virtuelle Maschinen gesichert werden:

```
DOMAIN.VMFULL VMHOSTCLUSTER=cluster01,cluster02;VM=Dept20*
```

Wenn Sie Datenschutzeinstellungen oder -tags verwenden, um die virtuelle Maschine `Dept204` auszuschließen, wird die virtuelle Maschine `Dept204` nicht gesichert.

- Die Einstellung für die Aufbewahrungsmaßnahme in der IBM Spectrum Protect vSphere-Client-Plug-in oder die Tageinstellung für die Kategorie `Management Class` (IBM Spectrum Protect) setzt die Clientoptionen `include.vm` und `vmmc` außer Kraft, jedoch nicht die Option `vmctlmc`.

Tipp: Wenn eine Einheit zum Versetzen von Daten als die Standardeinheit zum Versetzen von Daten konfiguriert werden soll, verwenden Sie die Option `Vmtagdefaultdatamover`.

Beispiele

Optionsdatei:

```
vmtagdat yes
```

Befehlszeile:

```
-vmtagdat=yes
```

Zugehörige Konzepte:

„Übersicht über das Datenschuttagging“ auf Seite 828

Zugehörige Verweise:

„Unterstützte Datenschuttags“ auf Seite 829

„Vmtagdefaultdatamover“

„Domain.vmfull“ auf Seite 414

„Include.vm“ auf Seite 481

„Vmmc“ auf Seite 659

„Vmctlmc“ auf Seite 639

„Set Vmtags“ auf Seite 826

Zugehörige Informationen:

 Tagging-Unterstützung aktivieren

Vmtagdefaultdatamover

Verwenden Sie die Option `vmtagdefaultdatamover`, um virtuelle Maschinen zu schützen, die in einem Zeitplan definiert sind und denen keine Kategorie und kein Tag Data Mover zugeordnet ist bzw. die keine derartige Kategorie und keinen derartigen Tag geerbt haben.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Wenn Sie den Knoten einer Einheit zum Versetzen von Daten mit der Option `vmtagdefaultdatamover` und der Option `vmtagdatamover yes` angeben, sichert die Einheit zum Versetzen von Daten alle neuen virtuellen Maschinen, die einem beliebigen Container im Datacenter hinzugefügt werden, wenn sich der Container bereits in einer Schutzgruppe befindet. Eine Schutzgruppe besteht aus den virtuellen Maschinen in einem Container, denen die Kategorie und der Tag `Schedule` (IBM Spectrum Protect) zugeordnet sind. Die Standardeinheit zum Versetzen von Daten sichert auch alle virtuellen Maschinen in der Schutzgruppe, denen nicht der Tag `Data Mover` zugeordnet ist.

Wenn mehr als eine Einheit zum Versetzen von Daten einem Zeitplan zugeordnet wird, definieren Sie eine der Einheiten zum Versetzen von Daten mithilfe der Option `vmtagdefaultdatamover` als die Standardeinheit zum Versetzen von Daten. Wenn nur eine einzige Einheit zum Versetzen von Daten einem Zeitplan zugeordnet wird, ordnen Sie diese Einheit zum Versetzen von Daten als die Standardeinheit zu.

Tipp: Geben Sie für jeden Zeitplan nur eine einzige Einheit zum Versetzen von Daten in der zugehörigen Liste der Einheiten zum Versetzen von Daten als die Standardeinheit an. Andernfalls werden alle neuen virtuellen Maschinen und alle virtuellen Maschinen, denen nicht der Tag `Data Mover` zugeordnet ist, mehrmals gesichert.

Datenschutztags können dem vSphere-Bestand zugeordnet werden, um den Schutz virtueller Maschinen zu steuern. Die Liste der unterstützten Kategorien und Tags finden Sie in "Unterstützte Datenschutztags".

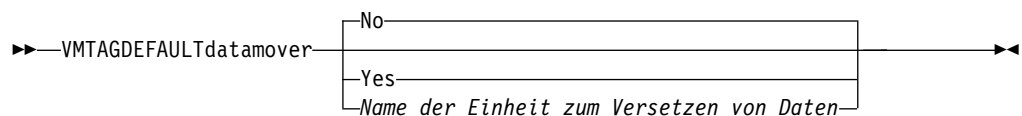
Unterstützte Clients

Diese Option kann für unterstützte Linux x86_64-Einheiten zum Versetzen von Daten verwendet werden.

Optionsdatei

Sie können diese Option in der Clientsystemoptionsdatei (`dsm.sys`) oder in der Befehlszeile für den Befehl **backup vm** angeben. Sie können diese Option auch auf dem IBM Spectrum Protect-Server in einer Clientoptionsgruppe angeben. Sie können diese Option nicht im Profileditor definieren.

Syntax



Parameter

No Die lokale Einheit zum Versetzen von Daten wird nicht als die Standardeinheit zum Versetzen von Daten verwendet. Virtuelle Maschinen, denen nicht der Tag

Data Mover zugeordnet ist, werden nicht durch diese Einheit zum Versetzen von Daten geschützt. Dies ist der Standardwert.

Yes

Gibt an, dass die lokale Einheit zum Versetzen von Daten (die Einheit zum Versetzen von Daten, für die diese Option angegeben wird) als die Standardeinheit zum Versetzen von Daten verwendet wird.

Sie müssen außerdem die Einheit zum Versetzen von Daten für die Tagging-Unterstützung aktivieren, indem Sie die Option `vmtagdatamover yes` angeben.

Name_der_Einheit_zum_Versetzen_von_Daten

Der Name der Einheit zum Versetzen von Daten, die als die Standardeinheit zum Versetzen von Daten verwendet werden soll. Diese Option ist nur erforderlich, wenn diese Option in der Optionsdatei für die Standardeinheit zum Versetzen von Daten festgelegt werden soll. Diese Option wird für alle Einheiten zum Versetzen von Daten außer der Standardeinheit zum Versetzen von Daten ignoriert.

Diese Option kann an alle Einheiten zum Versetzen von Daten im Zeitplanbefehl für den Server übergeben werden oder in alle Optionsdateien der Einheiten zum Versetzen eingeschlossen werden. Diese Option wird nur von der Standardeinheit zum Versetzen von Daten verwendet. Definieren Sie deshalb nur eine einzige Standardeinheit zum Versetzen von Daten.

Sie müssen außerdem die Option `vmtagdatamover yes` in der Optionsdatei auf der Einheit zum Versetzen von Daten angeben, die als die Standardeinheit zum Versetzen von Daten festgelegt werden soll.

Beispiel

Ihre Windows Data Protection for VMware-Konfiguration verwendet zwei Einheiten zum Versetzen von Daten, `VC1_DC1_DM1` und `VC1_DC1_DM2`. Um die Einheit zum Versetzen von Daten mit dem Namen `VC1_DC1_DM1` als die Standardeinheit zum Versetzen von Daten festzulegen, führen Sie die folgenden Schritte aus:

1. Fügen Sie in der Optionsdatei für die Einheit zum Versetzen von Daten mit dem Namen `VC1_DC1_DM1` (`dsm.VC1_DC1_DM1.opt`) die folgenden Anweisungen hinzu:

```
vmtagdatamover yes
vmtagdefaultdatamover yes
```

oder

```
vmtagdatamover yes
vmtagdefaultdatamover VC1_DC1_DM1
```

2. Fügen Sie in der Optionsdatei für die Einheit zum Versetzen von Daten mit dem Namen `VC1_DC1_DM2` (`dsm.VC1_DC1_DM2.opt`) die folgenden Anweisungen hinzu:

```
vmtagdatamover yes
vmtagdefaultdatamover VC1_DC1_DM1
```

Die Option `vmtagdefaultdatamover` kann auch an eine Zeitplandefinition oder einen Befehl übergeben werden, um die Standardeinheit zum Versetzen von Daten zuzuordnen. Wenn die Standardeinheit zum Versetzen von Daten in der Zeitplandefinition definiert wird, können alle Einheiten zum Versetzen von Daten, die dem Zeitplan zugeordnet sind, die Standardeinheit zum Versetzen von Daten für die Schutzgruppe identifizieren.

Beispiel: `dsmc backup vm -vmtagdefaultdatamover=VC1_DC1_DM1`


Zugehörige Verweise:

„Domain.vmfull“ auf Seite 414

„Vmtagdatamover“ auf Seite 668

„Set Vmtags“ auf Seite 826

Zugehörige Informationen:

 Tagging-Unterstützung aktivieren

Vmverifyifaction

Mit dieser Option können Sie die Aktion angeben, die ausgeführt werden soll, wenn die Einheit zum Versetzen von Daten Integritätsprobleme mit den jüngsten CTL- und Bitmapdateien für eine virtuelle Maschine erkennt.

Diese Option wirkt sich nur dann auf die Sicherungsverarbeitung für eine VM-Gastmaschine aus, wenn alle der folgenden Bedingungen vorliegen:

- Die vorherige Sicherungsoperation für die VM-Gastmaschine war eine immer inkrementelle Teilsicherung (mode=ifincremental).
- Die aktuelle Sicherungsoperation für die VM-Gastmaschine ist eine immer inkrementelle Teilsicherung.
- Die Einheit zum Versetzen von Daten erkennt ein Integritätsproblem mit den CTL- und Bitmapdaten der vorherigen immer inkrementellen Teilsicherungsoperation.
- Für die Option `vmverifyiflatest` ist `yes` definiert.

Wenn nicht alle diese Bedingungen für eine virtuelle Maschine zutreffen, findet die Sicherung wie gewohnt statt und die durch diese Option angegebene Aktion wird nicht eingeleitet.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Unterstützte Clients

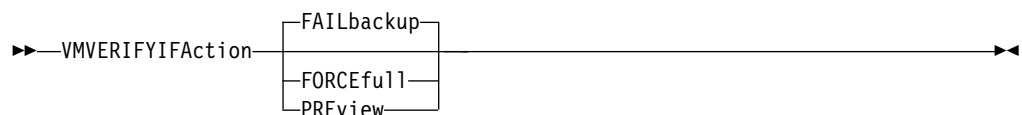
Diese Option ist für Linux-Clients gültig, die als Einheit zum Versetzen von Daten für Sicherungen von VMware-Gastmaschinen fungieren.

Optionsdatei

Definieren Sie diese Option in der Clientoptionsdatei (`dsm.opt`) oder in der Client-systemoptionsdatei (`dsm.sys`).

Diese Option kann auch in einer Clientoptionsgruppe, als Parameter in einem Befehl **backup vm** oder im Parameter **options** in einer Zeitplandefinition angegeben werden.

Syntax



Parameter

FAILbackup

Diese Aktion lässt die Sicherungsoperation fehlschlagen. Die folgenden Nachrichten werden in die Fehlerprotokolldatei der Einheit zum Versetzen von Daten (dsmerror.log) geschrieben:

ANS9921E Für die Platte der virtuellen Maschine *VM-Name* (Plattenkennsatz) ist die Prüfung fehlgeschlagen.

xxx/yyy in der Nachricht gibt die Größe der Bitmapdateien (xxx) und der CTL-Dateien (yyy) an.

ANS9919E Erwartete Steuerdateien für *VM-Name* wurden nicht gefunden.

Führen Sie eine VM-Gesamtsicherung (-mode=IFFull) für die betroffenen virtuellen Maschinen zu einem beliebigen Zeitpunkt aus. Eine Alternative ist die Verwendung von -vmverifyifaction=forcefull bei der nächsten geplanten immer inkrementellen Teilsicherungsoperation, um eine Gesamtsicherung dieser virtuellen Maschinen zu erzwingen, falls Sie feststellen, dass Ihr Fenster für die geplante Sicherung die VM-Gesamtsicherungen für diese virtuellen Maschinen aufnehmen kann. Dieser Wert ist der Standardaktionswert.

FORCEfull

Durch diese Aktion wird der Sicherungsmodus -mode=ifincremental durch -mode=iffull ersetzt; die aktuelle Sicherung wird zu einer VM-Gesamtsicherung. Die VM-Gesamtsicherung wird für Sie eingeleitet. Die folgenden Nachrichten werden in die Fehlerprotokolldatei der Einheit zum Versetzen von Daten (dsmerror.log) geschrieben:

ANS9921E Für die Platte der virtuellen Maschine *VM-Name* (Plattenkennsatz) ist die Prüfung fehlgeschlagen.

xxx/yyy in der Nachricht gibt die Größe der Bitmapdateien (xxx) und der CTL-Dateien (yyy) an.

ANS9919E Erwartete Steuerdateien für *VM-Name* wurden nicht gefunden.

ANS9922I VMVERIFYIFlatest ist für *VM-Name* aktiviert (Aktion: FORCEFULL).

ANS9920W Für *VM-Name* wird eine VM-Gesamtsicherung erzwungen.

Verwenden Sie diese Option, wenn Ihr aktuelles Fenster zum Durchführen von Sicherungen eine VM-Gesamtsicherung der betroffenen virtuellen Maschinen aufnehmen kann.

PREview

Diese Aktion führt keine Sicherungen aus. Stattdessen werden die CTL- und Bitmapdaten jeder VM-Gastmaschine, die der Befehl **backup vm** verarbeitet, in ein temporäres Verzeichnis zurückgeschrieben, wo sie auf Integrität überprüft werden. Wenn die Integritätsprüfung fehlschlägt, werden die folgenden Nachrichten in die Fehlerprotokolldatei der Einheit zum Versetzen von Daten (dsmerror.log) geschrieben:

ANS9921E Für die Platte der virtuellen Maschine *VM-Name* (Plattenkennsatz) ist die Prüfung fehlgeschlagen.

xxx/yyy in der Nachricht gibt die Größe der Bitmapdateien (xxx) und der CTL-Dateien (yyy) an.

ANS9919E Erwartete Steuerdateien für *VM-Name* wurden nicht gefunden.

ANS9922I VMVERIFYIFlatest ist für *VM-Name* aktiviert (Aktion: PREVIEW).

Mit dieser Option können Sie die Integrität der immer inkrementellen Teilsicherungen (-mode=ifincremental) überprüfen, die Sie bereits für mindestens eine virtuelle Maschine erstellt haben.

Wenn die Nachrichten anzeigen, dass einige der virtuellen Maschinen die Integritätsprüfungen nicht bestanden haben, starten Sie eine VM-Gesamtsicherung (-mode=iffull) zu einem beliebigen Zeitpunkt. Sie können auch -vmverifyifaction=forcefull bei der nächsten geplanten immer inkrementellen Teilsicherungsoperation angeben, um eine Gesamtsicherung dieser virtuellen Maschinen zu erzwingen. Das Fenster zum Durchführen von Sicherungen muss so groß sein, dass es mindestens eine VM-Gesamtsicherung aufnehmen kann.

Vmverifyiflatest

Diese Option ist nur für Sicherungsoperationen von virtuellen VMware-Maschinen gültig, die im Modus der immer inkrementellen Teilsicherung ausgeführt werden (d. h. ein Befehl **backup vm** mit der Angabe **-mode=IFIncremental**). Wenn die Option vmverifyiflatest aktiviert ist, führt die Einheit zum Versetzen von Daten eine Integritätsprüfung der CTL- und Bitmapdateien durch, die während der letzten Sicherung auf dem Server erstellt wurden, falls die letzte Sicherung eine immer inkrementelle Teilsicherung war.

Wenn die Dateien die Integritätsprüfungen bestehen, kann die virtuelle Maschine zurückgeschrieben werden. Die aktuelle Sicherung wird fortgesetzt und fügt der Momentaufnahme für die virtuelle Maschine eine weitere Momentaufnahme hinzu.

Wenn die Dateien die Integritätsprüfungen nicht bestehen, kann die virtuelle Maschine nicht zurückgeschrieben werden. Die Einheit zum Versetzen von Daten führt dann eine andere Aktion durch, die Sie mit der Option vmverifyifaction angeben haben. Sie können mit vmverifyifaction angeben, dass sofort eine VM-Gesamtsicherung erstellt wird, oder Sie können die Sicherung vollständig fehlschlagen lassen und eine VM-Gesamtsicherung zu einem anderen Zeitpunkt ausführen. Mit einem dritten Parameter kann angegeben werden, dass die CTL- und Bitmapdateien für eine virtuelle Maschine lediglich überprüft werden, ohne dass eine neue Sicherungsmomentaufnahme erstellt wird.

Die Überprüfung kann nur ausgeführt werden, wenn bei der vorherigen Sicherungsoperation für die virtuelle Maschine mode=IFIncr angegeben wurde und wenn bei der aktuellen Sicherungsoperation auch mode=IFIncr verwendet wird. Diese Option hat keinen Einfluss auf die anderen Sicherungsmodi für virtuelle Maschinen.

Wichtig:

Wird für diese Option no angegeben, wird die Sicherungsverarbeitung der virtuellen Maschinen ohne Prüftests fortgesetzt. Die Verarbeitungsressourcen, die an der Ausführung der Integritätsprüfungen beteiligt sind, sind unerheblich. Um eine fortlaufende Integrität Ihrer immer inkrementellen Teilsicherungskette zu gewährleisten, verwenden Sie den Standardwert (vmverifyiflatest yes). Geben Sie für diese Option nur dann no an, wenn Sie eine entsprechende Anweisung durch IBM Support erhalten.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Unterstützte Clients

Diese Option ist für Linux-Clients gültig, die als Einheit zum Versetzen von Daten für Sicherungen von VMware-Gastmaschinen fungieren.

Optionsdatei

Definieren Sie diese Option in der Clientoptionsdatei (dsm.opt) oder in der Client-systemoptionsdatei (dsm.sys).

Diese Option kann auch in einer Clientoptionsgruppe, als Parameter in einem Befehl **backup vm** oder im Parameter **options** in einer Zeitplandefinition angegeben werden.

Syntax



Parameter

YES

Diese Einstellung gibt an, dass die Überprüfung der CTL- und Bitmapdaten für jede virtuelle Maschine ausgeführt wird, die bei der aktuellen immer inkrementellen Teilsicherungsoperation (mode=IFIncr) verarbeitet wird, wenn die vorherige Sicherungsoperation dieser virtuellen Maschine auch eine immer inkrementelle Teilsicherung war. Dies ist der Standardwert.

NO Diese Einstellung gibt an, dass keine Überprüfung der CTL- und Bitmapdaten während der immer inkrementellen Teilsicherungsverarbeitung stattfindet. Geben Sie diesen Wert nur an, wenn Sie eine entsprechende Anweisung durch IBM Support erhalten.

Beispiele

Optionsdatei:

```
vmverifyiflatest yes
```

Befehlszeile:

```
dsmc backup vm vm1 -mode=ifincremental -vmverifyiflatest=yes
```

Vmvstorcom

Die Option **vmvstorcom** steuert, wie der IBM Spectrum Protect-Client bei Sicherungs- und Zurückschreibungsoperationen die Komprimierung verwendet.

Verwenden Sie diese Option, um die Transportleistung durch Verwendung des NBD-Protokolls (Network Block Device) zu erhöhen.

Drei Komprimierungstypen sind verfügbar: **ZLIB**, **FASTLZ** und **SKIPZ**. Zur Verwendung der Komprimierung müssen Sie die Transportoption mit der Option **Vmvstortransport** auf **NBDSSL** setzen.

Die **NBDSSL**-Komprimierung ist mit vSphere 6.5 und höher verfügbar.

Unterstützte Clients

Diese Option kann für unterstützte Linux x86_64-Clients verwendet werden.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Optionsdatei

Diese Option ist in der Clientsystemoptionsdatei (dsm.sys) oder in der Befehlszeile für **Backup VM** gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profileditor definiert werden.

Syntax



Parameter

ZLIB

Setzt den Komprimierungstyp auf ZLIB mit NBDSSL-Transport.

FASTLZ

Setzt den Komprimierungstyp auf FASTLZ mit NBDSSL-Transport.

SKIPZ

Setzt den Komprimierungstyp auf SKIPZ mit NBDSSL-Transport.

Beispiele

Befehlszeile:

Geben Sie den folgenden Befehl aus, um den Komprimierungstyp und Transportmodus für VM-Sicherungs- und -Zurückschreibungsoperationen mit NBDSSL-Transport zu definieren:

```
dsmc backup vm myVM -VMVSTORCOMP=SKIPZ -VMVSTORTRANSPORT=NBDSSL
```

Mit diesem Beispiel wird die VM myVM mit dem Komprimierungsprotokoll SKIPZ gesichert und die erforderliche Transporteinstellung NBDSSL angegeben.

Optionsdatei:

```
VMVSTORCOMP SKIPZ
```

Zugehörige Verweise:

„Backup VM“ auf Seite 710

„Vmvstortransport“

Vmvstortransport

Die Option `vmvstortransport` gibt die bevorzugte Transportreihenfolge (Hierarchie) an, die beim Sichern oder Zurückschreiben von virtuellen VMware-Maschinen verwendet werden soll. Wenn Sie einen bestimmten Transport mit dieser Option nicht einschließen, wird dieser Transport ausgeschlossen und nicht für die Übertragung von Daten verwendet.

Die von Ihnen angegebene Transportreihenfolge bestimmt, wie die VMware API for Data Protection (VADP) auf Daten virtueller Platten zugreift, aber sie hat keinen Einfluss auf den Datenpfad, der zwischen dem Client für Sichern/Archivieren und dem IBM Spectrum Protect-Server verwendet wird. Zu den gültigen Transportmethoden gehören die folgenden Optionen in beliebiger Reihenfolge oder Kombination:

- nbd** Netzbasierte Datenübertragung (Network based data transfer). Der Zugriff auf virtuelle Plattendaten erfolgt über das LAN. Dieser Transportpfad ist normalerweise in allen Konfigurationen verfügbar.
- nbdssl** Entspricht nbd, die Daten werden jedoch verschlüsselt, bevor sie über das LAN versendet werden. Die Verschlüsselung kann die Leistung beeinträchtigen.
- san** Storage Area Network-Übertragung: Der Zugriff auf virtuelle Plattendaten erfolgt über das SAN (Speicherbereichsnetz).
- hotadd** Wenn Sie den Client für Sichern/Archivieren in einer virtuellen Maschine verwenden, gestattet der Hot-Add-Transport den Transport gesicherter Daten in dynamisch hinzugefügten Speicher.

Trennen Sie die einzelnen Transportoptionen jeweils durch einen Doppelpunkt voneinander. Zum Beispiel: `san:nbd:nbdssl:hotadd`.

Wenn Sie keine Transporthierarchie angeben, lautet die Standardauswahlreihenfolge für den Transport `san:hotadd:nbdssl:nbd`.

Die erste verfügbare Transportmethode wird für die Datenübertragung verwendet. Wenn Sie den Datentransport über einen bestimmten Pfad verhindern wollen, darf er in der Transportliste nicht angegeben werden. Wenn es beispielsweise wichtig ist, den LAN-Verkehr nicht zu unterbrechen, lassen Sie die nbd-Transportmethoden in der Hierarchie weg.



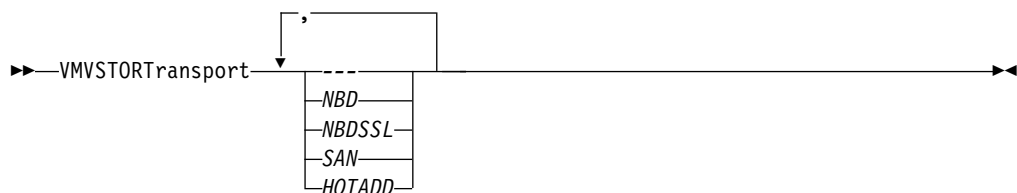
Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Definieren Sie diese Option in der Datei `dsm.sys`.

Unterstützte Clients

Diese Option ist für Linux-Clients gültig, die für die Sicherung oder Zurückschreibung von Dateien virtueller Maschinen mithilfe von VADP konfiguriert sind.

Syntax



Beispiele

Keine Sicherungen oder Zurückschreibungen über das LAN transportieren, wenn das SAN verfügbar ist

```
VMVSTORTTRANSPORT san
```

Der Client für Sichern/Archivieren wird auf einer virtuellen Maschine ausgeführt, den Hot-Add-Transport jedoch nicht verwenden

```
VMVSTORTTRANSPORT nbdssl:nbd
```

LAN-Transport verwenden, auch wenn nbdssl verfügbar ist, um eine bessere Leistung zu erzielen

```
VMVSTORTTRANSPORT nbd
```

Der SAN-Transport wird bevorzugt, aber nbd verwenden, wenn das SAN nicht verfügbar ist, und nicht nbdssl oder hotadd verwenden

```
VMVSTORTTRANSPORT san:nbd
```

Zugehörige Verweise:

„Vmvstorcom“ auf Seite 676

Vmtimeout

VMTIMEout gibt die maximale Wartezeit in Sekunden an, bevor eine VM-Sicherungsoperation (**backup vm**) abgebrochen wird, wenn die Option INCLUDE.VMTSMVSS für die Bereitstellung von Anwendungsschutz verwendet wird. Um diese Option verwenden zu können, muss die IBM Spectrum Protect for Virtual Environments-Lizenz installiert sein.

Für jede VM-Sicherungsoperation (**backup vm**), die auf einer virtuellen Maschine ausgeführt wird, die durch eine Option INCLUDE.VMTSMVSS geschützt wird, gibt es einen Zeitgeber. Der Zeitgeberwert legt fest, wie lange der Client warten soll, bis die Anwendung die Aktivität in den Wartemodus versetzt und ihre Protokolle abgeschnitten hat, so dass die Sicherung ausgeführt werden kann. Der Standardzeitlimitüberschreitungswert ist in den meisten Umgebungen ausreichend. Wenn Ihre Anwendungsdaten jedoch nicht gesichert werden können, weil die Anwendung mehr Zeit für die Vorbereitung der Momentaufnahme benötigt, können Sie den Zeitlimitüberschreitungswert erhöhen. Dieser Zeitgeber ist nur für VM-Sicherungsoperationen (**backup vm**) gültig, wenn die Option INCLUDE.VMTSMVSS für eine virtuelle Maschine definiert ist.

Unterstützte Clients

Diese Option kann für unterstützte Linux-x86_64-Clients verwendet werden.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei ein. Sie kann nicht in der Befehlszeile oder im Profileditor definiert werden.

Syntax



Parameter

Zeitlimitwert

Gibt die für die Ausführung von Sicherungsoperationen zulässige Zeit in Sekunden an, wenn eine virtuelle Maschine durch die Anwendungsschutzoption INCLUDE.VMTSMVSS geschützt ist. Der angegebene Wert muss eine ganze Zahl zwischen 180 und 500 sein. Der Standardwert ist 180 Sekunden.

Beispiele

Optionsdatei

VMTIMEout 500

Befehlszeile:

Nicht gültig. Diese Option kann nicht in der Befehlszeile angegeben werden.

Zugehörige Verweise:

„INCLUDE.VMTSMVSS“ auf Seite 488

Webports

Die Option webports ermöglicht die Verwendung des Web-Clients außerhalb einer Firewall.

Die Option webports ermöglicht die Verwendung des Web-Clients außerhalb einer Firewall, indem sie die TCP/IP-Anschlussnummer angibt, die der IBM Spectrum Protect-Clientakzeptorservice und der Web-Client-Agentenservice für die Kommunikation mit dem Web-Client verwenden.

Sowohl für den Clientakzeptor als auch für den Web-Client-Agentenservice sind Werte erforderlich.

Wenn Sie diese Option nicht angeben, wird der Standardwert 0 für beide Anschlüsse verwendet. Dies bewirkt, dass TCP/IP wahlfrei eine freie Anschlussnummer für den Clientakzeptor und den Web-Client-Agentenservice zuordnet.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe ein. Um diese Option im Profileditor des Clients zu definieren, klicken Sie auf **Editieren > Clientvorgaben > Web-Client** und geben Sie die Anschlüsse in den Feldern **Webagentenanschluss** und **Web-Clientakzeptoranschluss** an.

Syntax

►►—WEBPorts— —CAD-Anschluss— —Agentenanschluss—►►

Parameter

CAD-Anschluss

Gibt die erforderliche Anschlussnummer für den Clientakzeptor an. Der Werte-

bereich ist 1000 bis 32767. Wird kein Wert angegeben, bewirkt der Standardwert Null (0), dass TCP/IP wahlfrei eine freie Anschlussnummer zuordnet.

Agentenanschluss

Gibt die erforderliche Anschlussnummer für den Web-Client-Agentenservice an. Der Wertebereich ist 1000 bis 32767. Wird kein Wert angegeben, bewirkt der Standardwert Null (0), dass TCP/IP wahlfrei eine freie Anschlussnummer zuordnet.

Beispiele

Optionsdatei:

webports 2123 2124

Befehlszeile:

Nicht zutreffend.

Wildcardsareliteral

Die Option `wildcardsareliteral` gibt an, ob Fragezeichen (?) und Sterne (*) buchstäblich interpretiert werden, wenn sie in einer Dateilistenspezifikation in einer Option `filelist` angegeben werden.

Normalerweise akzeptiert der Client keine Platzhalterzeichen (?) und (*) in einer Dateilistenspezifikation, die in einer Option `filelist` enthalten ist. In einigen Dateisystemen sind Hochkommas oder Anführungszeichen in Datei- und Verzeichnisnamen zulässig. Um Fehler zu verhindern, die auftreten, wenn in einer Option `filelist` Dateispezifikationen angegeben werden, die Platzhalterzeichen enthalten, definieren Sie `wildcardsareliteral yes`. Wenn `wildcardsareliteral` auf `yes` gesetzt ist, werden Fragezeichen (?) und Sterne (*), die in einer Dateilistenspezifikation in der Option `filelist` enthalten sind, buchstäblich und nicht als Platzhalterzeichen interpretiert.

Diese Option ist für jeden Befehl gültig, der eine Option `filelist` als Befehlsparameter akzeptiert.

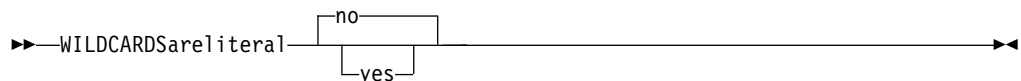
Unterstützte Clients

Diese Option ist für alle unterstützten Plattformen gültig. Die Option wird auf jeden Befehl angewendet, der eine Dateilistenspezifikation als Parameter akzeptiert.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (`dsm.opt`) ein.

Syntax



Parameter

no Gibt an, dass Fragezeichen und Sterne als Platzhalterzeichen interpretiert werden, wenn sie in einer Dateilistenspezifikation verwendet werden, die in einer Option `filelist` enthalten ist. No ist der Standardwert. Wenn eine Dateilisten-

spezifikation in einer Option `filelist` ein Fragezeichen oder einen Stern enthält, tritt ein Fehler auf und die Dateispezifikation kann nicht verarbeitet werden.

yes

Gibt an, dass Sterne und Fragezeichen in einer Dateilistenspezifikation, die in einer Option `filelist` enthalten ist, buchstäblich und nicht als Platzhalterzeichen interpretiert werden. Geben Sie diesen Wert an, wenn Sie Dateien aus einem Dateisystem sichern, in dem Platzhalterzeichen in Datei- oder Verzeichnisnamen zulässig sind.

Beispiele

Optionsdatei:

```
WILDCARDSARELITERAL YES
```

Befehlszeile:

Bei den folgenden Beispielen wird vorausgesetzt, dass das Dateisystem Platzhalterzeichen in Pfadangaben zulässt. Die Beispiele zeigen Dateien in einer Dateilistenspezifikation, die erfolgreich verarbeitet werden können, wenn `WILDCARDSARELITERAL` auf `YES` gesetzt wird.

Der ausgegebene Befehl ist `dsmc sel -filelist=/home/user1/important_files`, wobei `important_files` die Liste der zu verarbeitenden Dateien enthält.

`important_files.txt` enthält die folgende Dateiliste:

```
/home/user1/myfiles/file?9000  
/home/user1/myfiles/?file  
/home/user1/myfiles/**README**version2  
/home/user1/myfiles/ABC?file*
```

Wenn sowohl `WILDCARDSARELITERAL` als auch `QUOTESARELITERAL` auf `YES` gesetzt ist, können folgende Sicherungen erfolgreich verarbeitet werden:

```
/home/user1/myfiles/"file?  
/home/user1/myfiles/?file'  
/home/user1/myfiles/**"README Tomorrow"**  
/home/user1/myfiles/file*
```

Zugehörige Informationen

Informationen zur Option `filelist` finden Sie in „Filelist“ auf Seite 453.

Informationen zur Syntax für Dateispezifikationen finden Sie in „Eingabezeichenfolgen angeben, die Leerzeichen oder Hochkommas oder Anführungszeichen enthalten“ auf Seite 156.

„Quotesareliteral“ auf Seite 544

Kapitel 11. Befehle verwenden

Der Client für Sichern/Archivieren verfügt über eine Befehlszeilenschnittstelle, die Sie alternativ zur grafischen Benutzerschnittstelle verwenden können. Dieser Abschnitt enthält Informationen zum Starten und Beenden einer Clientbefehlssitzung und Anweisungen zur Eingabe von Befehlen.

Es folgt eine Liste der Tasks, die zur Befehlseingabe gehören.

- „Clientbefehlssitzung starten und beenden“ auf Seite 686
- „Clientbefehle, Optionen und Parameter eingeben“ auf Seite 688
- „Platzhalterzeichen“ auf Seite 691

Die folgende Tabelle stellt eine alphabetische Liste der Befehle und eine Kurzbeschreibung bereit.

Tabelle 80. Befehle

Befehl	Beschreibung
archive „Archive“ auf Seite 692	Archiviert Dateien von einer Workstation in den IBM Spectrum Protect-Speicher.
backup fastback „Backup FastBack“ auf Seite 697	Sichert durch die Optionen fbpolycname, fbclientname und fbvolumename angegebene Datenträger für die langfristige Aufbewahrung.
backup group „Backup Group“ auf Seite 699	Erstellt eine Gruppe, die eine Liste von Dateien aus einem oder mehreren Dateibereichsursprüngen enthält, und sichert sie in einem virtuellen Dateibereich auf dem IBM Spectrum Protect-Server.
backup image „Backup Image“ auf Seite 702	Erstellt eine Imagesicherung der von Ihnen angegebenen Dateisysteme oder logischen Datenträger.
backup nas „Backup NAS“ auf Seite 708	Erstellt eine Imagesicherung eines oder mehrerer Dateisysteme, die zu einem NAS-Dateiserver (NAS - Network Attached Storage, Netzspeicher) gehören.
backup vm „Backup VM“ auf Seite 710	Sichert virtuelle Maschinen, die in der Option vmlist angegeben sind.
cancel process „Cancel Process“ auf Seite 719	(Falls NDMP-Unterstützung aktiviert ist:) Zeigt eine Liste der aktuellen Prozesse für NAS-Imagesicherung und -zurückschreibung an, für die der Benutzer mit Verwaltungsaufgaben berechtigt ist.
cancel restore „Cancel Restore“ auf Seite 719	Zeigt eine Liste der wiederanlauffähigen Zurückschreibungssitzungen an, aus der Sie eine zum Abbrechen auswählen können.
delete access „Delete Access“ auf Seite 720	Löscht Berechtigungsregeln für Dateien, die auf dem Server gespeichert sind. Auf den Clients, die Imagesicherung unterstützen, löscht dieser Befehl die Berechtigungsregeln für Images, die auf dem Server gespeichert sind.
delete archive „Delete Archive“ auf Seite 721	Löscht archivierte Dateien aus dem IBM Spectrum Protect-Serverspeicher.
delete backup „Delete Backup“ auf Seite 722	Löscht aktive und inaktive Sicherungsdateien aus dem IBM Spectrum Protect-Serverspeicher.

Tabelle 80. Befehle (Forts.)

Befehl	Beschreibung
delete filespace „Delete Filespace“ auf Seite 727	Löscht Dateibereiche aus dem IBM Spectrum Protect-Serverspeicher.
delete group „Delete Group“ auf Seite 728	Löscht eine Gruppensicherung auf dem IBM Spectrum Protect-Server.
expire „Expire“ auf Seite 729	Inaktiviert die Sicherungsobjekte, die Sie in der Dateispezifikation oder mit der Option <code>filelist</code> angeben.
help „Help“ auf Seite 731	Zeigt ein Inhaltsverzeichnis der Hilfethemen für den Befehlszeilenclient an.
incremental „Incremental“ auf Seite 732	Sichert alle neuen oder geänderten Dateien oder Verzeichnisse in der Standardclientdomäne oder in von Ihnen angegebenen Dateisystemen, Verzeichnissen oder Dateien, sofern Sie sie nicht von den Sicherungsservices ausschließen.
loop „Loop“ auf Seite 739	Startet eine interaktive Befehlssitzung.
macro „Macro“ auf Seite 741	Führt Befehle innerhalb einer Makrodatei aus, die Sie angeben.
monitor process „Monitor Process“ auf Seite 742	Zeigt eine Liste der aktuellen NAS-Imagesicherungs- und -zurückschreibungsprozesse an, in der Sie einen Prozess auswählen können, der abgebrochen werden soll.
preview archive „Preview Archive“ auf Seite 742	Simuliert einen Archivierungsbefehl, ohne Daten an den Server zu senden.
preview backup „Preview Backup“ auf Seite 744	Simuliert einen Sicherungsbefehl, ohne Daten an den Server zu senden.
query access „Query Access“ auf Seite 745	Zeigt eine Liste der aktuellen Berechtigungsregeln an.
query archive „Query Archive“ auf Seite 745	Zeigt eine Liste der archivierten Dateien an.
query backup „Query Backup“ auf Seite 748	Zeigt eine Liste der Sicherungsversionen an.
query backupset „Query Backupset“ auf Seite 751	Frägt einen Sicherungssatz von einer lokalen Datei oder vom IBM Spectrum Protect-Server ab. Auf den Clients, die Bandeinheiten unterstützen, kann dieser Befehl einen Sicherungssatz von einer Bandeinheit abfragen.
query filespace „Query Filespace“ auf Seite 754	Zeigt eine Liste der Dateibereiche im IBM Spectrum Protect-Speicher an. Sie können auch einen einzelnen Dateibereich für die Abfrage angeben.
query group „Query Group“ auf Seite 756	Zeigt Informationen zu Gruppensicherungen und ihren Members an.
query image „Query Image“ auf Seite 758	Zeigt Informationen zu Imagesicherungen an.
query inclexcl „Query Inclexcl“ auf Seite 760	Zeigt eine Liste der Include/Exclude-Anweisungen in der Reihenfolge an, in der sie bei Sicherungs- und Archivierungsoperationen verarbeitet werden.
query mgmtclass „Query Mgmtclass“ auf Seite 761	Zeigt Informationen zu verfügbaren Verwaltungsklassen an.
query node „Query Node“ auf Seite 762	Zeigt alle Knoten an, für die eine Verwaltungsbenutzer-ID die Berechtigung zum Ausführen von Operationen hat.

Tabelle 80. Befehle (Forts.)

Befehl	Beschreibung
query options „Query Options“ auf Seite 763	Zeigt alle oder einen Teil Ihrer Optionen und ihre aktuellen Einstellungen an.
query restore „Query Restore“ auf Seite 764	Zeigt eine Liste der wiederanlauffähigen Zurückschreibungssitzungen in der Serverdatenbank an.
query schedule „Query Schedule“ auf Seite 765	Zeigt Informationen zu geplanten Ereignissen für Ihren Knoten an.
query session „Query Session“ auf Seite 765	Zeigt Informationen zu Ihrer Sitzung an, z. B. den aktuellen Knotennamen, die Angabe, wann die Sitzung aufgebaut wurde, Serverinformationen und Serververbindungsdaten.
query systeminfo „Query Systeminfo“ auf Seite 766	Stellt IBM Spectrum Protect-Systeminformationen zusammen und gibt diese Informationen in einer Datei oder an der Konsole aus.
query vm „Query VM“ auf Seite 768	Überprüft, ob die virtuellen Maschinen erfolgreich von dem vStorage-Sicherungsserver gesichert wurden.
restart restore „Restart Restore“ auf Seite 771	Zeigt eine Liste der wiederanlauffähigen Zurückschreibungssitzungen an, aus der Sie eine zum erneuten Starten auswählen können.
restore „Restore“ auf Seite 771	Schreibt Kopien von Sicherungsversionen Ihrer Dateien vom IBM Spectrum Protect-Server zurück.
restore backupset „Restore Backupset“ auf Seite 777	Schreibt einen Sicherungssatz vom IBM Spectrum Protect-Server oder aus einer lokalen Datei zurück. Auf den Clients, die Bandeinheiten unterstützen, kann dieser Befehl einen Sicherungssatz von einer Bandeinheit zurückschreiben.
restore group „Restore Group“ auf Seite 784	Schreibt bestimmte oder alle Member einer Gruppensicherung zurück.
restore image „Restore Image“ auf Seite 786	Schreibt ein Dateisystemimage oder das Image eines unformatierten Datenträgers zurück.
restore nas „Restore NAS“ auf Seite 789	Schreibt das Image eines Dateisystems zurück, das zu einem NAS-Dateiserver gehört.
restore vm „Restore VM“ auf Seite 791	Schreibt eine VM-Gesamtsicherung zurück und stellt die Dateien der VM-Gesamtsicherung in das Verzeichnis <code>vmbackdir</code> auf dem vStorage-Sicherungsserver.
retrieve „Retrieve“ auf Seite 805	Ruft Kopien archivierter Dateien vom IBM Spectrum Protect-Server ab.
schedule „Schedule“ auf Seite 808	Startet den Client-Scheduler auf der Workstation.
selective „Selective“ auf Seite 810	Sichert ausgewählte Dateien.
set access „Set Access“ auf Seite 814	Berechtigt einen anderen Benutzer für den Zugriff auf Ihre Sicherungsversionen oder Archivierungskopien. Auf den Clients, die Imagesicherung unterstützen, können Sie mit diesem Befehl die Berechtigungsregeln für Images definieren, die auf dem Server gespeichert sind.
set event „Set Event“ auf Seite 817	Ermöglicht Ihnen die Angabe der Umstände, wenn archivierte Daten gelöscht werden.

Tabelle 80. Befehle (Forts.)

Befehl	Beschreibung
set netappsvm Set Netappsvm	Ordnet die Berechtigungsnachweise für Anmeldung eines Cluster-Management-Servers einer NetApp Storage Virtual Machine und dem Daten-SVM-Namen (Data Vserver) zu. Dieser Befehl muss eingegeben werden, bevor Sie eine Momentaufnahmedifferenzteilsicherung eines NetApp-Clusterdatenträgers erstellen können.
set password „Set Password“ auf Seite 820	Ändert das IBM Spectrum Protect-Kennwort für die Workstation.

Für den ordnungsgemäßen Betrieb ist es unbedingt erforderlich, dass der WAS-Knoten an derselben Position und unter demselben Namen zurückgeschrieben wird.

Wichtig: Um Probleme zu vermeiden, sollten Sie Ihre Daten nur auf der Ebene des Network Deployment Manager-Knotens oder des Application Server-Knotens zurückschreiben.

Zugehörige Verweise:

„Syntaxdiagramme lesen“ auf Seite xiv

Clientbefehlssitzung starten und beenden

Eine Clientbefehlssitzung kann im Stapelbetrieb oder im interaktiven Modus gestartet oder beendet werden.

Den Stapelbetrieb verwenden, wenn ein *einzelner* Clientbefehl eingegeben werden soll. Der Client für Sichern/Archivieren verarbeitet den Befehl und kehrt zur Eingabeaufforderung zurück.

Den interaktiven Modus verwenden, wenn eine *Reihe* von Befehlen eingegeben werden soll. Da der Client die Verbindung zum Server nur einmal für den interaktiven Modus aufbaut, können mehrere Befehle schneller verarbeitet werden. Der Client verarbeitet die Befehle und kehrt zur Eingabeaufforderung Protect> zurück.

Befehle im Stapelbetrieb verarbeiten

Einige Optionen sind *nur* in Anfangsbefehlszeile und nicht im interaktiven Modus gültig. Diese Optionen haben im Allgemeinen Auswirkungen auf den Betrieb der gesamten Sitzung.

Beispielsweise wird der Befehl **dsmc query session -errorlogname=myerror.log** akzeptiert und gibt den Namen des Fehlerprotokolls an. Er wird jedoch aus dem einfachen Grund akzeptiert, dass er im Anfangsbefehl erscheint, obwohl die Option für den Befehl query nicht gültig ist.

Es gibt auch einige Optionen, die immer in der Anfangsbefehlszeile als auch in einzelnen Befehlen im interaktiven Modus gültig sind. Demzufolge werden bestimmte Optionen in der Anfangsbefehlszeile selbst dann akzeptiert, wenn sie keine Auswirkungen auf den eingegebenen Befehl haben. Beispielsweise ist **dsmc query session -subdir=yes** ein gültiger Befehl; in diesem Fall hat die Option *-subdir* jedoch keine Auswirkungen auf den eingegebenen Befehl.

Wird ein *einzelner* Befehl im Stapelbetrieb eingegeben, muss ihm der Name des ausführbaren Programms, **dsmc**, vorangestellt werden. Soll beispielsweise der Befehl **incremental** im Stapelbetrieb verarbeitet werden, Folgendes eingeben:

```
dsmc incremental
```

Der Client für Sichern/Archivieren fordert Sie bei jeder Befehlseingabe zur Eingabe des Kennworts auf, wenn die Option *passwordaccess* auf *prompt* und die Authentifizierung auf dem Server auf *On* gesetzt ist. Das Kennwort eingeben und die Eingabetaste drücken.

Das Kennwort kann auch mit der Option *password* in einem Befehl eingegeben werden. In diesem Fall wird das Kennwort jedoch auf dem Bildschirm angezeigt. Lautet das Kennwort zum Beispiel *secret*, Folgendes eingeben:

```
dsmc incremental -password=secret
```

Wird die Option *passwordaccess* in der Datei *dsm.opt* auf *generate* gesetzt, muss das Kennwort nicht im Befehl angegeben werden. Der Client fordert die Eingabe des Kennworts nur an, wenn Sie die Workstation bei einem Server registrieren oder das Kennwort manuell ändern.

Zugehörige Konzepte:

Kapitel 10, „Verarbeitungsoptionen“, auf Seite 323

Befehle im interaktiven Modus verarbeiten

Der *interaktive Modus* (Dialogmodus oder *Schleifenmodus*) dient zur Eingabe einer Reihe von Befehlen.

Geben Sie **dsmc** in die Befehlszeile ein und drücken Sie die Eingabetaste. Wenn die Eingabeaufforderung *Protect>* angezeigt wird, geben Sie den Befehlsnamen ein und drücken Sie die Eingabetaste. Den einzelnen Befehlen muss nicht der Name des ausführbaren Programms, **dsmc**, vorangestellt werden. Alternativ können Sie **dsmc loop** in die Befehlszeile eingeben, um eine Clientbefehlssitzung im interaktiven Modus zu starten. **Loop** ist der Standardbefehl für **dsmc**.

Falls ein Kennwort erforderlich ist, fordert Sie der Client für Sichern/Archivieren vor der Eingabe des ersten Befehls zur Eingabe des Kennworts auf.

Geben Sie Ihre Benutzer-ID und Ihr Kennwort ein und drücken Sie die Eingabetaste.

Das Kennwort kann auch mit der Option *password* im Befehl **loop** eingegeben werden. In diesem Fall wird das Kennwort jedoch auf dem Bildschirm angezeigt. Lautet das Kennwort zum Beispiel *secret*, Folgendes eingeben:

```
dsmc loop -password=secret
```

Soll eine interaktive Sitzung beendet werden, *quit* an der Eingabeaufforderung eingeben.

Anmerkung für UNIX- und Linux-Clients:

Im Schleifenmodus wird der Mountpunkt nach einer Zurückschreibungsoperation direkt vom Band nicht freigegeben, falls weitere Zurückschreibungsanforderungen an den Datenträger gestellt werden. Wenn Sie eine Sicherungsoperation in derselben Sitzung anfordern und dieser Mountpunkt der einzig verfügbare ist, stoppt die Sicherungsoperation mit der folgenden Nachricht:

Auf Laden von Offlinedatenträger warten

In diesem Fall wird der Mountpunkt erst freigegeben, wenn eine der folgenden Bedingungen erfüllt ist:

- Der Grenzwert der Einheitenklasse MOUNTRETENTION ist erreicht.
- Das Clientinaktivitätszeitlimit ist erreicht.
- Die Sitzung dsmc loop wird geschlossen, nachdem die Zurückschreibungsoperation beendet ist. Dies ermöglicht Ihnen den Start einer nachfolgenden Sitzung im Schleifenmodus, um die Sicherungsoperation auszuführen.

Clientbefehle, Optionen und Parameter eingeben

Ein Clientbefehl kann eine oder mehrere der folgenden Komponenten beinhalten: *Befehlsname*, *Optionen* und *Parameter*. Diese Komponenten werden in den folgenden Abschnitten beschrieben.

Befehlsname

Der erste Teil eines Befehls ist der Befehlsname. Der Befehlsname besteht aus einem Wort, wie z. B. **help** (Hilfe) oder **schedule** (Zeitplan), oder aus einem Aktionswort und einem Objekt für die Aktion, wie z. B. **query archive** (Archivierung abfragen).

Der Benutzer kann den vollständigen Befehlsnamen oder seine Mindestabkürzung eingeben.

Für den Befehl **query schedule** sind beispielsweise folgende Versionen möglich:

```
query schedule
q sc
q sched
query sc
```

Optionen

Werden Optionen mit einem Befehl eingegeben, muss der Option immer ein Bindestrich (-) vorausgehen. Fügen Sie zwischen dem Bindestrich und dem Optionsnamen kein Leerzeichen ein!

In einen Befehl können mehrere Optionen in beliebiger Reihenfolge vor oder hinter der Dateispezifikation eingegeben werden. Mehrere Optionen müssen durch eine Leerstelle voneinander getrennt werden.

Für Befehle können zwei Gruppen von Optionen verwendet werden: Clientoptionen (in der Optionsdatei definiert) oder Clientbefehlsoptionen (in der Befehlszeile verwendet).

- **Clientoptionen:** Die Gruppe von Optionen, die in Ihrer Clientoptionsdatei definiert sind. Sie können eine Option in der Clientoptionsdatei überschreiben, indem Sie die Option zusammen mit einem Befehl in die Befehlszeile eingeben.
- **Clientbefehlsoptionen:** Verwenden Sie eine Clientbefehlsoption *nur*, wenn Sie die Option zusammen mit einem Befehl in die Befehlszeile eingeben. Sie können diese Optionen nicht in einer Optionsdatei definieren.

Zugehörige Konzepte:

„Clientoptionsreferenz“ auf Seite 355

Optionen im interaktiven Modus

Im interaktiven Modus überschreiben die Optionen, die Sie in der Anfangsbefehlszeile eingeben, den Wert, den Sie in Ihrer Optionsdatei angegeben haben.

Dieser Wert bleibt für die gesamte interaktive Sitzung aktiv, solange er nicht durch einen anderen Wert in einem angegebenen interaktiven Befehl überschrieben wird.

Beispiel: Wenn Sie die Option `subdir` in Ihrer Datei `dsm.opt` oder `dsm.sys` auf `yes` setzen und in der Anfangsbefehlszeile `subdir=no` angeben, bleibt die Einstellung `subdir=no` während der gesamten interaktiven Sitzung aktiv, wenn sie nicht durch den Wert `subdir=yes` in einem angegebenen interaktiven Befehl überschrieben wird. Der in der interaktiven Sitzung angegebene Wert `subdir=yes` betrifft jedoch nur den Befehl, in dem er eingegeben wird. Wenn dieser Befehl beendet ist, wird der Wert auf `subdir=no` zurückgesetzt, d. h. auf den Wert, den die Option zu Beginn der interaktiven Sitzung hatte.

Parameter

Befehle können erforderliche Parameter, optionale Parameter oder keine Parameter haben.

Erforderliche Parameter liefern Informationen zur Ausführung einer Task. Der am häufigsten verwendete erforderliche Parameter ist eine Dateispezifikation.

Soll beispielsweise die Datei `budget.fin` aus dem Verzeichnis `/project` archiviert werden, geben Sie Folgendes ein:

```
dsmc archive /project/budget.fin
```

Einige Befehle verfügen über optionale Parameter. Wird für einen optionalen Parameter kein Wert eingegeben, verwendet der Client für Sichern/Archivieren den Standardwert. Der Befehl **restore** verfügt beispielsweise über einen erforderlichen Parameter, **Quelldateispezifikation**, der den Pfad und den Namen der Datei im Speicher angibt, die zurückgeschrieben werden soll. Der optionale Parameter, **Zieldateispezifikation**, gibt den Pfad für die Speicherung der zurückgeschriebenen Dateien an. Wird die **Zieldateispezifikation** nicht angegeben, schreibt der Client die Dateien standardmäßig in den ursprünglichen Quellenpfad zurück. Sollen die Dateien in ein *anderes* Verzeichnis zurückgeschrieben werden, geben Sie einen Wert für **Zieldateispezifikation** ein.

Beispiel: Die Datei `/project/budget.fin` in den neuen Pfad `/newproj/newbudg.fin` zurückschreiben.

```
dsmc restore /project/budget.fin /newproj/
```

Die Parameter müssen in der im Befehlssyntaxdiagramm angegebenen Reihenfolge eingegeben werden.

Syntax der Dateispezifikation

Es gelten einige Syntaxregeln, die Sie kennen sollten, wenn Sie Dateispezifikationsparameter wie **Dateispezifikation**, **Quelldateispezifikation** und **Zieldateispezifikation** angeben.

Es folgen die Syntaxregeln:

- Der Dateibereichsname und die **Zieldateispezifikation** dürfen keine Platzhalterzeichen enthalten. Eine Ausnahme bildet hierbei der Befehl **set access**, bei dem Platzhalterzeichen in den beiden niedrigsten Ebenen der Dateispezifikation zulässig sind.

Beispiel: Zugriff auf alle Dateien in allen Verzeichnissen in und unter dem Verzeichnis /home erteilen:

```
set access backup /home/* * *  
set access backup /home/*/* * *
```

Bei UNIX-Clients dürfen in einem Verzeichnispfadnamen keine Platzhalterzeichen verwendet werden, z. B.:

```
/home/j*asler/file1.c
```

- Beachten Sie die maximale Anzahl der Dateispezifikationen pro Befehl:
 - Die Befehle **Query** können nur eine Dateispezifikation enthalten.
 - Die Befehle **restore** und **retrieve** können eine Quelldateispezifikation und eine Zieldateispezifikation enthalten.
 - Für einige Befehle gilt eine Begrenzung auf 20 Operanden. Mithilfe dieses Grenzwerts wird verhindert, dass sehr viele Sitzungen geöffnet werden, wenn die Platzhalterzeichen vom Befehlsprozessor der UNIX-Shell erweitert werden.

Sie können verhindern, dass aufgrund der Shellerweiterung der Grenzwert von 20 Operanden überschritten wird, indem Sie am Anfang und am Ende der Erweiterungszeichen Ihrer Quelldateispezifikation in Befehlen zum Zurückschreiben Anführungszeichen eingeben.

Anmerkung: Die Verwendung von Anführungszeichen bewirkt als Nebeneffekt die Ausführung einer Zurückschreibung ohne Abfrage.

Sie können mit der Option `removeoperandlimit` angeben, dass der Client für Sichern/Archivieren die Begrenzung auf 20 Operanden entfernen soll. Wenn Sie die Option `removeoperandlimit` mit dem Befehl **incremental**, **selective**, **archive** oder **backup image** angeben, wird die Beschränkung auf 20 Operanden nicht umgesetzt und nur durch die verfügbaren Ressourcen oder andere Begrenzungen des Betriebssystems eingeschränkt.

- Die Länge einer Dateispezifikation ist begrenzt.
 - Bei AIX, Solaris und Mac: Die maximale Anzahl Zeichen für einen Dateinamen beträgt 255. Die maximale Länge der Kombination aus Dateiname und Pfadname ist 1024 Zeichen. Die Unicode-Darstellung eines Zeichens kann mehrere Byte in Anspruch nehmen, sodass die maximale Anzahl Zeichen, die ein Dateiname enthalten könnte, variieren kann.
 - Unter Linux: Die maximale Länge für einen Dateinamen beträgt 255 Byte. Die maximale Länge der Kombination aus Dateiname und Pfadname beträgt 4096 Byte. Diese Länge entspricht dem vom Betriebssystem unterstützten Wert für `PATH_MAX`. Die Unicode-Darstellung eines Zeichens kann mehrere Byte in Anspruch nehmen, sodass die maximale Anzahl Zeichen, aus denen ein Pfad- und Dateiname besteht, variieren kann. Die tatsächliche Begrenzung ist die Anzahl Byte in den Pfad- und Dateikomponenten, die einer gleichen Anzahl Zeichen entsprechen kann.

Unter Linux: Bei Archivierungs- oder Abrufoperationen bleibt die maximale Länge, die Sie für eine Kombination aus Pfad- und Dateinamen angeben können, bei 1024 Byte.

- Wenn bei Eingabe der **Quelldateispezifikation** der Verzeichnisname mit / endet, wird /* impliziert.

Wenn bei Eingabe einer **Zieldateispezifikation** der Name mit / endet, wird er als Verzeichnis betrachtet, andernfalls als Datei.

Das folgende Beispiel verdeutlicht diese beiden Regeln. Obwohl es sich bei `mydir` und `yourdir` um Verzeichnisse handelt, schlägt der Befehl fehl, weil /* hinter `mydir` impliziert und `yourdir` als Datei betrachtet wird.

```
restore /home/mydir/ /away/yourdir
restore c:\home\mydir\ c:\away\yourdir
```

- Wenn eine Dateispezifikation nicht mit einem Verzeichnisbegrenzer beginnt, wird die Dateispezifikation als ein Unterverzeichnis des aktuellen Arbeitsverzeichnisses betrachtet. Der Client hängt die Dateispezifikation an das Arbeitsverzeichnis an, um den vollständigen Pfad zu erstellen.

Beispiel: Ist das aktuelle Arbeitsverzeichnis /home/me und der Befehl `dsmc res "/fs/dir1/*" mydir/`, lautet der vollständige Zurückschreibungspfad wie folgt: /home/me/mydir.

- Nur der Befehl **incremental** akzeptiert einen einfachen Dateibereichsnamen. Das folgende Beispiel ist gültig:

```
dsmc i /Users
```

Das folgende Beispiel ist nicht gültig, da es sich bei dem Befehl um den Befehl **selective** handelt:

```
dsmc sel /Users
```

Zugehörige Verweise:

„Filelist“ auf Seite 453

„Removeoperandlimit“ auf Seite 546

Platzhalterzeichen

Platzhalterzeichen werden verwendet, wenn mehrere Dateien mit ähnlichen Namen in *einem* Befehl angegeben werden sollen. Ohne Platzhalterzeichen muss der Befehl für jede Datei wiederholt werden.

In einem Befehl können Sie Platzhalterzeichen *nur* innerhalb des Dateinamens oder innerhalb der Dateierweiterung verwenden. Sie können nicht zur Angabe von Zieldateien, Dateisystemen oder Servernamen verwendet werden. Sie können kein Verzeichnis angeben, dessen Name einen Stern (*) oder ein Fragezeichen (?) enthält.

Folgende Platzhalterzeichen sind gültig:

- * Stern. Entspricht null oder mehr Zeichen.
- ? Fragezeichen. Entspricht einem beliebigen Einzelzeichen an der aktuellen Position.

Die folgende Tabelle zeigt Beispiele der einzelnen Platzhalterzeichen.

Tabelle 81. Platzhalterzeichen

Muster	Entspricht	Entspricht nicht
Stern (*)		
ab*	ab, abb, abxxx	a, b, aa, bb
ab*rs	abrs, abtrs, abrsrs	ars, aabrs, abrss
ab*ef*rs	abefrs, abefghrs	abefr, abers
abcd.*	abcd.c, abcd.txt	abcd, abcdc, abcdtxt
Fragezeichen (?)		
ab?	abc	ab, abab, abzzz
ab?rs	abfrs	abrs, abllrs
ab?ef?rs	abdefrs	abefrs, abdefrs, abefjrs

Tabelle 81. Platzhalterzeichen (Forts.)

Muster	Entspricht	Entspricht nicht
ab??rs	abcdrs, abzzrs	abrs, abjrs, abkkrs

Wichtig: Verwenden Sie einen Stern (*) statt eines Fragezeichens (?) als Platzhalterzeichen, wenn Sie nach einer Übereinstimmung mit einem Muster in einer Mehrfachbyte-Codepage suchen, um unerwartete Ergebnisse zu verhindern.

Anmerkung: Im Stapelbetrieb schließen Sie Werte, die Platzhalterzeichen enthalten, in Anführungszeichen ein. Andernfalls erweitern UNIX-Shells Platzhalterzeichen (ohne Anführungszeichen), und es wird schnell die Begrenzung auf 20 Operanden überschritten. Es ist effizienter, dem Client die Verarbeitung von Dateispezifikationen mit Platzhalterzeichen zu überlassen, da hier viel weniger Serverinteraktionen benötigt werden, um die Task zu beenden. Beispiel:

```
dsmc selective "/home/me/*.c"
```

Clientbefehlsreferenz

Die folgenden Abschnitte enthalten detaillierte Informationen zu den Befehlen des Clients für Sichern/Archivieren.

Die Informationen zu jedem Befehl umfassen Folgendes:

- Eine Beschreibung des Befehls.
- Ein Syntaxdiagramm des Befehls.
- Detaillierte Beschreibungen der Befehlsparameter. Ist der Parameter eine Konstante (ein Wert, der sich nicht ändert), wird die Mindestabkürzung in Großbuchstaben angezeigt.
- Beispiele für die Verwendung des Befehls.

Archive

Mit dem Befehl **archive** können einzelne Dateien, ausgewählte Dateien oder alle Dateien in einem Verzeichnis und in den zugehörigen Unterverzeichnissen auf einem Server archiviert werden.

Es werden die Dateien archiviert, deren aktueller Status aufbewahrt werden soll. Um Speicherbereich auf Ihrer Workstation freizugeben, sollten Sie Dateien mit Hilfe der Option **deletefiles** nach ihrer Archivierung löschen. Werden die archivierten Dateien wieder auf der Workstation benötigt, können sie jederzeit abgerufen werden.

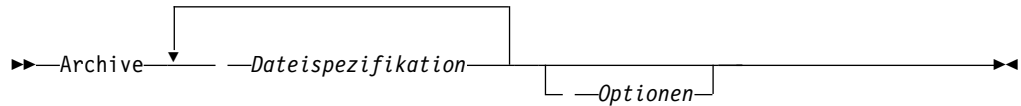
Wenn Sie eine Anwendung eines unabhängigen Softwareanbieters zur Erstellung einer Momentaufnahme eines logischen Datenträgers benutzen, verwenden Sie die Option **snapshotroot** im Befehl **archive**, um die Daten der lokalen Momentaufnahme den originalen Dateibereichsdaten zuzuordnen, die auf dem IBM Spectrum Protect-Server gespeichert sind. Die Option **snapshotroot** bietet keine Funktionen zur Erstellung einer Datenträgermomentaufnahme, sondern ausschließlich Funktionen zur Verwaltung von Daten, die durch Erstellen einer Datenträgermomentaufnahme generiert werden.

Nur für AIX: Mit Hilfe der Option **snapshotproviderfs=JFS2** können Sie die Dateiarchivierung auf Momentaufnahmebasis aktivieren.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax



Parameter

Dateispezifikation

Gibt den Pfad und den Namen der Datei an, die archiviert werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis anzugeben.

Sollen mehrere Dateispezifikationen angegeben werden, trennen Sie die einzelnen Parameter *Dateispezifikation* durch ein Leerzeichen voneinander. Werden mehrere Dateispezifikationen angegeben und haben mindestens zwei der Spezifikationen gemeinsame übergeordnete Verzeichnisse, kann es vorkommen, dass die gemeinsamen Verzeichnisobjekte mehrmals archiviert werden. Die Bedingungen, unter denen dieses Verhalten auftritt, sind laufzeitabhängig; das Verhalten selbst hat jedoch keine nachteiligen Auswirkungen.

Lautet die Dateispezifikation beispielsweise `/home/amr/ice.doc /home/amr/fire.doc`, könnten `/home` und `/home/amr` zweimal archiviert werden. Die Dateiobjekte `ice.doc` und `fire.doc` werden nur einmal archiviert.

Wenn Sie verhindern wollen, dass das gemeinsame übergeordnete Verzeichnis mehrmals angegeben wird, verwenden Sie separate, nicht überlappende **archive**-Befehle, um jede Dateispezifikation zu archivieren.

Wenn Sie ein Dateisystem archivieren, geben Sie einen abschließenden Schrägstrich an (`/home/`).

Es gilt eine Begrenzung auf 20 Operanden. Diese Begrenzung verhindert, dass sehr viele Sitzungen geöffnet werden, wenn die Platzhalterzeichen vom Befehlsprozessor der UNIX-Shell erweitert werden. Sie können verhindern, dass aufgrund der Shellerweiterung der Grenzwert von 20 Operanden überschritten wird, indem Sie am Anfang und am Ende der Dateispezifikationen, die Platzhalterzeichen enthalten ("`home/docs/*`"), Anführungszeichen eingeben.

Sie können mit der Option **removeoperandlimit** angeben, dass die Beschränkung auf 20 Operanden entfernt wird. Wenn Sie die Option **removeoperandlimit** angeben, wird die Beschränkung auf 20 Operanden nicht umgesetzt und nur durch die verfügbaren Ressourcen oder andere Begrenzungen des Betriebssystems eingeschränkt. Entfernen Sie beispielsweise die Begrenzung auf 20 Operanden, um 21 Dateispezifikationen zu archivieren:

```
selective -removeoperandlimit filespec1 filespec2 ... filespec21
```

Sie können die Option **filelist** anstelle von Dateispezifikationen verwenden, um anzugeben, welche Dateien bei dieser Operation berücksichtigt werden sollen. Diese beiden Methoden schließen sich jedoch gegenseitig aus. Sie können nicht sowohl Dateispezifikationsparameter angeben als auch die Option **filelist** verwenden. Wenn die Option **filelist** angegeben wird, werden alle angegebenen Dateispezifikationen ignoriert.

Tabelle 82. Befehl Archive: Zugehörige Optionen

Option	Verwendung
archmc	Nur in der Befehlszeile.
archsmlinkasfile	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
autofsrename	Nur Clientoptionsdatei (dsm.opt).
changingretries	Clientsystemoptionsdatei oder Befehlszeile.
compressalways	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
compression	Datei dsm.sys innerhalb einer Serverzeilengruppe oder Befehlszeile.
deletefiles	Nur in der Befehlszeile.
description	Nur in der Befehlszeile.
dironly	Nur in der Befehlszeile.
encryptiontype	Datei dsm.sys innerhalb einer Serverzeilengruppe.
encryptkey	Datei dsm.sys innerhalb einer Serverzeilengruppe.
filelist	Nur in der Befehlszeile.
filesonly	Nur in der Befehlszeile.
preservelastaccessdate	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
removeoperandlimit	Nur in der Befehlszeile.
snapshotcachesize	Clientoptionsdatei (dsm.opt) oder Option include.fs.
snapshotroot	Nur in der Befehlszeile.
subdir	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
tapeprompt	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
v2archive	Nur in der Befehlszeile.

Beispiele

Task Eine einzelne Datei mit dem Namen budget im Verzeichnis /home/proj1 archivieren.

Befehl: archive /home/proj1/budget

Task Alle Dateien im Verzeichnis /home/proj1 mit der Dateierweiterung .txt archivieren.

Befehl: archive "/home/proj1/*.txt"

Task Alle Dateien in der Verzeichnisbaumstruktur unter dem Verzeichnis /home archivieren.

Befehl: archive -subdir=yes "/home/*"

Task Angenommen, Sie haben eine Momentaufnahme des Dateisystems /usr gestartet und die Momentaufnahme als /snapshot/day1 angehängt. Archivieren Sie die Verzeichnisbaumstruktur /usr/dir1/sub1 aus der lokalen Momentaufnahme und verwalten Sie sie auf dem IBM Spectrum Protect-Server unter dem Dateibereichsnamen /usr.

Befehl: dsmc archive /usr/dir1/sub1/ -subdir=yes -snapshotroot=/snapshot/day1

Zugehörige Konzepte:

„Dateisystem- und ACL-Unterstützung“ auf Seite 174

Archive FastBack

Mit dem Befehl **archive fastback** können Sie Tivoli Storage Manager FastBack-Datenträger, die durch die Optionen `fbpolicyname`, `fbclientname` und `fbvolumename` angegeben sind, für die langfristige Aufbewahrung archivieren.

Bevor Sie diesen Befehl verwenden, müssen Sie den Client für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Daten konfigurieren. Wenn Sie diesen Befehl ausgeben, sollte zudem mindestens eine Momentaufnahme im FastBack-Repository für die FastBack-Maßnahme vorhanden sein, die archiviert oder gesichert wird.

Wenn eine Maßnahmenspezifikation sowohl Windows als auch Linux FastBack-Clients enthält, werden nur die Linux-Datenträger vom Linux-Client für Sichern/Archivieren auf dem IBM Spectrum Protect-Server gesichert oder archiviert.

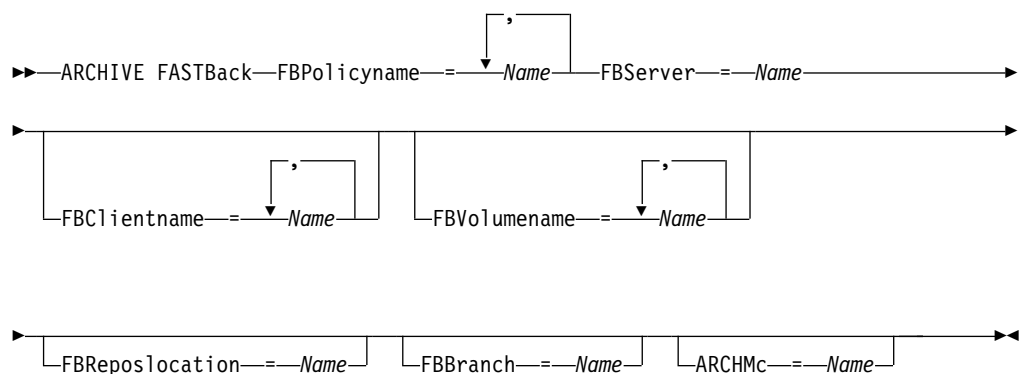
Sie können Tivoli Storage Manager FastBack-Optionen verwenden, um die neuesten Momentaufnahmen der folgenden Datenträger zu archivieren:

- Alle Clients und Datenträger, die einer bestimmten FastBack-Maßnahme oder einer Liste von FastBack-Maßnahmen zugeordnet sind.
- Alle Datenträger, die einem bestimmten FastBack-Client oder einer Liste von FastBack-Clients für eine angegebene FastBack-Maßnahme zugeordnet sind.
- Ein bestimmter Datenträger oder Datenträger, die einem bestimmten FastBack-Client für eine angegebene FastBack-Maßnahme zugeordnet sind.

Unterstützte Clients

Diese Option ist für Linux x86_64-Clients gültig.

Syntax



Wichtig:

1. Mindestens ein Wert für FBpolicyName ist immer erforderlich.
2. Sie können bis zu 10 Werte für FBPolicyName angeben, wenn weder für FBClientName noch für FBVolumeName Werte angegeben sind.

3. Wenn Sie einen Wert für FBClientName angeben, darf nur ein Wert für FBPolicyName vorhanden sein.
4. Sie können bis zu 10 Werte für FBClientName angeben, wenn nur ein Wert für PolicyName angegeben ist und keine Werte für FBVolumeName angegeben sind.
5. Wenn Sie die Option FBVolumeName angeben, kann nur ein Wert für FBPolicy und nur ein Wert für FBClientName angegeben werden.
6. Sie können mehrere Werte für FBVolumeName angeben, wenn Bedingung 5 erfüllt ist.
7. Sie müssen immer die Option FBReposLocation für Linux angeben.

Parameter

Tabelle 83. Befehl Archive FastBack: Zugehörige Optionen

Option	Verwendung
fbpolicyname „Fbpolicyname“ auf Seite 448	Befehlszeile und Scheduler.
fbserver „Fbserver“ auf Seite 451	Befehlszeile und Scheduler.
fbclientname „Fbclientname“ auf Seite 447	Befehlszeile und Scheduler.
fbvolumename „Fbvolumename“ auf Seite 452	Befehlszeile und Scheduler.
fbreposlocation „Fbreposlocation“ auf Seite 449	Befehlszeile und Scheduler.
fbbranch „Fbbranch“ auf Seite 446	Befehlszeile und Scheduler.
archmc „Archmc“ auf Seite 357	Befehlszeile und Scheduler.

Beispiele

Befehlszeile:

Der Client für Sichern/Archivieren ist auf einer Linux-Proxy-Client-Maschine installiert. Verwenden Sie diesen Befehl, um alle FastBack-Datenträger für alle Linux FastBack-Clients zu archivieren, die für die FastBack-Maßnahme Policy1 definiert sind:

```
dsmc archive fastback -fbpolicyname=Policy1
-fbserver=myfbserver -fbreposlocation=myfbserver@WORKGROUP
```

Der FastBack-Servername -myFbDrHub ist der kurze Hostname des FastBack Disaster Recovery Hub-Servers, auf dem sich das Repository befindet.

Der Parameter -fbreposlocation gibt die Position des Repositorys an. Die Repository-Position ist erforderlich. Wenn Sie die Repository-Position nicht angeben, schlägt der Befehl fehl.

FBServer sollte in diesem Fall auf den kurzen Hostnamen des FastBack DR Hub verweisen.

Befehlszeile:

Das Repository rep_server1 befindet sich auf dem FastBack DR Hub myFbDrHub.

```
dsmc archive fastback -fbpolicyname="Policy 1"
-fbserver=myFbDrHub -fbreposlocation=\\myFbDrHub\rep_server1
```

Die Repository-Position ist erforderlich. Wenn Sie die Repository-Position nicht angeben, schlägt der Befehl fehl.

Der FastBack-Servername -myFbDrHub ist der kurze Hostname des FastBack Disaster Recovery Hub, auf dem sich das Repository befindet.

FBServer sollte in diesem Fall auf den kurzen Hostnamen des FastBack DR Hub verweisen.

Befehlszeile:

Alle Datenträger, die durch die FastBack-Maßnahme mit dem Namen policy1 geschützt sind, für den FastBack-Server mit dem Namen basil archivieren:

```
dsmc archive fastback -Fbpolicyname=policy1
-FBServer=basil -ARCHMC="my_tsm_mgmt_class"
-fbreposlocation=basil@WORKGROUP
```

Zugehörige Konzepte:

„Client für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Daten konfigurieren“ auf Seite 106

Backup FastBack

Mit dem Befehl **backup fastback** können Sie Tivoli Storage Manager FastBack-Datenträger sichern, die durch die Optionen fbpolicyname, fbclientname und fbvolumename für die langfristige Aufbewahrung angegeben sind.

Bevor Sie diesen Befehl verwenden, müssen Sie den Client für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Daten konfigurieren. Wenn Sie diesen Befehl ausgeben, sollte zudem mindestens eine Momentaufnahme im Tivoli Storage Manager FastBack-Repository für die Tivoli Storage Manager FastBack-Maßnahme vorhanden sein, die archiviert oder gesichert wird.

Wenn eine Maßnahmenspezifikation sowohl Windows als auch Linux FastBack-Clients enthält, werden nur die Linux-Datenträger vom Linux-Client für Sichern/Archivieren auf dem IBM Spectrum Protect-Server gesichert oder archiviert.

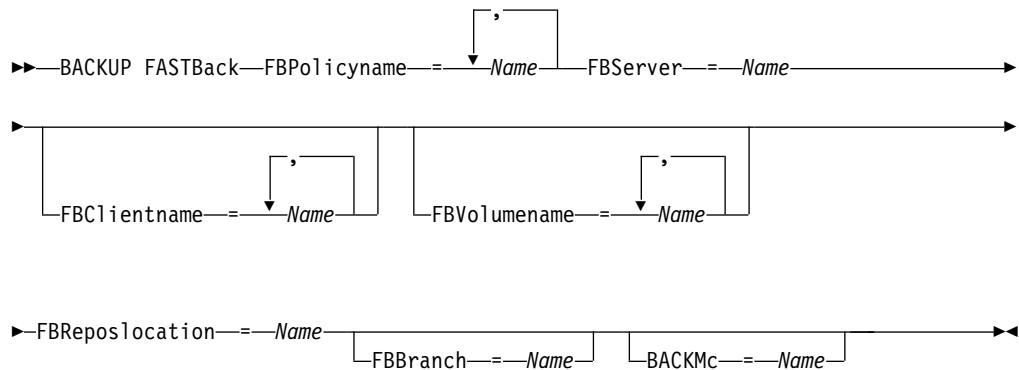
Tivoli Storage Manager FastBack-Optionen werden je nach der angegebenen Option für die Teilsicherung der neuesten Momentaufnahmen unterstützt:

- Alle Clients und Datenträger, die der FastBack-Maßnahme oder einer Liste von FastBack-Maßnahmen zugeordnet sind.
- Alle Datenträger, die einem bestimmten FastBack-Client oder einer Liste von FastBack-Clients für eine angegebene FastBack-Maßnahme zugeordnet sind.
- Ein bestimmter Datenträger oder Datenträger, die einem bestimmten FastBack-Client für eine angegebene FastBack-Maßnahme zugeordnet sind.

Unterstützte Clients

Dieser Befehl ist für Linux x86_64-Clients gültig, die als dedizierte Tivoli Storage Manager FastBack-Proxys konfiguriert sind.

Syntax



Wichtig:

1. Mindestens ein Wert für FBpolicyName ist immer erforderlich.
2. Sie können bis zu 10 Werte für FBPolicyName angeben, wenn weder für FBClientName noch für FBVolumeName Werte angegeben sind.
3. Wenn Sie einen Wert für FBClientName angeben, darf nur ein Wert für FBPolicyName vorhanden sein.
4. Sie können bis zu 10 Werte für FBClientName angeben, wenn nur ein Wert für PolicyName angegeben ist und keine Werte für FBVolumeName angegeben sind.
5. Wenn Sie die Option FBVolumeName angeben, kann nur ein Wert für FBPolicy und nur ein Wert für FBClientName angegeben werden.
6. Sie können mehrere Werte für FBVolumeName angeben, wenn Bedingung 5 erfüllt ist.
7. Sie müssen die Option FBReposLocation angeben.

Tabelle 84. Befehl Backup FastBack: Zugehörige Optionen

Option	Verwendung
fbpolicyname „Fbpolicyname“ auf Seite 448	Befehlszeile und Scheduler.
fbserver „Fbserver“ auf Seite 451	Befehlszeile und Scheduler.
fbclientname „Fbclientname“ auf Seite 447	Befehlszeile und Scheduler.
fbvolumename „Fbvolumename“ auf Seite 452	Befehlszeile und Scheduler.
fbreposlocation „Fbreposlocation“ auf Seite 449	Befehlszeile und Scheduler.
fbbranch „Fbbranch“ auf Seite 446	Befehlszeile und Scheduler.
backmc „Backmc“ auf Seite 369	Befehlszeile und Scheduler.

Beispiele

Befehlszeile:

Der Client für Sichern/Archivieren ist auf einer Linux-Proxy-Client-Maschine installiert. Verwenden Sie diesen Befehl, um alle FastBack-Datenträger für alle Linux FastBack-Clients zu sichern, die für die FastBack-Maßnahme Policy1 definiert sind:

```
dsmc backup fastback -fbpolicyname=Policy1  
-fbserver=myfbserver  
-fbreposlocation=myfbserver@WORKGROUP
```

Die Repository-Position ist erforderlich. Wenn Sie die Repository-Position nicht angeben, schlägt der Befehl fehl.

Der FastBack-Servername -myfbserver ist der kurze Hostname des FastBack-Servers, auf dem sich das Repository befindet.

Befehlszeile:

Das Repository rep_server1 befindet sich auf dem FastBack Disaster Recovery Hub myFbDrHub.

```
dsmc backup fastback -fbpolicyname="Policy 1"  
-fbserver=myFbDrHub -fbreposlocation=\\myFbDrHub\rep_server1
```

Der FastBack-Servername -myFbDrHub ist der kurze Hostname des FastBack Disaster Recovery Hub-Servers, auf dem sich das Repository befindet.

Die Option -fbreposlocation gibt die Position des Repositories an. Die Repository-Position ist erforderlich. Wenn Sie die Repository-Position nicht angeben, schlägt der Befehl fehl.

Die Option FBServer sollte in diesem Fall auf den kurzen Hostnamen des FastBack DR Hub verweisen.

Befehlszeile:

Alle Datenträger, die durch die FastBack-Maßnahme mit dem Namen policy1 geschützt sind, für den FastBack-Server mit dem Namen basil sichern:

```
dsmc backup fastback -Fbpolicyname=policy1  
-FBServer=basil -BACKMC="my_tsm_mgmt_class"  
-fbreposlocation=basil@WORKGROUP
```

Zugehörige Konzepte:

„Client für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Daten konfigurieren“ auf Seite 106

Backup Group

Verwenden Sie den Befehl **backup group**, um eine Gruppe, die eine Liste von Dateien aus einem oder mehreren Dateibereichsursprüngen enthält, zu erstellen und in einem virtuellen Dateibereich auf dem IBM Spectrum Protect-Server zu sichern.

Nur für AIX: Mit Hilfe der Option `snapshotproviderfs=JFS2` können Sie die Gruppensicherung auf Momentaufnahmebasis aktivieren.

Über eine Gruppensicherung können Sie eine konsistente zeitpunktgesteuerte Sicherung für eine Gruppe von Dateien erstellen, die gemeinsam als logische Einheit verwaltet werden. Für die Objekte in der Gruppe gelten die folgenden Verarbeitungsregeln:

- Erneutes Binden der Verwaltungsklasse für gruppierte Objekte:

- Während Gesamtsicherungen wird allen Objekten in einer Sicherungsgruppe dieselbe Verwaltungsklasse zugeordnet.
- Während Differenzsicherungen tritt folgendes Verhalten auf, wenn eine neue Verwaltungsklasse in einer Anweisung include für eine vorhandene Sicherungsgruppe angegeben wird:
 - Alle neuen und geänderten Objekte in der Sicherungsgruppe werden an die neue Verwaltungsklasse gebunden.
 - Alle Mitgliedsobjekte der Gruppe, die nicht geändert werden, erscheinen so, als ob sie nicht an die neue Verwaltungsklasse gebunden wären. Diese unveränderten Objekte sind nicht in den Statistikdaten **Gesamtzahl erneut gebundener Objekte** enthalten, die nach Beendigung des Befehls **Backup Group** angezeigt werden.
 - Die unveränderten Objekte werden einer neu erstellten Sicherungsgruppe neu zugeordnet und die neue Sicherungsgruppe wird an die neue Verwaltungsklasse gebunden. Für die unveränderten Gruppenobjekte wird jedoch weiterhin der Name der ursprünglichen Verwaltungsklasse angezeigt.

Auch wenn für die unveränderten Objekte weiterhin der Name der ursprünglichen Verwaltungsklasse angezeigt wird, sind sie tatsächlich an die neue Verwaltungsklasse der Sicherungsgruppe gebunden.
- Vorhandene Anweisungen exclude für Dateien in der Gruppe werden ignoriert.
- Alle Objekte in der Gruppe werden gemeinsam exportiert.
- Alle Objekte in der Gruppe verfallen gemeinsam wie in der Verwaltungsklasse angegeben. Keine Objekte in der Gruppe verfallen, bevor nicht alle anderen Objekte in der Gruppe verfallen, selbst wenn eine andere Gruppe, zu denen diese Objekte gehören, verfällt.
- Werden vollständige und differenzielle Gruppensicherungen auf eine sequenzielle Einheit ausgeführt, sind die Daten bei der Zurückschreibung an nur zwei Positionen vorhanden. Führen Sie zum Optimieren der Zurückschreibungszeit regelmäßige Gesamtsicherungen aus, um die Daten an eine Position auf dem sequenziellen Datenträger zu sichern.
- Bei einer vollständigen Gruppensicherung werden alle Objekte in der Dateiliste an den Server gesendet. Bei einer differenziellen Gruppensicherung werden nur die Daten, die seit der letzten Gesamtsicherung geändert wurden, an den Server gesendet. Die Objekte in der Dateiliste, die sich seit den letzten Gesamtsicherungen nicht geändert haben, werden als Member der differenziellen Gruppensicherung zugeordnet. Ihre Daten werden jedoch nicht an den Server gesendet, so dass sich die Sicherungszeit verkürzt.

Für den Befehl **backup group** sind die folgenden Optionen erforderlich:

filelist

Gibt eine Liste von Dateien an, die einer neuen Gruppe hinzugefügt werden sollen.

groupname

Gibt den vollständig qualifizierten Namen der Gruppe an, die eine Liste von Dateien enthält.

virtualfsname

Gibt den Namen des virtuellen Dateibereichs für die Gruppe an, mit der die Operation ausgeführt werden soll. Die Option virtualfsname darf nicht mit einem vorhandenen Dateibereichsnamen übereinstimmen.

mode

Gibt an, ob alle Dateien in der Dateiliste gesichert werden oder nur die Dateien, die sich seit der letzten Gesamtsicherung geändert haben.

Anmerkung:

1. Wenn eine Datei in der Gruppensicherung fehlschlägt, schlägt die gesamte Gruppensicherung fehl.
2. Verwenden Sie den Befehl **query group**, um Member einer Gruppensicherung auf dem IBM Spectrum Protect-Server abzufragen.
3. Verwenden Sie den Befehl **restore group**, um bestimmte Member oder alle Member einer Gruppensicherung auf dem Server zurückzuschreiben.
4. Sofern Sie nicht unter Mac OS X arbeiten, verwenden Sie den Befehl **delete group**, um eine bestimmte Gruppensicherung vom Server zu löschen.
5. Verwenden Sie den Befehl **query filesystem**, um Namen der virtuellen Dateibereiche für Ihren Knoten anzuzeigen, die auf dem Server gespeichert sind.
6. Eine Gruppensicherung kann zu einem Sicherungssatz hinzugefügt werden.

Unterstützte Clients

Dieser Befehl ist für alle UNIX- und Linux-Clients mit Ausnahme von Mac OS X gültig.

Syntax

►► Backup Group — *Optionen* —►►

Parameter

Tabelle 85. Befehl Backup Group: Zugehörige Optionen

Option	Verwendung
filelist „Filelist“ auf Seite 453	Nur in der Befehlszeile.
groupname „Groupname“ auf Seite 464	Nur in der Befehlszeile.
mode „Mode“ auf Seite 509	Nur in der Befehlszeile.
snapshotproviderfs „Snapshotproviderfs“ auf Seite 591	Systemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe oder mit der Option include.fs.
virtualfsname „Virtualfsname“ auf Seite 630	Nur in der Befehlszeile.

Beispiele

Task Eine Gesamtsicherung aller in der Datei /home/dir1/filelist1 angegebenen Dateien auf den virtuellen Dateibereich mit dem Namen accounting und mit der Hauptmemberdatei /home/group1 ausführen.

Befehl:

```
backup group -filelist=/home/dir1/filelist1 -groupname=group1  
-virtualfsname=/virtfs -mode=full
```

Zugehörige Informationen

„Include-Optionen“ auf Seite 473

„Query Group“ auf Seite 756

„Restore Group“ auf Seite 784

„Delete Group“ auf Seite 728

„Query Filespace“ auf Seite 754

Backup Image

Mit dem Befehl **backup image** wird eine Imagesicherung eines oder mehrerer Datenträger auf Ihrem System erstellt.

Mit dem Befehl **backup image** können Sie NTFS-, ReFS- oder unformatierte (RAW) Datenträger sichern. Wenn ein Datenträger mit NTFS formatiert ist, werden nur die vom Dateisystem verwendeten Blöcke gesichert. Bei ReFS-Datenträgern werden alle Blöcke gesichert.

Wenn Sie die Option **imagegapsize** auf 0 setzen, werden alle Blöcke einschließlich der unbenutzten Blöcke am Ende des Datenträgers gesichert.

Wenn Sie ein AIX JFS2-Dateisystem für die Imagesicherung angeben, werden nur die vom Dateisystem verwendeten Blöcke gesichert. Wenn Sie die Option **imagegapsize** auf null setzen, werden alle Blöcke einschließlich der unbenutzten Blöcke am Ende des Datenträgers gesichert.

Anmerkung:

1. Nur für AIX: Standardmäßig ist die Imagesicherung auf Momentaufnahmebasis für JFS2-Datenträger aktiviert. Geben Sie `-snapshotproviderimage=NONE` in diesem Befehl an, um momentaufnahmebasierte Imagesicherungen zu inaktivieren.
2. Für die Linux-Clients wird die Imagesicherung nur auf Partitionen mit der ID 0x83 oder auf logischen Datenträgern unterstützt, die mit dem Linux Logical Volume Manager erstellt wurden. Beim Sichern anderer Partitionen, wie z. B. bei erweiterten Partitionen, die angehängte Dateisysteme oder Datenbankdaten enthalten, kann es zu inkonsistenten Sicherungsdaten kommen, wenn sich die Daten während der Imagesicherungsoperation ändern.
3. Für den Linux-Client wird die Imagesicherung von DASD-Einheiten mit dem Modus 'raw_track_access' unter Linux on z Systems nicht unterstützt.
4. Der Befehl 'backup image' wird nicht auf GPFS-Dateisystemen unterstützt.
5. Die IBM Spectrum Protect-API muss installiert sein, um den Befehl **backup image** verwenden zu können.
6. Wenn Sie das Attribut eines JFS2-Dateisystems in ein von HSM verwaltetes Dateisystem ändern, wird keine Imagesicherung für dieses Dateisystem ausgeführt.
7. Die Imagesicherungsoperation wird auf Partitionen, die sich auf einer Multi-path-Einheit befinden, nicht unterstützt.

Wichtig: Der Zeitpunkt der letzten Teilsicherung bezieht sich auf die Serverzeit und der Zeitpunkt der letzten Dateiänderung auf die Clientzeit. Sind die Clientzeit und die Serverzeit nicht synchronisiert oder befinden der Client und der Server sich in verschiedenen Zeitzonen, wirkt sich dies auf die Teilsicherung nach Datum und die Imagesicherung mit `mode=incremental` aus.

Der Client sichert die Dateien, deren Änderungsdatum und -zeit (Clientzeit) nach dem Datum und der Zeit der letzten Teilsicherung des Dateisystems liegen, auf dem die Dateien gespeichert werden (Serverzeit).

Liegt die Serverzeit vor der Clientzeit, überspringen Teilsicherungen nach Datum oder Imagesicherungen mit `mode=incremental` die Dateien, die nach der letzten Teilsicherung oder Imagesicherung mit einem Änderungsdatum vor der Zeitmarke der letzten Teilsicherung erstellt oder geändert wurden.

Ist die Clientzeit der Serverzeit voraus, werden alle Dateien erneut gesichert, die vor der letzten Teil- oder Imagesicherung erstellt oder geändert wurden und deren Änderungszeit nach dem Zeitpunkt liegt, den die Zeitmarke der letzten Teilsicherung angibt. Normalerweise würden diese Dateien nicht gesichert, da sie bereits gesichert wurden.

Das Sicherungsdatum kann mit dem Befehl **query filesystem** überprüft werden.

Der Client für Sichern/Archivieren muss den Einheitentyp "unformatierte Einheit" auf der jeweiligen Plattform unterstützen, um eine Imagesicherung einer unformatierten Einheit ausführen zu können. Sie können eine Imagesicherung nur auf lokalen Einheiten ausführen. Gruppeneinheiten oder -dateisysteme sowie Einheiten oder Dateisysteme, die von mindestens zwei Systemen gemeinsam benutzt werden, werden nicht unterstützt. Wenn Sie eine Imagesicherung für ein Dateisystem ausführen wollen, das an eine unformatierte Einheit angehängt ist, muss die unformatierte Einheit unterstützt werden.

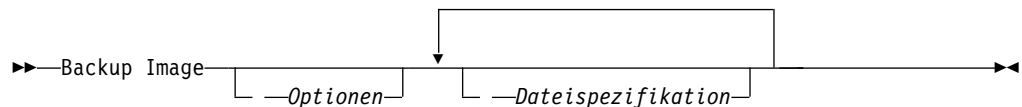
Verwenden Sie die Option **include.image**, um ein Dateisystem oder einen logischen Datenträger für die Imagesicherung einzubeziehen oder um datenträgerspezifische Optionen für die Imagesicherung anzugeben.

Der Befehl **backup image** verwendet die Option **compression**.

Unterstützte Clients

Diese Option ist für AIX-, Linux- und Oracle Solaris-Clients gültig.

Syntax



Parameter

Dateispezifikation

Gibt den Namen eines oder mehrerer logischer Datenträger an. Wenn Sie mehrere Dateisysteme sichern wollen, müssen Sie ihre Namen mit Leerzeichen voneinander trennen. Verwenden Sie keine Mustererkennungszeichen. Wenn Sie keinen Datenträgernamen angeben, werden die mit der Option **domain.image** angegebenen logischen Datenträger verarbeitet. Wenn Sie die Option **domain.image** nicht verwenden, um Dateisysteme für die Verarbeitung anzugeben, wird eine Fehlermeldung angezeigt, und es erfolgt keine Imagesicherung.

Den Dateibereich, über den der logische Datenträger angehängt ist, oder den Namen des logischen Datenträgers angeben. Ist im System ein Dateisystem für einen bestimmten Datenträger konfiguriert, können Sie den Datenträger nicht mit dem Einheitenamen sichern.

Beispiel: Ist der Dateibereich /dev/lv01 auf dem Datenträger /home angehängt, können Sie `backup image /home` ausgeben; `backup image /dev/lv01` schlägt jedoch mit folgendem Fehler fehl:

ANS1063E Ungültiger Pfad angegeben

Es gilt eine Begrenzung auf 20 Operanden. Diese Begrenzung verhindert, dass sehr viele Sitzungen geöffnet werden, wenn die Platzhalterzeichen vom Befehlsprozessor der UNIX-Shell erweitert werden. Sie können verhindern, dass aufgrund der Shellerweiterung der Grenzwert von 20 Operanden überschritten wird, indem Sie am Anfang und am Ende der Dateispezifikationen, die Platzhalterzeichen enthalten ("home/docs/*"), Anführungszeichen eingeben.

Sie können mit der Option `removeoperandlimit` angeben, dass die Beschränkung auf 20 Operanden entfernt wird. Wenn Sie die Option `removeoperandlimit` angeben, wird die Beschränkung auf 20 Operanden nicht umgesetzt und nur durch die verfügbaren Ressourcen oder andere Begrenzungen des Betriebssystems eingeschränkt. Entfernen Sie beispielsweise die Begrenzung auf 20 Operanden, um 21 Dateispezifikationen zu sichern:

```
backup image -removeoperandlimit filespec1 filespec2 ... filespec21
```

Anmerkung: Für Sun-Systeme geben Sie entweder einen Dateisystemnamen oder den Namen einer unformatierten Einheit (des Typs Blockeinheit) an.

Tabelle 86. Befehl `Backup Image`: Zugehörige Optionen

Option	Verwendung
asnodename „Asnodename“ auf Seite 359	Clientsystemoptionsdatei (dsm.sys) oder Befehlszeile.
compressalways „Compressalways“ auf Seite 379	Clientsystemoptionsdatei (dsm.sys) oder Befehlszeile.
compression „Compression“ auf Seite 380	Clientoptionsdatei oder Befehlszeile.
dynamicimage „Dynamicimage“ auf Seite 423	Mit dem Befehl <code>backup image</code> oder der Option <code>include.image</code> in der Optionsdatei.
imagegapsize „Imagegapsize“ auf Seite 469	Mit dem Befehl <code>backup image</code> , mit der Option <code>include.image</code> oder in der Optionsdatei.
mode „Mode“ auf Seite 509	Nur in der Befehlszeile.
postsnapshotcmd „Postsnapshotcmd“ auf Seite 533	Mit dem Befehl <code>backup image</code> , mit der Option <code>include.image</code> oder in der Optionsdatei.
presnapshotcmd „Presnapshotcmd“ auf Seite 540	Mit dem Befehl <code>backup image</code> , mit der Option <code>include.image</code> oder in der Optionsdatei.
removeoperandlimit	Nur in der Befehlszeile.
snapshotcachesize „Snapshotcachesize“ auf Seite 590	Mit dem Befehl <code>backup image</code> , mit der Option <code>include.image</code> oder in der Optionsdatei.

Tabelle 86. Befehl Backup Image: Zugehörige Optionen (Forts.)

Option	Verwendung
snapshotproviderimage „Snapshotproviderimage“ auf Seite 592	Clientoptionsdatei oder mit der Option include.image .

Beispiele

Task Den Dateibereich /home/test, über den der logische Datenträger angehängt ist, sichern und eine Imageteilsicherung ausführen, bei der nur neue und geänderte Dateien nach der letzten vollständigen Imagesicherung gesichert werden.

```
dsmc backup image /home/test -mode=incremental
```

Task Eine statische Imagesicherung des logischen Datenträgers ausführen, der im Verzeichnis /home angehängt ist.

```
dsmc backup image /home -snapshotproviderimage=none
```

Task Eine dynamische Imagesicherung des logischen Datenträgers ausführen, der im Verzeichnis /home angehängt ist.

Befehl: dsmc backup image /home -dynamicimage=yes

Task Eine Momentaufnahmeimagesicherung des Verzeichnisses /home ausführen.

```
AIX-Client: dsmc backup image /home
             -snapshotproviderimage=JFS2
Linux-Client: dsmc backup image /home
              -snapshotproviderimage=LINUX_LVM
```

Task Den unformatierten logischen Datenträger /dev/lv01 sichern.

```
dsmc backup image /dev/lv01
```

Zugehörige Informationen

„Imagegapsize“ auf Seite 469

„Snapshotproviderimage“ auf Seite 592

„Snapshotcachesize“ auf Seite 590

„Mode“ auf Seite 509

„Vergleich der Methoden 1 und 2“ auf Seite 212 Hilft Ihnen bei der Entscheidung, welche Methode für Ihre Umgebung geeignet ist.

Statische, dynamische und Momentaufnahmeimagesicherung

Die traditionelle Imagesicherung verhindert während der Operation den Schreibzugriff auf den Datenträger durch andere Systemanwendungen.

Verwenden Sie die Option **dynamicimage**, um den Datenträger im aktuellen Status ohne erneutes Anhängen mit Lesezugriff zu sichern. Die Sicherung kann beschädigt werden, wenn Anwendungen auf den Datenträger schreiben, während die Sicherung ausgeführt wird. Führen Sie in diesem Fall **fsck** nach einer Zurückschreibung aus.

Die Option `dynamicimage` wird für JFS2-Datenträger nicht unterstützt.

Nur für Linux x86_64-Clients: Standardmäßig führt der Client für Sichern/Archivieren eine Momentaufnahmeimagesicherung von Dateisystemen auf einem logischen Datenträger aus, der von Linux Logical Volume Manager erstellt wurde, während der der Datenträger für andere Systemanwendungen verfügbar ist. Die Momentaufnahmeimagesicherung erfordert einen IBM Spectrum Protect-Server der Version 5.1.

Nur für AIX-Clients: Standardmäßig führt der Client für Sichern/Archivieren eine Momentaufnahmeimagesicherung von JFS2-Datenträgern aus, während der der Datenträger für andere Systemanwendungen verfügbar ist. AIX gestattet die Erstellung einer Momentaufnahme eines JFS2-Datenträgers, während er noch online ist. Die Momentaufnahme wird innerhalb derselben Datenträgergruppe wie der Quelldatenträger erstellt. Sie müssen sicherstellen, dass die Datenträgergruppe über genügend freien Plattenspeicherplatz für die Erstellung der Momentaufnahme verfügt. Die Momentaufnahme enthält die alten Datenblöcke; die geänderten Daten werden im Quelldatenträger gespeichert. Geben Sie mit der Option `snapshotcachesize` im Befehl `backup image`, in der Datei `dsm.sys` oder in Verbindung mit der Option `include.image` eine geeignete Momentaufnahmengröße an, sodass während der Imagesicherung alle alten Datenblöcke gespeichert werden können.

Der Linux Logical Volume Manager gestattet die Erstellung einer Momentaufnahme eines logischen Datenträgers, während der logische Datenträger selbst noch online ist. Die Momentaufnahme wird innerhalb derselben Datenträgergruppe wie der logische Quelldatenträger erstellt. Sie müssen sicherstellen, dass die Datenträgergruppe über genügend freien Plattenspeicherplatz für die Erstellung der Momentaufnahme verfügt. Die Momentaufnahme enthält die alten Datenblöcke; die geänderten Daten werden im logischen Quelldatenträger gespeichert. Geben Sie mit der Option `snapshotcachesize` im Befehl **backup image**, in der Datei `dsm.sys` oder in Verbindung mit der Option `include.image` eine geeignete Momentaufnahmengröße an, sodass während der Imagesicherung alle alten Datenblöcke gespeichert werden können. Eine Momentaufnahmengröße von 100 Prozent gewährleistet eine gültige Momentaufnahme.

Verwendung der Imagesicherung für die Dateisystemteilsicherung

Es gibt zwei Methoden, um durch die Verwendung von Imagesicherungen effiziente Teilsicherungen Ihrer Dateisysteme auszuführen. Mit Hilfe dieser Sicherungsmethoden können Sie eine zeitpunktgesteuerte Zurückschreibung für Ihre Dateisysteme ausführen und den Durchsatz beim Sichern und Zurückschreiben verbessern.

Sie können die Sicherung nur auf formatierten Datenträgern und nicht auf unformatierten logischen Datenträgern ausführen. Sie können entweder *Imagesicherung mit Dateisystemteilsicherung* oder *Imagesicherung mit dem Imageteilsicherungsmodus* verwenden, um Imagesicherungen für Datenträger mit angehängten Dateisystemen auszuführen.

Es folgen einige Beispiele für die Verwendung der *Imagesicherung mit Dateisystemteilsicherung*.

- Eine vollständige Teilsicherung des Dateisystems ausführen: `dsmc incremental /myfilesystem`
- Eine Imagesicherung desselben Dateisystems ausführen: `dsmc backup image /myfilesystem`

- In regelmäßigen Abständen Teilsicherungen ausführen: `dsmc incremental /myfilesystem`

Sie müssen die nächsten Schritte in der angegebenen Reihenfolge ausführen, um sicherzustellen, dass der Server Hinzufüge- und Löschvorgänge genau aufzeichnet.

Verwenden Sie diesen Befehl, um das Dateisystem mit exakt dem Status der letzten Teilsicherung zurückzuschreiben: `dsmc restore image /myfilesystem -incremental -deletefiles`.

Während der Zurückschreibung führt der Client Folgendes durch:

- Er schreibt das neueste Image auf dem Server zurück.
- Er löscht alle im vorherigen Schritt zurückgeschriebenen Dateien, die auf dem Server inaktiv sind. Dies sind Dateien, die zum Zeitpunkt der Imagesicherung vorhanden waren, aber danach gelöscht und durch eine spätere Teilsicherung aufgezeichnet wurden.
- Er schreibt neue und geänderte Dateien aus den Teilsicherungen zurück.

Wenn Sie die Schritte nicht exakt einhalten, können zwei Dinge passieren:

1. Nach dem Zurückschreiben des ursprünglichen Images werden alle Dateien, die mit dem Befehl **incremental** gesichert wurden, einzeln zurückgeschrieben.
2. Wird ein Befehl **backup image** vor einem Befehl **incremental** ausgeführt, werden Dateien, die aus dem ursprünglichen Image gelöscht wurden, *nicht* aus dem endgültig zurückgeschriebenen Dateisystem gelöscht.

Es folgen einige Beispiele für die Verwendung der *Imagesicherung mit dem Imageteilsicherungsmodus*.

- Eine Imagesicherung desselben Dateisystems ausführen: `dsmc backup image /myfilesystem`
- Eine Imageteilsicherung des Dateisystems ausführen: `dsmc backup image /myfilesystem -mode=incremental`

Hierdurch werden nur die Dateien an den Server gesendet, die seit der letzten Imagesicherung hinzugefügt oder geändert wurden.

- In regelmäßigen Abständen vollständige Imagesicherungen ausführen: `dsmc backup image /myfilesystem`
- Das Image zurückschreiben: `dsmc restore image /myfilesystem -incremental`
Beim Zurückschreiben ignoriert der Client für Sichern/Archivieren die Option `deletefiles`, wenn die Sicherungstechnik Image + Imageteilsicherung verwendet wurde. Die Zurückschreibung schließt Dateien ein, die nach der letzten vollständigen Imagesicherung gelöscht wurden, sowie die aktuellsten Versionen von Dateien, die nach der letzten Imagesicherung hinzugefügt oder geändert wurden.

Anmerkung: In den folgenden Fällen sollten Sie regelmäßig vollständige Imagesicherungen ausführen. Dadurch wird die Zurückschreibungszeit verbessert, da weniger Änderungen von Teilsicherungen angewendet werden.

- Wenn sich ein Dateisystem beträchtlich ändert (mehr als 40%).
- Einmal pro Monat.
- Entsprechend den Anforderungen in Ihrer Umgebung.

Die folgenden Einschränkungen gelten, wenn Sie Imagesicherung mit dem Imageteilsicherungsmodus verwenden:

- Das Dateisystem darf keine früheren, durch den Befehl **incremental** generierten vollständigen Teilsicherungen aufweisen.

- Durch eine Teilsicherung nach Datum werden Dateien auf dem Server nicht inaktiviert. Daher können beim Zurückschreiben von Dateien keine gelöscht werden.
- Bei der ersten Imagesicherung des Dateisystems wird eine vollständige Imagesicherung ausgeführt.
- Bei Verwendung von *mode=incremental* werden nur Dateien mit einem geänderten Datum und keine Dateien mit geänderten Berechtigungen gesichert.
- Wenn die maximale Kapazität der Dateisysteme bereits oder fast erreicht ist, kann hierdurch eine Bedingung 'Zu wenig Speicherbereich' während der Zurückschreibung auftreten.

Backup NAS

Mit dem Befehl **backup nas** wird eine Imagesicherung eines oder mehrerer Dateisysteme erstellt, die zu einem NAS-Dateiserver (NAS = Network Attached Storage) gehören (wird auch als NDMP-Sicherung bezeichnet). Sie werden zur Eingabe der IBM Spectrum Protect-Administrator-ID aufgefordert.

Der NAS-Dateiserver führt die Gerätedatenversetzung aus. Ein Serverprozess wird gestartet, um die Sicherung auszuführen.

Verwenden Sie die Option *nasnodename*, um den Knotennamen für den NAS-Dateiserver anzugeben. Der NAS-Knotenname identifiziert den NAS-Dateiserver für den IBM Spectrum Protect-Server; der NAS-Knotenname muss beim Server registriert sein. Fügen Sie die Option *nasnodename* in Ihre Clientoptionsdatei (*dsm.opt*) ein. Der Wert in der Clientoptionsdatei ist der Standardwert; er kann jedoch in der Befehlszeile überschrieben werden.

Verwenden Sie die Option *toc* mit dem Befehl **backup nas** oder der Option *include.fs.nas*, um anzugeben, ob der IBM Spectrum Protect-Server für jede Dateisystemsicherung Inhaltsverzeichnisangaben (TOC) speichert. Wenn Sie TOC-Angaben speichern, können Sie den Serverbefehl **QUERY TOC** verwenden, um den Inhalt einer Dateisystemsicherung festzustellen, sowie den Serverbefehl **RESTORE NODE**, um einzelne Dateien oder Verzeichnisstrukturen zurückzuschreiben.

Sie können auch den IBM Spectrum Protect-Web-Client verwenden, um die gesamte Baumstruktur des Dateisystems zu untersuchen und zurückzuschreibende Dateien und Verzeichnisse auszuwählen. Die Erstellung eines Inhaltsverzeichnisses erfordert, dass Sie das Attribut **tocdestination** in der Sicherungskopiengruppe für die Verwaltungsklasse definieren, an die dieses Sicherungsimage gebunden wird. Die TOC-Erstellung erfordert während der Sicherungsoperation zusätzliche Verarbeitung, zusätzliche Netzressourcen, zusätzlichen Speicherpoolbereich und möglicherweise einen zusätzlichen Mountpunkt. Wenn Sie keine TOC-Angaben speichern, können Sie über den Befehl **RESTORE NODE** dennoch einzelne Dateien und Verzeichnisstrukturen zurückschreiben, wenn Sie den vollständig qualifizierten Namen jeder Datei bzw. jedes Verzeichnisses und das Image kennen, in dem das Objekt gesichert wurde.

Die Option *toc* wird nur für Images unterstützt, die mit Client und Server mit mindestens Version 5.2 gesichert wurden.

Wenn Sie *mode=differential* im Serverbefehl **BACKUP NODE** oder im Befehl **backup nas** angeben, ohne dass ein Gesamtimage vorhanden ist, wird angezeigt, dass eine Gesamtsicherung gestartet wurde. Die Verwendung des Serverbefehls **QUERY PROCESS** zeigt, dass eine Gesamtsicherung in Bearbeitung ist.

Mit der Option `mode` geben Sie an, ob eine vollständige oder eine differenzielle NAS-Imagesicherung ausgeführt werden soll. Bei einer vollständigen Imagesicherung wird das gesamte Dateisystem gesichert. Der Standardwert ist eine differenzielle NAS-Imagesicherung für Dateien, die sich nach der letzten vollständigen Imagesicherung ändern. Ist keine auswählbare vollständige Imagesicherung vorhanden, erfolgt eine vollständige Imagesicherung. Ist ein Gesamtimage vorhanden, wird bei Angabe von `mode =differential` eine differenzielle Imagesicherung gesendet, unabhängig davon, ob das Image zurückgeschrieben werden kann oder verfallen ist und nur wegen abhängiger differenzieller Images aufbewahrt wird. Wird ein Gesamtimage während einer differenziellen Sicherung gesendet, wird es mit Hilfe des Serverbefehls **QUERY NASBACKUP** als Gesamtimage angezeigt. Auch der Serverbefehl **QUERY NASBACKUP** zeigt zurückschreibbare NAS-Images an und "Gesamtimage" oder "differenzielles Image" als Objekttyp.

Mit der Option `monitor` geben Sie an, ob Sie eine NAS-Imagesicherung eines Dateisystems überwachen und Verarbeitungsinformationen anzeigen wollen.

Mit dem Befehl **monitor process** können Sie eine Liste aller Prozesse anzeigen, für die eine Verwaltungsbenutzer-ID über eine Berechtigung verfügt. Die Verwaltungsbenutzer-ID sollte mindestens die Clienteignerberechtigung sowohl über den NAS-Knoten als auch den Client-Workstation-Knoten besitzen, der entweder von der Befehlszeile oder vom Web aus verwendet wird.

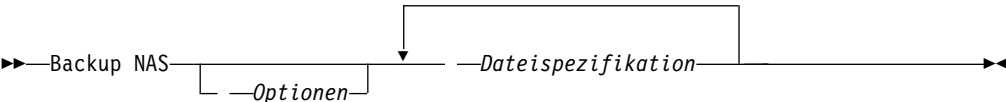
Mit dem Befehl **cancel process** können Sie die NAS-Sicherungsverarbeitung stoppen.

Unabhängig von der Clientplattform wird in NAS-Dateisystemspezifikationen der Schrägstrich (/) als Trennzeichen verwendet. Zum Beispiel: /vol/vol0.

Unterstützte Clients

Dieser Befehl ist nur für AIX- und Solaris-Clients gültig.

Syntax



Parameter

Dateispezifikation

Gibt den Namen eines oder mehrerer Dateisysteme auf dem NAS-Dateiserver an. Wenn Sie diesen Parameter nicht angeben, verarbeitet der Client für Sichern/Archivieren alle Dateisysteme, die durch die Option `domain.nas` definiert sind.

Wenn Sie die Option *Dateispezifikation* oder `domain.nas` nicht angeben, wird der Standardwert **all-nas** für `domain.nas` verwendet, und es werden alle Dateisysteme auf dem NAS-Dateiserver gesichert.

Tabelle 87. Befehl Backup NAS: Zugehörige Optionen

Option	Verwendung
mode „Mode“ auf Seite 509	Nur in der Befehlszeile.

Tabelle 87. Befehl Backup NAS: Zugehörige Optionen (Forts.)

Option	Verwendung
monitor „Monitor“ auf Seite 512	Nur in der Befehlszeile.
nasnodename „Nasnodename“ auf Seite 515	Clientoptionsdatei (dsm.sys) oder Befehlszeile.
toc „Toc“ auf Seite 619	Befehlszeile oder mit der Option include.fs.nas in Ihrer Clientoptionsdatei (dsm.sys).

Beispiele

- Task** Die NAS-Imagesicherung des gesamten Dateisystems ausführen.
Befehl: backup nas -mode=full -nasnodename=nas1 /vol/vol0 /vol/vol2
- Task** Die NAS-Imagesicherung des gesamten Dateiservers ausführen.
Befehl: backup nas -nasnodename=nas1
- Task** Die NAS-Imagesicherung des gesamten Dateisystems ausführen und TOC-Angaben für die Dateisystemsicherung speichern.
Befehl: backup nas -mode=full -nasnodename=netappsj /vol/vol0 -toc=yes

Zugehörige Informationen

„Nasnodename“ auf Seite 515

„Toc“ auf Seite 619

„Mode“ auf Seite 509

„Monitor“ auf Seite 512

„Cancel Process“ auf Seite 719

„Domain.nas“ auf Seite 413

Backup VM

Mit dem Befehl **backup vm** können Sie eine Gesamtsicherung einer virtuellen Maschine starten.

Virtuelle VMware-Maschinen sichern

Mit dem Befehl **backup vm** können Sie virtuelle VMware-Maschinen sichern.

Eine oder mehrere virtuelle Maschinen werden durch den Knoten der IBM Spectrum Protect-Einheit zum Versetzen von Daten gesichert. Als *Knoten der Einheit zum Versetzen von Daten* wird eine Konfiguration bezeichnet, in der der Client für Sichern/Archivieren auf einem vStorage-Sicherungsserver ausgeführt wird und für den Schutz der virtuellen Maschinen auf einem Virtual Center- oder ESX-/ESXi-Server konfiguriert ist. Sie müssen die virtuelle VMware-Maschine konfigurieren,

bevor Sie diesen Befehl verwenden. Informationen zur Konfiguration der virtuellen VMware-Maschine finden Sie in Umgebung für Gesamtsicherungen virtueller VMware-Maschinen vorbereiten. .

Bei einer VM-Gesamtsicherung wird eine Sicherungskopie aller virtuellen Plattenimages und Konfigurationsinformationen einer virtuellen Maschine gespeichert. VM-Gesamtsicherungen ermöglichen eine vollständige Zurückschreibung einer virtuellen Maschine, sie erfordern jedoch mehr Zeit und mehr Speicherbereich auf dem Server als eine Teilsicherung.

Wenn Sie die Option `vmenabletemplatebackups` auf **yes** setzen, umfasst eine VM-Sicherungsoperation (**backup vm**) die virtuellen Schablonenmaschinen, vorausgesetzt, der vStorage-Sicherungsserver ist mit einem vCenter-Server und nicht mit einem ESX- oder ESXi-Host verbunden.

Schlägt eine Momentaufnahme während der Sicherungsverarbeitung fehl, unternimmt der Client noch einen Versuch, die virtuelle VMware-Maschine zu sichern. Die Gesamtzahl der Momentaufnahmeversuche können Sie mit der Option `INCLUDE.VMSNAPSHOTATTEMPTS` in der Clientoptiondatei definieren.

Datenschutztags werden verwendet, um die Sicherungsmaßnahme virtueller Maschinen in VMware-Objekten zu konfigurieren. Die Tags und Kategorien werden erstellt, wenn Sie eine der folgenden Methoden verwenden:

- Aktivieren Sie mit der Option `vmtagdatamover` die Tagging-Unterstützung auf dem Knoten der Einheit zum Versetzen von Daten und führen Sie den Befehl **backup vm** aus.
- Verwenden Sie die IBM Spectrum Protect vSphere-Client-Plug-in, um IBM Spectrum Protect-Sicherungen zu verwalten.
- Führen Sie den Befehl **set vmtags** auf einem beliebigen Knoten einer Einheit zum Versetzen von Daten aus.

Wenn die Option `vmtagdatamover` auf *yes* gesetzt wird, werden alle Tags, die einer virtuellen Maschine zugeordnet sind, während der Ausführung von Operationen **backup vm** gesichert. Die Tags werden zurückgeschrieben, wenn der Befehl **restore vm** ausgeführt wird. Tags, die anderen Bestandsobjekten zugeordnet sind, werden nicht gesichert und können nicht zurückgeschrieben werden.

Weitere Informationen zu Datenschutztags finden Sie in Übersicht über das Datenschutztagging.

Eine VM-Gesamtsicherung verwendet die VMware-Überwachung geänderter Blöcke (Changed Block Tracking, CBT), um inhaltsgesteuerte Sicherungen (nur verwendete Blöcke) zu erstellen. Der Client aktiviert die Überwachung geänderter Blöcke (CBT) auf einem ESX- oder ESXi-Server, wenn eine Sicherung beginnt. Für VMware CBT ist ein Host mit ESX 4.1 (oder höher) und mit virtueller Hardware 7 (oder höher) erforderlich. Sie können keine inhaltsgesteuerten VM-Teilsicherungen oder VM-Gesamtsicherungen auf virtuellen Maschinen ausführen, die CBT nicht unterstützen.

Wenn CBT aktiviert ist, überwacht es Plattenänderungen, wenn der ESX- oder ESXi-Serverspeicherstack E/A-Operationen auf den folgenden Platten verarbeitet:

- Eine im VMFS gespeicherte virtuelle Platte. Die Platte kann eine iSCSI-Platte, eine lokale Platte oder eine Platte in einem SAN sein.
- Eine im NFS gespeicherte virtuelle Platte.

- Eine RDM-Platte, die sich im Modus für virtuelle Kompatibilität befindet.

Wenn der ESX- oder ESXi-Speicherstack keine E/A-Operationen verarbeitet, kann CBT nicht für die Überwachung von Plattenänderungen verwendet werden. Die folgenden Platten können CBT nicht verwenden:

- Eine RDM-Platte, die sich im Modus für physische Kompatibilität befindet.
- Eine Platte, auf die direkt aus einer virtuellen Maschine heraus zugegriffen wird. vSphere kann beispielsweise keine Änderungen an einer iSCSI-LUN überwachen, auf die ein iSCSI-Initiator in der virtuellen Maschine zugreift.

Vollständige Informationen zu den Anforderungen für die Überwachung geänderter Blöcke (Changed Block Tracking, CBT) finden Sie in der Veröffentlichung *VMware Virtual Disk API Programming Guide* in der VMware-Produktdokumentation. Suchen Sie in dem Handbuch nach „Low Level Backup Procedures“ und lesen Sie den Abschnitt „Changed Block Tracking on Virtual Disks“.

Bei VMware-Servern, die CBT nicht unterstützen, werden sowohl die verwendeten als auch die nicht verwendeten Bereiche der Platte gesichert; außerdem wird eine Informationsnachricht in der Datei `dsmerror.log` protokolliert. Verwenden Sie die Option `-preview` im Befehl **backup vm**, um den aktuellen CBT-Status anzuzeigen. Der CBT-Status hat drei Werte:

Off Gibt an, dass der CBT-Konfigurationsparameter (**ctkEnabled**) in den Konfigurationsparametern der virtuellen Maschine nicht aktiviert ist. **Off** ist der Standardstatus.

Not Supported

Gibt an, dass die virtuelle Maschine CBT nicht unterstützt. Sicherungen von ausschließlich geänderten Blöcken sind nicht möglich.

On Gibt an, dass die virtuelle Maschine CBT unterstützt und dass CBT in den Konfigurationsparametern der virtuellen Maschine aktiviert ist (`ctkEnabled=true`).

Der Client aktiviert CBT (Einstellung `ctkEnable=true`) bei jedem Sicherungsversuch. Nachdem der Client CBT aktiviert hat, bleibt es aktiviert, auch wenn die virtuelle Maschine auf dem IBM Spectrum Protect-Server gelöscht wird. Wenn CBT aktiviert ist, werden nach der Ausführung der ersten VM-Gesamtsicherung nur die geänderten Blöcke auf der Platte gesichert oder zurückgeschrieben.

Wenn Sie keine IBM Spectrum Protect-Sicherungen einer virtuellen Maschine mehr ausführen, können Sie CBT inaktivieren. Für die Inaktivierung von CBT klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, für die Sie CBT im vSphere-Client inaktivieren wollen. Klicken Sie auf **Einstellungen editieren > Optionen > Allgemein > Konfigurationsparameter**. Setzen Sie dann den Konfigurationsparameter **ctkEnabled** auf `false`.

Tipp: Sie können die Komprimierungsoption nur dann für Sicherungen verwenden, wenn die Sicherung in einem Speicherpool gespeichert wird, der für die clientseitige Deduplizierung aktiviert wurde.

Sie können die Optionen `-vmbackuptype` und `-mode` angeben, um festzulegen, wie die Sicherungen ausgeführt werden sollen. Verwenden Sie für VM-Gesamtsicherungen `-vmbackuptype=fullvm` und geben Sie eine der folgenden Optionen für den Modus an:

IFFull Modus 'Immer inkrementell - Vollständig'. In diesem Modus wird eine Momentaufnahme aller verwendeten Blöcke auf den Platten einer virtuellen

Maschine auf dem Server gesichert. Für diese Option benötigen Sie eine Lizenz für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware oder IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V.

IFIncremental

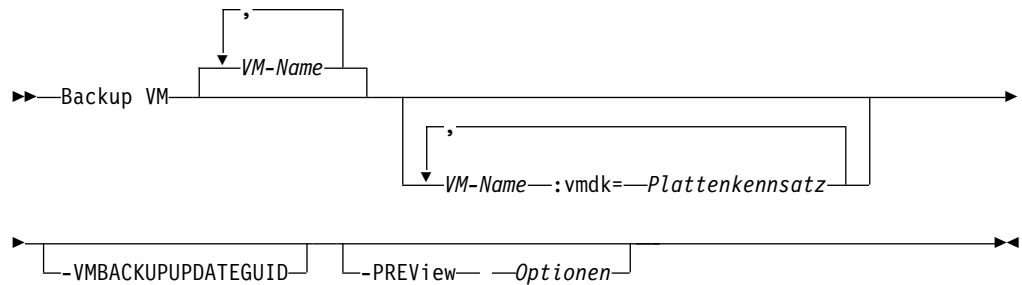
Immer inkrementell - Inkrementell. In diesem Modus wird eine Momentaufnahme erstellt, die aus den Blöcken besteht, die sich seit der letzten Sicherung geändert haben. Für diese Option benötigen Sie eine Lizenz für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware oder IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V.

Informationen zur Sicherungsstrategie "Immer inkrementell" finden Sie in Sicherungsstrategie "Immer inkrementell".

Unterstützte Clients

Dieser Befehl ist nur auf unterstützten Linux-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind, der virtuelle VMware-Maschinen schützt.

Syntax



Parameter

VM-Name

Geben Sie den Namen einer virtuellen Maschine oder die Namen mehrerer virtueller Maschinen an, die gesichert werden soll(en). Der Name ist der Anzeigename der virtuellen Maschine. Trennen Sie die Namen mehrerer virtueller Maschinen durch Kommas. Wenn Sie die Option `vmenabletemplatebackups` auf **yes** gesetzt haben, kann `VM-Name` den Namen einer virtuellen Schablonenmaschine angeben, die gesichert werden soll.

In VMware vCenter dürfen zwei oder mehr virtuelle Maschinen denselben Anzeigenamen haben. Für den Client für Sichern/Archivieren müssen jedoch alle Namen virtueller Maschinen in einer vCenter-Serverkonfiguration eindeutig sein. Damit während der Verarbeitung keine Fehler auftreten, stellen Sie sicher, dass alle virtuellen Maschinen einen eindeutigen Anzeigenamen haben.

In den Namen virtueller Maschinen, die in diesem Parameter angegeben werden, können Platzhalterzeichen verwendet werden. Die Verarbeitung von Platzhalterzeichen unterscheidet sich jedoch je nach dem verwendeten Sicherungsmodus.

- Für Sicherungen mit den Optionen `mode=iffull` und `mode=ifincremental` können Platzhalterzeichen bei VM-Namensmustern verwendet werden. Zum Beispiel:
 - `backup vm VM_TEST*` umfasst alle virtuelle Maschinen, deren Name mit `VM_TEST` beginnt.
 - `backup vm VM??` umfasst alle virtuellen Maschinen, deren Name mit den Buchstaben „VM“ beginnt, gefolgt von 2 beliebigen Zeichen.

Wenn Sie *VM-Name* nicht angeben, können Sie die virtuelle Maschine mit der Option `domain.vmfull` identifizieren.

:vmdk=Plattenkennsatz

Dieses Schlüsselwort ist eine Erweiterung von *VM-Name*. Es gibt den Kennsatz (Namen) der Platte der virtuellen Maschine an, die in die Sicherungsoperation eingeschlossen werden soll. Sie können eine Platte ausschließen, indem Sie dem Schlüsselwort den Ausschlussoperator (-) voranstellen. Weitere Methoden zum Einschließen oder Ausschließen von Platten für die Verarbeitung finden Sie unter `Domain.vmfull`, `Exclude.vmdisk` und `Include.vmdisk`.

-VMBACKUPUPDATEGUID

Für diese Option benötigen Sie eine Lizenzvereinbarung für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Mit dieser Option wird die global eindeutige ID (GUID) für die zu sichernde virtuelle Maschine aktualisiert. Dieser Parameter ist ausschließlich für die Verwendung in dem folgenden Szenario vorgesehen:

Sie möchten eine bereits gesicherte virtuelle Maschine mit dem Namen ORION zurückschreiben. Bevor Sie jedoch das System herunterfahren und die in der Produktionsumgebung ausgeführte Kopie von ORION durch die zurückgeschriebene Kopie ersetzen, möchten Sie die Konfiguration der zurückgeschriebenen virtuellen Maschine überprüfen.

1. Sie schreiben die virtuelle Maschine ORION zurück und ordnen ihr einen neuen Namen zu: `dsmc restore vm Orion -vmname=Orion2`.
2. Sie aktualisieren und überprüfen die virtuelle Maschine ORION2 und stellen fest, dass sie die vorhandene virtuelle Maschine mit dem Namen ORION ersetzen kann.
3. Sie schalten das System aus und löschen ORION.
4. Sie benennen ORION2 in ORION um.
5. Bei der nächsten Sicherung von ORION mit einer immer inkrementellen Gesamtsicherung oder einer immer inkrementellen Teilsicherung fügen Sie dem Befehl **backup vm** den Parameter **-VMBACKUPUPDATEGUID** hinzu. Durch diese Option wird die GUID auf dem IBM Spectrum Protect-Server aktualisiert, sodass die neue GUID den gespeicherten Sicherungen für die virtuelle Maschine ORION zugeordnet ist. Die Kette der Teilsicherungen bleibt erhalten; es ist nicht erforderlich, vorhandene Sicherungen zu löschen und durch neue Sicherungen zu ersetzen.

-PREView

Diese Option zeigt Informationen zu einer virtuellen Maschine an, ein-

schließlich der Kennsätze der Festplatten in der virtuellen Maschine und der Verwaltungsklasseninformationen für eine virtuelle Maschine.

Sie können die Plattenkennsätze mit den Schlüsselwörtern `:vmdk=` oder `:-vmdk=` verwenden, um Platten bei einer Sicherungsoperation ein- oder auszuschließen. Das folgende Beispiel zeigt Ausgabe vom Parameter

-preview:

```
backup vm vm1 -preview
Gesamtsicherung der virtuellen Maschine 'VM1'

vmName:vm1
VMDK[1]Label: Hard disk 1
VMDK[1]Name: [ds5k_svt_1] tsmcetlnx14/tsmcetlnx14.vmdk
VMDK[1]Status: Included
VMDK[2]Label: Hard disk 2
VMDK[2]Name: [ds5k_svt_1] tsmcetlnx14/tsmcetlnx14_1.vmdk
VMDK[2]Status: Excluded - user,Independent,pRDM
```

Diese `-preview`-Beispielausgabe zeigt, dass VMDK2 von der vorherigen Sicherung ausgeschlossen war. In eine Sicherung eingeschlossene Platten haben den Status `Included` (Eingeschlossen). Von der Sicherung ausgeschlossene Platten haben den Status `Excluded` (Ausgeschlossen), an den sich ein Ursachencode anschließt. Folgende Ursachencodes sind möglich:

user Gibt an, dass die Platte übersprungen wurde, weil sie in einer Anweisung `domain.vmfull`, in der Befehlszeile oder in der `Clientoptionsdatei` ausgeschlossen wurde.

Independent

Gibt an, dass die Platte eine unabhängige Platte ist. Unabhängige Platten können nicht Teil einer Momentaufnahme sein, daher werden sie bei VM-Sicherungsoperationen (**backup vm**) ausgeschlossen. Stellen Sie sicher, dass die Option `vmprocessvmwithindependent` auf 'yes' gesetzt ist. Andernfalls wird die gesamte virtuelle Maschine bei einer Sicherungsoperation übergangen, wenn sie eine oder mehrere unabhängige Platten enthält.

pRDM

Gibt an, dass die Platte eine pRDM-Platte ist (pRDM = physical Raw Device Mapping). pRDM-Platten können nicht Teil einer Momentaufnahme sein, daher werden sie bei VM-Sicherungsoperationen (**backup vm**) ausgeschlossen. Stellen Sie sicher, dass die Option `vmprocessvmwithprdm` auf 'yes' gesetzt ist. Andernfalls wird die gesamte virtuelle Maschine von einer Sicherungsoperation übergangen, wenn sie mindestens einen RDM-Datenträger enthält, der im Modus für physische Kompatibilität (pRDM) bereitgestellt wird (RDM = Raw Device Mapping).

In der Ausgabe des Parameters **-preview** wird auch der Name der Verwaltungsklasse angezeigt, die der virtuellen Maschine zugeordnet ist, sowie Informationen dazu, wo die Verwaltungsklasse definiert wurde. Mithilfe dieser Informationen können Sie überprüfen, ob die Domänen- und Tagwerte für die Verwaltungsklasse korrekt definiert sind. Beispiel:

```
backup vm -preview
Full BACKUP VM der virtuellen Maschinen, die in der Option DOMAIN.VMFULL angegeben sind.
```

```
1. vmName: tag_vm_2
   DomainKeyword: all-vm
   toolsRunningStatus: guestToolsNotRunning
   toolsVersionStatus: guestToolsNotInstalled
   consolidationNeeded: No
   Change Block Tracking: On
```

```

managementClassName: STANDARD
managementClassLocation: Node Default

VMDK[1]Label: 'Hard disk 1' (Hard Disk 1)
VMDK[1]Name: '[Raid1-lannds2] tag_vm_2/tag_vm_2.vmdk'
VMDK[1]Status: Included
...

12. vmName: vm-jean
DomainKeyword: all-vm
toolsRunningStatus: guestToolsNotRunning
toolsVersionStatus: guestToolsNotInstalled
consolidationNeeded: No
Change Block Tracking: On
managementClassName: MGMTCLASS1 (invalid)
managementClassLocation: VM Tag Management Class (IBM Spectrum Protect)

VMDK[1]Label: 'Hard disk 1' (Hard Disk 1)
VMDK[1]Name: '[Raid1-lannds2] vm-jean/vm-jean.vmdk'
VMDK[1]Status: Included

```

Hierbei gilt Folgendes:

managementClassName

Zeigt den Namen der Verwaltungsklasse an, an die die virtuelle Maschine gebunden ist.

Wird neben dem Namen der Verwaltungsklasse "(invalid)" (ungültig) angezeigt, wurde entweder der Name falsch angegeben oder die Verwaltungsklasse auf dem IBM Spectrum Protect-Server entfernt oder keine Sicherungskopiengruppe in der Verwaltungsklasse auf dem Server gefunden. Wenn der Name der Verwaltungsklasse ungültig ist, schlägt die Sicherungsoperation für die virtuelle Maschine fehl.

managementClassLocation

Zeigt an, wo die Verwaltungsklasse definiert wurde. Die folgenden Positionen sind möglich:

Node Default

Die Verwaltungsklasse wurde in der Standarddomäne des VMware-Datencenterknotens definiert.

VMMC option

Die Verwaltungsklasse wurde mit der Option `vmmc` definiert.

VMCTLMC option

Die Verwaltungsklasse wurde mit der Option `vmctlmc` definiert.

INCLUDE.VM option

Die Verwaltungsklasse wurde mit der Option `include.vm` definiert.

VM Tag Management Class (IBM Spectrum Protect)

Die Verwaltungsklasse wurde als Tagwert der Tagkategorie Management Class (IBM Spectrum Protect) definiert. Tagwerte können mit Datenschutzeinstellungen in der IBM Spectrum Protect vSphere-Client-Plug-in im vSphere-Web-Client oder mithilfe von Tools wie beispielsweise VMware vSphere PowerCLI Version 5.5 R2 oder höher festgelegt werden.

Wichtig: Um die durch Tags definierten Verwaltungsklasseninformationen anzuzeigen, müssen Sie die Option `vmtagdatamover yes` in der Clientopti-

onsdatei definieren oder den Parameter **-vmtagdatamover=yes** einschließen, wenn Sie den Befehl **dsmc backup vm** ausführen. Wenn Sie die Option **vmtagdatamover** nicht definiert haben oder die Option auf **no** gesetzt haben, ignoriert der Client alle Tagwerte für die Verwaltungsklasse und zeigt die Verwaltungsklassendefinition an, die in der Standarddomäne des Datacenterknotens, in der Option **vmc** oder in der Option **include.vm** definiert ist.

Rückkehrcodes für Sicherungsoperationen für virtuelle Maschinen

Bei der Beendigung von Sicherungsoperationen für virtuelle Maschinen können die Rückkehrcodes ausgegeben werden, die in der folgenden Tabelle enthalten sind.

Rückkehrcode	Beschreibung
0	Ein Befehl zum Sichern einer oder mehrerer virtueller Maschinen wurde erfolgreich ausgeführt.
8	Ein Befehl zum Sichern mehrerer virtueller Maschinen wurde nur für einige der virtuellen Maschinen, für die der Befehl galt, erfolgreich ausgeführt. Der Protokolldatei können Sie den Verarbeitungsstatus jeder der virtuellen Maschinen entnehmen, für die der Befehl galt.
12	Gibt an, dass eine der folgenden Fehlerbedingungen aufgetreten ist: <ul style="list-style-type: none"> Durch den Sicherungsbefehl konnte keine der virtuellen Maschinen gesichert werden, die Ziele der Sicherungsoperation waren. Der Sicherungsbefehl ist fehlgeschlagen und wurde gestoppt, bevor alle angegebenen virtuellen Maschinen überprüft wurden. Untersuchen Sie die Protokolldatei, um die Fehlerursache festzustellen.

vStorage API for Data Protection - Beispielbefehle

Eine IFIncremental-Sicherung zweier VMs mit den Namen **vm3** und **vm4** ausführen.

```
dsmc backup vm vm3,vm4 -vmbackuptype=fullvm -mode=ifincremental
```

Eine IFFull-Sicherung einer VM mit dem Namen **vm1** ausführen.

```
dsmc backup vm vm1 -vmbackuptype=fullvm -mode=iffull
```

Eine IFFull-Sicherung einer VM mit dem Namen **vm1** ausführen, aber nur 'Festplatte 1' in die Sicherungsoperation einschließen.

```
dsmc backup vm "vm1:vmdk=Festplatte 1" -vmbackuptype=fullvm -mode=iffull
```

Eine immer inkrementelle Sicherung der virtuellen Maschine **vm1** ausführen, 'Festplatte 1' und 'Festplatte 4' jedoch von der Sicherungsoperation ausschließen.

```
dsmc backup vm "vm1:-vmdk=Festplatte 1:-vmdk=Festplatte 4"
-vmbackuptype=fullvm -mode=iffull
```

Eine immer inkrementelle Gesamtsicherung der virtuellen Maschinen mit den Namen **vm1** und **vm2** ausführen. Auf **vm1** nur 'Festplatte 2' und 'Festplatte 3' sichern. Auf **vm2** alle virtuellen Platten sichern.

```
dsmc backup vm "vm1:vmdk=Festplatte 2:vmdk=Festplatte 3",
vm2 -vmbackuptype=fullvm -mode=iffull
```

Parallele immer inkrementelle Gesamtsicherungen der virtuellen VMware-Maschinen ausführen, die mithilfe der Auswahlkriterien (Domänenparameter) in der An-

weisung `domain.vmfull` für die Sicherung ausgewählt werden. Die maximale Anzahl paralleler Sicherungen auf 5 virtuelle Maschinen und 10 Sitzungen setzen und die Sicherungen auf 5 virtuelle Maschinen pro Host und 5 virtuelle Maschinen pro Datenspeicher begrenzen.

```
dsmc backup vm -vmbackuptype=fullvm -mode=iffull -vmmaxparallel=5  
-vmmaxbackupsessions=10 -vmlimitperhost=5 -vmlimitperdatastore=5
```

Zugehörige Links für die Sicherung virtueller VMware-Maschinen

- **Query VM**
- **Restore VM**
- `Domain.vmfull`
- `Include.vm`
- `Mbobjrefreshthresh`
- `Mbpctrefreshthresh`
- `Mode`
- `Vmbackdir`
- `Vmbackuplocation`
- `Vmbackupmailboxhistory`
- `Vmbackuptype`
- `Vmchost`
- `Vmctlmc`
- `Vmcpw`
- `Vmcuser`
- `Vmdatastorethreshold`
- `Vmenabletemplatebackups`
- `Vmlimitperdatastore`
- `Vmlimitperhost`
- `Vmmaxbackupsessions`
- `Vmmaxparallel`
- `Vmmaxvirtualdisks`
- `Vmmc`
- `Vmpreferdagpassive`
- `Vmprocessvmwithindependent`
- `Vmprocessvmwithprdm`
- `Vmskipctlcompression`
- `Vmskipmaxvirtualdisks`
- `Vmtagdatamover`
- `Vmtagdefaultdatamover`
- `Vmverifyifaction`
- `Vmverifyiflatest`
- `Vmvstortransport`
- `Vmvstorcom`
- `Vmtimeout`
- **Set Vmtags**
- **Exclude-Optionen für virtuelle Maschinen**
- **Include-Optionen für virtuelle Maschinen**

I

Cancel Process

Der Befehl **cancel process** zeigt (sofern die NDMP-Unterstützung aktiviert ist) eine Liste der aktuellen NAS-Imagesicherungs- und -zurückschreibungsprozesse an, für die der Benutzer mit Verwaltungsaufgaben die Berechtigung hat. Sie werden zur Eingabe der IBM Spectrum Protect-Administrator-ID aufgefordert.

Aus der Liste kann der Benutzer mit Verwaltungsaufgaben einen Prozess zum Abbrechen auswählen. Die Clientegnereberechtigung ist als Berechtigung ausreichend, um die ausgewählten NAS-Imagesicherungs- oder -zurückschreibungsprozesse abzubrechen.

Unterstützte Clients

Dieser Befehl ist nur für AIX-, Linux- und Solaris-Clients gültig.

Syntax

►—Cancel Process—◄◄

Parameter

Für diesen Befehl gibt es keine Parameter.

Beispiele

Task Die aktuellen NAS-Imagesicherungs- oder -zurückschreibungsprozesse abbrechen.

Befehl: cancel process

Cancel Restore

Mit dem Befehl **cancel restore** kann eine Liste der wiederanlauffähigen Zurückschreibungssitzungen des Benutzers in der Serverdatenbank angezeigt werden.

Sie können nur jeweils eine wiederanlauffähige Zurückschreibungssitzung abbrechen. Führen Sie den Befehl **cancel restore** erneut aus, um weitere Zurückschreibungen abzubrechen. Zum erneuten Starten wiederanlauffähiger Zurückschreibungssitzungen den Befehl **restart restore** verwenden.

Verwenden Sie den Befehl **cancel restore** in den folgenden Fällen:

- Dateien, die von der wiederanlauffähigen Zurückschreibung betroffen sind, können nicht gesichert werden.
- Wiederanlauffähige Zurückschreibungssitzungen sperren den Dateibereich, so dass Dateien nicht von den sequenziellen Serverdatenträgern weg verschoben werden können.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

►►—Cancel Restore—◄◄

Parameter

Für diesen Befehl gibt es keine Parameter.

Beispiele

Task Eine Operation zum Zurückschreiben abbrechen.

```
cancel restore
```

Delete Access

Der Befehl **delete access** löscht Berechtigungsregeln für Dateien, die auf dem Server gespeichert sind.

Wenn Sie eine Berechtigungsregel löschen, wird der Benutzerzugriff für alle Dateien oder Images, die diese Regel angibt, widerrufen.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

►►—Delete— —Access—◄◄

Parameter

Für diesen Befehl gibt es keine Parameter.

Beispiele

Task Eine Liste der aktuellen Berechtigungsregeln anzeigen und die zu löschen- den Regeln auswählen.

```
delete access
```

Siehe hierzu das folgende Anzeigenbeispiel:

Index	Art	Knoten	Eigner	Pfad
1	Sichern	NODE1	USER1	home/dev/proja/list/
2	Archiv.	NODE3	LUIE	home/fin/budg/depta/
3	Sichern	NODE4	USER2	home/plan/exp/deptc/
4	Archiv.	NODE5	USER2S	home/mfg/invn/parta/

Index der zu löschenden Regel(n) eingeben oder Abbrechen:

Sollen die Berechtigungsregeln gelöscht werden, die luie und user2s den Zugriff auf Ihre Dateien oder Images erlauben, geben Sie 2 4 oder 2,4 ein und drücken Sie die Eingabetaste.

Delete Archive

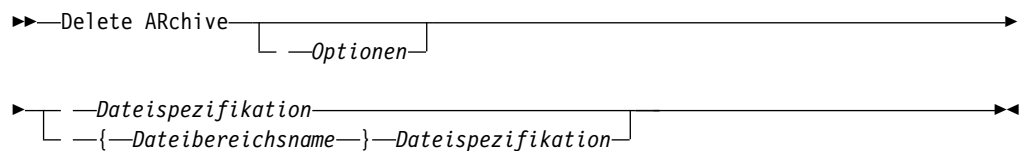
Mit dem Befehl **delete archive** können archivierte Dateien aus dem IBM Spectrum Protect-Serverspeicher gelöscht werden. Der Benutzer kann archivierte Dateien nur löschen, wenn ihm der Administrator die entsprechende Berechtigung erteilt hat.

Wichtig: Nach dem Löschen archivierter Dateien können diese nicht mehr abgerufen werden. Daher muss vor dem Löschen sichergestellt werden, dass die Dateien nicht mehr benötigt werden.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax



Parameter

Dateispezifikation

Gibt den Pfad und den Namen der Datei an, die aus dem Speicher gelöscht werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis anzugeben. Sie können auch die Option **filelist** verwenden, um eine Liste von Dateien zu verarbeiten. Der Client für Sichern/Archivieren öffnet die Datei, die Sie mit dieser Option angeben, und verarbeitet die darin enthaltene Liste der Dateien dem jeweiligen Befehl entsprechend.

Anmerkung: Wenn *Dateibereichsname* angegeben wird, darf die Dateispezifikation keinen Laufwerkbuchstaben enthalten.

{Dateibereichsname}

Gibt den Dateibereich (zwischen geschweiften Klammern) auf dem Server an, in dem sich die zu löschende Datei befindet. Dies ist der Name auf dem Workstationlaufwerk, auf dem die Datei archiviert wurde.

Verwenden Sie *Dateibereichsname*, wenn der Name geändert wurde oder wenn Sie Dateien löschen, die auf einem anderen Knoten archiviert wurden, dessen Laufwerkbezeichnungen sich von Ihren unterscheiden.

Tabelle 88. Befehl Delete Archive: Zugehörige Optionen

Option	Verwendung
dateformat „Dateformat“ auf Seite 389	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
description „Description“ auf Seite 397	Nur in der Befehlszeile.
filelist „Filelist“ auf Seite 453	Nur in der Befehlszeile.

Tabelle 88. Befehl Delete Archive: Zugehörige Optionen (Forts.)

Option	Verwendung
noprompt „Noprompt“ auf Seite 519	Nur in der Befehlszeile.
numberformat „Numberformat“ auf Seite 521	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
pick „Pick“ auf Seite 528	Nur in der Befehlszeile.
subdir „Subdir“ auf Seite 605	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
tapeprompt „Tapeprompt“ auf Seite 607	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
timeformat „Timeformat“ auf Seite 616	Clientoptionsdatei (dsm.opt) oder Befehlszeile.

Beispiele

Task Eine Datei mit dem Namen budget löschen.

```
dsmc delete archive /user/home/proj1/budget
```

Task Alle Dateien löschen, die aus dem Verzeichnis /user/home/proj1 archiviert wurden und die Dateierweiterung .txt haben.

```
dsmc del arch "/user/home/proj1/*.txt"
```

Task Dateien löschen, die aus dem Verzeichnis /user/project archiviert wurden; dabei die Option **pick** verwenden, um eine Liste der Archivierungskopien anzuzeigen, die mit der Dateispezifikation übereinstimmen. Aus der Liste können die zu verarbeitenden Versionen ausgewählt werden.

```
dsmc delete archive "/user/project/*" -pick
```

Task Ausgewählte Dateien aus der Dateigruppe löschen, die mit der Beschreibung „Monthly Budgets 2010“ archiviert wurde und sich in /user/projects und dessen Unterverzeichnissen befindet.

```
dsmc delete ar "/user/projects/*" -description="Monthly Budgets 2010" -pick -subdir=yes
```

Zugehörige Informationen

Delete Backup

Der Befehl **delete backup** löscht Dateien, Images und virtuelle Maschinen, die im IBM Spectrum Protect-Serverspeicher gesichert wurden. Ihr Administrator muss Ihnen die Berechtigung zum Löschen von Objekten erteilen.

Wenn Sie Dateien löschen, inaktiviert der IBM Spectrum Protect-Server alle gesicherten Dateien, die den angegebenen Optionen Dateispezifikation und deltype entsprechen. Außerdem ordnet der Server das Inaktivierungsdatum *unendlich-minus* zu, sodass die Dateien nicht mehr für Zurückschreibungen verfügbar sind und bei der nächsten Ausführung des Dateiverfalls sofort gelöscht werden. Die Datei wird erst bei der Ausführung des Verfallsprozesses physisch gelöscht.

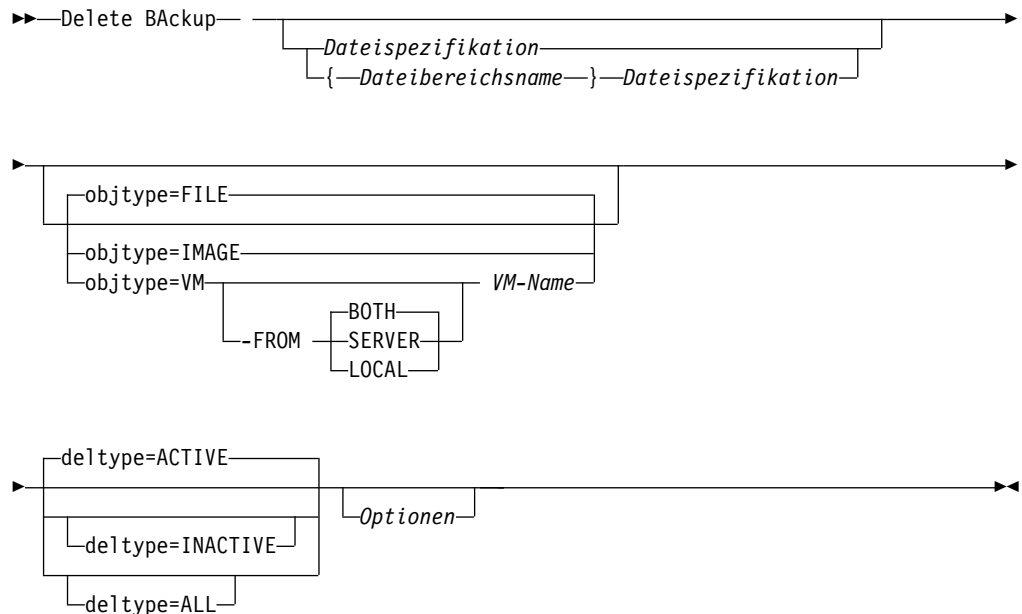
Wichtig: Nach dem Löschen von Sicherungsdateien können diese nicht mehr zurückgeschrieben werden. Stellen Sie vor dem Löschen sicher, dass die Sicherungs-

dateien nicht mehr benötigt werden. Sie werden aufgefordert, die Fortsetzung des Löschvorgangs zu bestätigen. Wenn Sie **ja** angeben, werden die angegebenen Sicherungsdateien in den Zeitplan zum Löschen aufgenommen und aus dem Serverspeicher entfernt.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax



Parameter

Dateibereich/Dateispezifikation

Dateispezifikation

Gibt den Pfad und den Namen der Datei an, die aus dem Speicher gelöscht werden soll. Um eine Datei in einem anderen Dateibereich anzugeben, geben Sie vor dem Dateinamen den Dateibereichsnamen ein. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis anzugeben. Trennen Sie die Dateispezifikationen durch ein Leerzeichen. Sie können auch die Option `filelist` verwenden, um eine Liste von Dateien zu verarbeiten. Der Client für Sichern/Archivieren öffnet die Datei, die mit dieser Option angegeben wird, und verarbeitet die darin enthaltene Liste der Dateien dem jeweiligen Befehl entsprechend.

Anmerkung: Wenn *Dateibereichsname* angegeben wird, darf die Dateispezifikation keinen Laufwerkbuchstaben enthalten.

Verwenden Sie bei Angabe von `-deltype=inactive` oder `-deltype=active` Platzhalterzeichen, um eine Dateigruppe oder alle Dateien in einem Verzeichnis anzugeben.

Geben Sie bei Verwendung von `-deltype=all` ein Verzeichnis an, das ausschließlich aus Platzhalterzeichen besteht.

objtype

Gibt den Typ des zu löschenden Objekts an. Sie können einen der folgenden Werte angeben:

FILE

Gibt an, dass Dateien und Verzeichnisse gelöscht werden sollen. Dieser Wert ist der Standardobjekttyp.

IMAGE

Gibt an, dass eine Imagesicherung gelöscht werden soll. Gibt an, dass eine Imagesicherung gelöscht werden soll. Objtype=image wird unter Mac OS X nicht unterstützt.

VM VM-Name

Gibt an, dass Sie mindestens eine Version einer Sicherung einer virtuellen Maschine löschen möchten; die virtuelle Maschine wird durch den Variablenparameter *VM-Name* angegeben. Der Name der virtuellen Maschine darf keine Platzhalterzeichen enthalten.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Wird objtype=VM angegeben, kann die Option filelist nicht verwendet werden. Die Angabe von objtype=VM ändert das Verhalten der Option -deltype. Wird objtype=vm angegeben, können Sie entweder -deltype=active oder -deltype=inactive verwenden. Sie können nicht -deltype=all verwenden. Bei Angabe von -deltype=inactive wird eine Liste der aktiven und der inaktiven Sicherungen angezeigt. Anhand dieser Liste können Sie die Sicherungen virtueller Maschinen angeben, die gelöscht werden sollen. Sollen nur die aktiven Sicherungen virtueller Maschinen gelöscht werden, verwenden Sie -deltype=active.

Wenn Sie -objtype=VM angeben, löscht dieser Befehl nur Sicherungen virtueller Maschinen, die mit einem der folgenden Modi erstellt wurden: IFINCR und IFFULL.

Für Sicherungen, die mit Clients der Version 7.1 oder früher erstellt wurden: Einzelne Teilsicherungen (mit MODE=INCR erstellte Sicherungen), die nach der Ausführung einer Gesamtsicherung erstellt wurden, können nicht mit diesem Befehl gelöscht werden. Löschen Sie jedoch eine Imagegesamtsicherung einer virtuellen Maschine (mit MODE=FULL erstellte Sicherung) und verfügt der Server über Teilsicherungen (MODE=INCR), die für diese VM nach der Gesamtsicherung erstellt wurden, werden beim Löschen der VM-Gesamtsicherung auch die Sicherungsdateien gelöscht, die mit MODE=INCR erstellt wurden.

Wenn Sie eine aktive Sicherung für eine virtuelle Maschine löschen, wird die neueste inaktive Kopie zur aktiven Sicherung. Wenn Sie die Option -pick oder -inactive angeben, wird nur die von Ihnen angegebene Sicherung gelöscht. Wenn Sie eine mit MODE=IFINCR erstellte Sicherung auswählen, wird nur die ausgewählte Teilsicherung gelöscht, andere Teilsicherungen für die virtuelle Maschine werden nicht gelöscht.

-FROM

Geben Sie die Sicherungsposition oder -positionen an, an denen Sicherungen virtueller Maschinen gelöscht werden sollen. Sie können einen der folgenden Werte angeben:

SERVER

Sicherungen virtueller Maschinen werden vom IBM Spectrum Protect-Server gelöscht.

LOCAL

Gespeicherte Momentaufnahmen virtueller Maschine werden aus dem Hardwarespeicher gelöscht.

BOTH Sicherungen virtueller Maschinen, die sich auf dem IBM Spectrum Protect-Server befinden, und Momentaufnahmen, die sich im Hardwarespeicher befinden, werden gelöscht. Dies ist der Standardwert.

Bei Angabe dieses Werts wird eine Liste der Sicherungspositionen angezeigt. Aus der Liste können Sie die Position auswählen, an der Sicherungen virtueller Maschinen gelöscht werden sollen.

deltype

Gibt den Löschtyp an. Geben Sie einen der folgenden Werte an:

ACTIVE

Es sollen nur aktive Dateiobjekte gelöscht werden. Verzeichnisobjekte werden nicht gelöscht. Dieser Wert ist der Standardlöschtyp.

Anmerkung: Sind inaktive Objekte vorhanden, nachdem das aktive Objekt gelöscht wurde, wird das aktuellste inaktive Objekt von "inaktiv" in "aktiv" geändert.

Sollen alle Versionen einer Datei gelöscht werden, setzen Sie zunächst den Befehl **delete backup** mit `-deltype=inactive` ab und geben Sie anschließend den Befehl mit `-deltype=active` erneut ein.

INACTIVE

Es sollen nur inaktive Dateiobjekte gelöscht werden. Verzeichnisobjekte werden nicht gelöscht.

ALL

Alle aktiven und inaktiven Objekte unter einem bestimmten Verzeichnis, einschließlich aller Unterverzeichnisse und der darin enthaltenen Dateien, löschen.

Anmerkung: Das übergeordnete Verzeichnis der gelöschten Dateien und Unterverzeichnisse wird nicht gelöscht. Wenn Sie `deltype=ALL` angeben, können Sie nicht die Option `pick` verwenden, da sich `deltype=ALL` und die Option `pick` gegenseitig ausschließen.

Tabelle 89. Befehl Delete Backup: Zugehörige Optionen

Option	Verwendung
description „Description“ auf Seite 397	Nur in der Befehlszeile.
filelist „Filelist“ auf Seite 453	Nur in der Befehlszeile.
fromdate „Fromdate“ auf Seite 461	In der Befehlszeile und in der GUI-Suchfunktion.
fromtime „Fromtime“ auf Seite 463	In der Befehlszeile und in der GUI-Suchfunktion.

Tabelle 89. Befehl Delete Backup: Zugehörige Optionen (Forts.)

Option	Verwendung
noprompt „Noprompt“ auf Seite 519	Nur in der Befehlszeile.
pick „Pick“ auf Seite 528	Nur in der Befehlszeile.
pitdate „Pitdate“ auf Seite 529	In der Befehlszeile und in der GUI-Suchfunktion.
pittime „Pittime“ auf Seite 530	In der Befehlszeile und in der GUI-Suchfunktion.
subdir „Subdir“ auf Seite 605	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
tapeprompt „Tapeprompt“ auf Seite 607	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
timeformat „Timeformat“ auf Seite 616	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
todate „Todate“ auf Seite 621	In der Befehlszeile und in der GUI-Suchfunktion.
totime „Totime“ auf Seite 622	In der Befehlszeile und in der GUI-Suchfunktion.

Beispiele

Task Alle aktiven und inaktiven Dateiobjekte mit dem Namen budget im Verzeichnis /data/plan/proj1 löschen.

Befehle:

```
delete backup /data/plan/proj1/budget.jan
    -deltype=inactive
delete backup /data/plan/proj1/budget.jan
    -deltype=active
```

Task Alle inaktiven Dateien mit der Erweiterung .txt löschen, die im Verzeichnis /data/plan/proj1 und dessen Unterverzeichnissen gesichert wurden.

Befehl: delete backup "/data/plan/proj1/*.txt" -deltype=inactive
-subdir=yes

Task Ausgewählte aktive Dateien löschen, die im Verzeichnis /home/marymb/project gesichert wurden. Verwenden Sie die Option -pick, um eine Liste der Sicherungskopien anzuzeigen, die mit der Dateispezifikation übereinstimmen. Aus der Liste können Sie die zu löschenden Versionen auswählen.

Befehl: delete backup "/home/marymb/project/*" -pick

Task Alle aktiven und inaktiven Versionen von Dateien und Unterverzeichnissen im Verzeichnis /home/storman/myproject löschen. Anschließend alle aktiven und inaktiven Versionen des Verzeichnisses /user/myproject löschen.

Befehl:

```
delete backup "/home/storman/myproject*"
    -deltype=all
```

Zugehörige Verweise:

„Filelist“ auf Seite 453

Delete Filespace

Mit dem Befehl **delete filesystem** können Dateibereiche im IBM Spectrum Protect-Serverspeicher gelöscht werden. Ein Dateibereich ist ein logischer Speicherbereich auf dem Server, der die gesicherten oder archivierten Dateien enthält.

Sie müssen ein berechtigter Benutzer sein, um diesen Befehl verwenden zu können.

IBM Spectrum Protect ordnet jedem Workstationdateisystem, von dem Sie Dateien sichern oder archivieren, einen separaten Dateibereich auf dem Server zu. Der Dateibereichsname entspricht dem Namen des Dateisystems.

Wenn Sie den Befehl **delete filesystem** eingeben, wird eine Liste Ihrer Dateibereiche angezeigt. Wählen Sie aus dieser Liste den Dateibereich aus, der gelöscht werden soll.

Ihr IBM Spectrum Protect-Administrator muss Ihnen die Berechtigung zum Löschen eines Dateibereichs erteilen. Sie benötigen die Berechtigung BACKDEL, wenn der zu löschende Dateibereich Sicherungsversionen enthält, oder die Berechtigung ARCHDEL, wenn der Dateibereich Archivierungskopien enthält. Enthält der Dateibereich sowohl Sicherungsversionen als auch Archivierungskopien, muss der Benutzer über beide Berechtigungen verfügen.

Wichtig: Beim Löschen eines Dateibereichs werden alle Sicherungsversionen und Archivierungskopien innerhalb dieses Dateibereichs gelöscht. Nach dem Löschen eines Dateibereichs **können Sie die Dateien nicht zurückschreiben**. Daher muss vor dem Löschen sichergestellt werden, dass die Dateien nicht mehr benötigt werden.

Mit dem Befehl **delete filesystem** können Sie NAS-Dateibereiche interaktiv aus dem Serverspeicher löschen. Verwenden Sie die Option `nasnodename`, um den NAS-Dateiserver zu identifizieren. Mit der Option `class` können Sie die Klasse des zu löschenden Dateibereichs angeben.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

►► Delete Filespace —Optionen— ►►

Parameter

Tabelle 90. Befehl Delete Filespace: Zugehörige Optionen

Option	Verwendung
<code>class</code> „Class“ auf Seite 374	Nur in der Befehlszeile.
<code>detail</code> „Detail“ auf Seite 398	Nur in der Befehlszeile.
<code>nasnodename</code> „Nasnodename“ auf Seite 515	Clientsystemoptionsdatei oder Befehlszeile.
<code>scrolllines</code> „Scrolllines“ auf Seite 572	Clientsystemoptionsdatei oder Befehlszeile.
<code>scrollprompt</code> „Scrollprompt“ auf Seite 573	Clientsystemoptionsdatei oder Befehlszeile.

Beispiele

Task Einen Dateibereich löschen.

Befehl: delete filespace

Task Auf dem Server gespeicherte NAS-Dateibereiche aus dem NAS-Dateiserver **dagordon** löschen.

Befehl: delete filespace -nasnodename=dagordon -class=nas

Zugehörige Informationen

„Nasnodename“ auf Seite 515

„Class“ auf Seite 374

Delete Group

Verwenden Sie den Befehl **delete group**, um eine Gruppensicherung auf dem IBM Spectrum Protect-Server zu löschen.

Nach dem Löschen einer Gruppe verbleibt das Hauptmember (virtualfsname) auf dem IBM Spectrum Protect-Server. Es enthält keine Member (Dateien oder Verzeichnisse), wird aber in einem nachfolgenden Befehl **query filespace** aufgelistet. Es werden keine Dateien aufgelistet, wenn die Option **showmembers** hinzugefügt wird. Durch das Löschen einer Gruppe wird der Dateibereich, in dem die Gruppe enthalten ist, nicht entfernt, da er noch andere Gruppen enthalten kann. Verwenden Sie **delete filespace**, wenn Sie den Dateibereich und alle darin enthaltenen Daten entfernen wollen.

Anmerkung:

1. Verwenden Sie die Option **inactive**, um sowohl aktive als auch inaktive Gruppensicherungsversionen anzuzeigen. Standardmäßig zeigt der Client aktive Versionen an.
2. Verwenden Sie die Option **pick**, um eine bestimmte Gruppe auszuwählen, die vom IBM Spectrum Protect-Server gelöscht werden soll.
3. Verwenden Sie die Option **noprompt**, um die Bestätigungsaufforderung zu unterdrücken, die normalerweise vor dem Löschen einer Gruppensicherungsversion angezeigt wird. Standardmäßig fordert der Client eine Bestätigung an, bevor die Gruppensicherung gelöscht wird. Mit dieser Option kann die Löschprozedur beschleunigt werden. Die Gefahr, eine Gruppensicherungsversion versehentlich zu löschen, ist hierbei jedoch größer. Diese Option ist mit Vorsicht zu verwenden.
4. Verwenden Sie den Befehl **query filespace**, um Namen der virtuellen Dateibereiche für Ihren Knoten anzuzeigen, die auf dem Server gespeichert sind.

Unterstützte Clients

Dieser Befehl ist für alle UNIX- und Linux-Clients gültig, mit Ausnahme von Mac OS X.

Syntax

►► Delete Group — *Dateispezifikation* — *Optionen* ►►

Parameter

Dateispezifikation

Gibt den Namen des virtuellen Dateibereichs und den Namen der Gruppe an, die Sie aus dem Serverspeicher löschen wollen.

Tabelle 91. Befehl Delete Group: Zugehörige Optionen

Option	Verwendung
inactive „Inactive“ auf Seite 471	Nur in der Befehlszeile.
noprompt „Noprompt“ auf Seite 519	Nur in der Befehlszeile.
pick „Pick“ auf Seite 528	Nur in der Befehlszeile.
pitdate „Pitdate“ auf Seite 529	Nur in der Befehlszeile.
pittime „Pittime“ auf Seite 530	Nur in der Befehlszeile.

Beispiele

Task Die zurzeit aktive Version der Gruppe /virtfs/group1 löschen.

Befehl:

```
delete group /virtfs/group1
```

Task Eine Sicherungsversion der Gruppe /virtfs/group1 aus einer Liste von aktiven und inaktiven Versionen löschen.

Befehl:

```
delete group /virtfs/group1 -inactive -pick
```

Zugehörige Informationen

„Inactive“ auf Seite 471

„Pick“ auf Seite 528

„Noprompt“ auf Seite 519

„Query Filespace“ auf Seite 754

Expire

Mit dem Befehl **expire** werden die Sicherungsobjekte, die Sie in der Dateispezifikation oder mit der Option `filelist` angeben, inaktiviert. Sie können eine einzelne Datei als verfallen definieren oder eine Datei, die eine Liste mit Dateien enthält, die als verfallen definiert werden sollen. Wird `OBJTYPE=VM` angegeben, inaktiviert dieser Befehl die aktuelle Sicherung für eine virtuelle Maschine.

Im interaktiven Modus werden Sie durch eine Bedienerführung informiert, bevor Dateien verfallen.

Der Befehl **expire** entfernt keine Workstationdateien. Wenn eine Datei oder ein Verzeichnis verfällt, die bzw. das auf Ihrer Workstation noch vorhanden ist, wird die Datei bzw. das Verzeichnis während der nächsten Teilsicherung erneut gesichert, sofern Sie das Objekt nicht von der Sicherungsverarbeitung ausschließen.

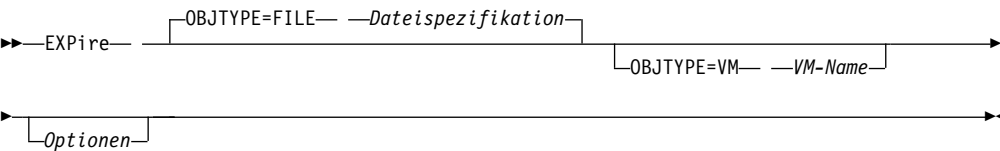
Wenn ein Verzeichnis verfällt, das aktive Dateien enthält, werden diese Dateien bei einer nachfolgenden Abfrage von der GUI nicht angezeigt. Diese Dateien werden jedoch in der Befehlszeile angezeigt, wenn Sie die korrekte Abfrage mit einem Platzhalterzeichen für das Verzeichnis angeben.

Anmerkung: Da der Befehl **expire** das Bild des Servers vom Clientdateisystem ändert, ohne das Clientdateisystem zu ändern, ist der Befehl **expire** für Dateien in einem Dateisystem, das durch den IBM Spectrum Protect-Journaaldämon überwacht wird, nicht zulässig.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax



Parameter

OBJTYPE=FILE Dateispezifikation

Gibt einen Pfad und Dateinamen an, der verfallen soll. Sie können in diesem Befehl nur eine Dateispezifikation eingeben. Sie können jedoch Platzhalterzeichen verwenden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis auszuwählen. Wenn Sie die Option `filelist` angeben, wird der in Dateispezifikation angegebene Name ignoriert.

OBJTYPE=VM VM-Name

VM-Name gibt den Namen einer virtuellen Maschine an. Die aktive Sicherung für die angegebene virtuelle Maschine verfällt. Der Name der virtuellen Maschine darf keine Platzhalterzeichen enthalten.

Wird `objtype=VM` angegeben, verfallen durch den Befehl 'expire' nur VM-Gesamtsicherungen (`MODE=IFFULL`) für die virtuelle Maschine, die im Parameter VM-Name angegeben wird.


 Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Tabelle 92. Befehl Expire: Zugehörige Optionen

Option	Verwendung
<code>dateformat</code> „Dateformat“ auf Seite 389	Clientbenutzeroptionsdatei (<code>dsm.opt</code>) oder Befehlszeile.
<code>filelist</code> „Filelist“ auf Seite 453	Nur in der Befehlszeile.
<code>noprompt</code> „Noprompt“ auf Seite 519	Nur in der Befehlszeile.
<code>numberformat</code> „Numberformat“ auf Seite 521	Clientbenutzeroptionsdatei (<code>dsm.opt</code>) oder Befehlszeile.

Tabelle 92. Befehl *expire*: Zugehörige Optionen (Forts.)

Option	Verwendung
<code>pick</code> „Pick“ auf Seite 528	Nur in der Befehlszeile.
<code>timeformat</code> „Timeformat“ auf Seite 616	Clientbenutzeroptionsdatei (<code>dsm.opt</code>) oder Befehlszeile.

Beispiele

Task Die Datei `letter1.txt` im Verzeichnis `home` inaktivieren.

Befehl: `expire "/home/letter1.txt"`

Task Alle Dateien im Verzeichnis `/admin/mydir` inaktivieren.

Befehl: `expire /admin/mydir/*`

Task Alle Dateien inaktivieren, die in der Datei `/home/avi/filelist.txt` aufgeführt sind.

Befehl: `expire -filelist=/home/avi/filelist.txt`

Help

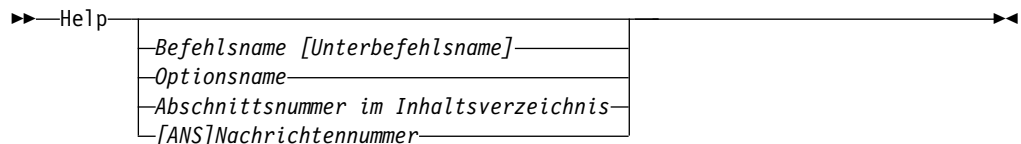
Verwenden Sie den Befehl **help**, um Informationen zu Befehlen, Optionen und Nachrichten anzuzeigen.

Tipp: Wenn Sie den Befehl **help** in der Anfangsbefehlszeile verwenden, wird keine Verbindung zum Server hergestellt und es ist kein Kennwort erforderlich.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax



Wenn Sie den Befehl **help** ohne Argumente eingeben, wird das vollständige Inhaltsverzeichnis angezeigt. Die folgenden Parameter können Sie entweder mit dem ersten Befehl eingeben oder eingeben, wenn **HELP** eine Bedienerführung anzeigt.

Parameter

Befehlsname [Unterbefehlsname]

Gibt einen Befehlsnamen und optional einen Unterbefehlsnamen bzw. die entsprechenden Abkürzungen an, beispielsweise **backup image** oder **b i**. In letzterem Fall muss die Kombination eindeutig sein. Bei nicht eindeutigen Abkürzungen wird der erste Abschnitt der gesamten Hilfedatei angezeigt, die der Abkürzung entspricht. Dieser Parameter ist optional.

Optionsname

Gibt den Namen einer Option an, beispielsweise `domain` oder `do`. Dieser Parameter ist optional.

Abschnittsnummer im Inhaltsverzeichnis

Gibt eine Abschnittsnummer im Inhaltsverzeichnis an, beispielsweise 1.5.3. Dieser Parameter ist optional.

[ANS]Nachrichtenummer

Gibt eine Nachrichtenummer mit oder ohne zugehöriges Präfix an, beispielsweise ans1036 oder 1036. Dieser Parameter ist optional. Der Bewertungscode muss in keinem Fall angegeben werden. Wird ans1036E eingegeben, werden keine Informationen gefunden.

Wichtig: Wenn Sie Argumente eingeben, die diesen Beschreibungen nicht entsprechen, werden möglicherweise unerwartete Ergebnisse (oder keine Ergebnisse) angezeigt. Wenn Sie mehr als zwei Argumente eingeben, wird Ihre Hilfeanforderung zurückgewiesen. Wenn ein Befehlsname und ein Optionsname identisch sind, beispielsweise **incremental** (Befehl) und incremental (Option), können Sie Hilfe zu der Option aufrufen, indem Sie die entsprechende Abschnittsnummer im Inhaltsverzeichnis eingeben.

Der angeforderte Hilfetext wird je nach der Anzahl der Anzeigzeilen in Ihrem Befehlsfenster in einem Abschnitt oder in mehreren Abschnitten angezeigt. Wenn der Anzeigebereich mit Zeilen gefüllt ist oder wenn das Ende des angeforderten Hilfetexts erreicht ist, werden eine Bedienerführung sowie Anweisungen zu den möglichen Eingaben bei der Bedienerführung angezeigt. Soll mit der Anzeige von Text zu Ihrer aktuellen Auswahl fortgefahren werden, drücken Sie die Eingabetaste oder die Taste 'd', um abwärts zu blättern. Um in der aktuellen Auswahl aufwärts zu blättern, drücken Sie die Taste 'u' und drücken die Eingabetaste. Möglicherweise stehen weitere Auswahlmöglichkeiten zur Verfügung; lesen Sie also die angezeigten Anweisungen.

Für eine ordnungsgemäße Anzeige des Hilfetexts ist eine verwendbare Anzeigebreite von 72 Zeichen erforderlich. Eine Anzeigebreite von weniger als 72 Zeichen hat zur Folge, dass Sätze mit einer Breite von 72 Zeichen in der nächsten Zeile fortgesetzt werden. Dies kann dazu führen, dass nicht der Anfang, sondern ein Abschnitt in der Mitte des Hilfetexts angezeigt wird. Die nicht angezeigten Zeilen können mit der Blätterfunktion der Datenstation angezeigt werden.

Beispiele

Task Das Inhaltsverzeichnis der Hilfethemen anzeigen.

Befehl: dsmc help

Task Die Informationen in Hilfethema 2.1.2 anzeigen.

Befehl: dsmc help 2.1.2

Task Hilfeinformationen zum Befehl **archive** anzeigen.

Befehl: dsmc help archive

Task Hilfeinformationen zu der Nachricht ANS1036 anzeigen.

Befehl: dsmc help 1036

Befehl: dsmc help ANS1036

Incremental

Der Befehl **incremental** sichert alle neuen oder geänderten Daten an den Positionen, die Sie angeben, sofern Sie sie nicht von den Sicherungsservices ausschließen.

Sie können alle neuen oder geänderten Dateien oder Verzeichnisse in der Standardclientdomäne oder in Dateisystemen, Verzeichnissen oder Dateien sichern.

Für eine Teilsicherung ausgewählter Dateien oder Verzeichnisse muss die Dateispezifikation im Befehl angegeben werden. Wenn Sie keine Dateispezifikation eingeben, werden standardmäßig Dateien oder Verzeichnisse in der Standarddomäne gesichert.

Nur für AIX: Mit Hilfe der Option `snapshotproviderfs=JFS2` können Sie die Teilsicherung auf Momentaufnahmebasis aktivieren.

Die folgenden Attribute der Verwaltungsklasse, die der Datei oder dem Verzeichnis zugeordnet ist, bestimmen, ob die Daten gesichert werden:

Häufigkeit

Die Anzahl der Tage, die zwischen aufeinanderfolgenden Sicherungen des Objekts vergehen müssen. Das Attribut **Häufigkeit** gilt nur für eine vollständige Teilsicherung.

Dieses Verwaltungsklassenattribut wird während einer journalgestützten Sicherung ignoriert.

Modus

Gibt an, ob sich Änderungen seit der letzten Sicherungsoperation auf die Verarbeitung auswirken. Bei Angabe von `mode=modified` werden nur die Objekte verarbeitet, die sich seit der letzten Sicherungsoperation geändert haben. Bei Angabe von `mode=absolute` wird jedes Objekt verarbeitet, unabhängig davon, ob sich das Objekt seit der letzten Sicherungsoperation geändert hat.

Wenn als Kopiengruppenmodus `modified` definiert ist, kann dieser mithilfe der Clientoption **absolute** außer Kraft gesetzt werden. Weitere Informationen zur Option **absolute** finden Sie in „Absolute“ auf Seite 355.

Durchnummerierung

Ermöglicht oder verhindert die Sicherung von Dateien oder Verzeichnissen gemäß den folgenden Werten:

- **Statisch:** Damit eine Sicherung erfolgt, dürfen Daten während einer Sicherung oder Archivierung nicht geändert werden.
- **Gemeinsam statisch:** Ändern sich die Daten in der Datei oder in dem Verzeichnis während der zulässigen Sicherungs- oder Archivierungsversuche, werden sie nicht gesichert oder archiviert. Der Wert der Option `changingretries` legt fest, wie viele Versuche unternommen werden. Der Standardwert ist 4.
- **Dynamisch:** Das Objekt wird beim ersten Versuch gesichert oder archiviert, auch wenn sich die Daten während der Verarbeitung ändern.
- **Gemeinsam dynamisch:** Das Objekt wird beim letzten Versuch gesichert oder archiviert, auch wenn sich die Daten während der Verarbeitung ändern.

Mit Hilfe der Option **include** können Sie in einer Einschluss-/Ausschlussliste die Standardverwaltungsklasse für eine Datei oder eine Gruppe von Dateien überschreiben.

Es kann eine vollständige Teilsicherung oder eine Teilsicherung nach Datum ausgeführt werden. Standardwert ist eine vollständige Teilsicherung.

Wenn Sie für ein Dateisystem die Journalführung verwenden und das Journal gültig ist, wird bei der vollständigen Teilsicherung eine journalgestützte Sicherung ausgeführt. Es können mehrere journalgestützte Sicherungssitzungen gestartet werden, aber nur eine journalgestützte Sicherungssitzung kann fortgesetzt werden. Alle anderen journalgestützten Sicherungssitzungen, die auf denselben Dateibereich zugreifen müssen, müssen warten, bis die aktuelle journalgestützte Sicherungssitzung beendet ist, bevor die nächste Sitzung fortgesetzt werden kann. Sie können eine vollständige Teilsicherung ohne Journal ausführen, indem Sie die Option **nojournal** verwenden.

Mit dem Befehl **selective** kann auch eine selektive Sicherung ausgeführt werden, bei der nur die von Ihnen angegebenen Dateien, Verzeichnisse oder leeren Verzeichnisse gesichert werden, unabhängig davon, ob sie sich geändert haben.

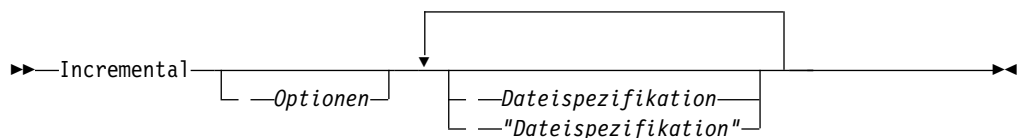
Bei einer vollständigen Teilsicherung werden alle neuen Dateien und Verzeichnisse sowie Dateien und Verzeichnisse, die sich seit der letzten Teilsicherung geändert haben, gesichert. Während einer vollständigen Teilsicherung fragt der Client den Server ab. IBM Spectrum Protect verwendet diese Informationen, wenn folgende Aktionen ausgeführt werden:

- Neue Dateien oder Verzeichnisse sichern.
- Dateien oder Verzeichnisse sichern, deren Inhalt sich seit der letzten Sicherung geändert hat.
- Sicherungsversionen auf dem Server für Dateien oder Verzeichnisse, die aus der Workstation gelöscht wurden, als inaktiv markieren.
- Sicherungsversionen erneut an Verwaltungsklassen binden, wenn sich die Zuordnung der Verwaltungsklassen ändert.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax



Parameter

Dateispezifikation

Gibt den Pfad und den Namen der Datei an, die gesichert werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis auszuwählen. Wenn Sie keine Dateispezifikation angeben, bestimmt die Option **domain**, was gesichert wird.

Wenn Sie ein Dateisystem angeben, werden alle neuen und geänderten Dateien gesichert. Zusätzlich wird auf dem Server das Datum der letzten Teilsicherung des Dateibereichs aktualisiert. Wenn Sie eine Datei oder ein Verzeichnis angeben, wird das Datum der letzten Teilsicherung nicht aktualisiert. Dies bedeutet, dass die Datei oder das Verzeichnis möglicherweise erneut gesichert wird, wenn eine spätere Sicherung mit der Option **incrbydate** durchgeführt wird. Bei der Angabe eines Dateisystems müssen Sie das Dateisystem ohne abschließenden Schrägstrich angeben.

Tabelle 93. Befehl *Incremental*: Zugehörige Optionen

Option	Verwendung
absolute „Absolute“ auf Seite 355	Nur in der Befehlszeile.
changingretries „Changingretries“ auf Seite 373	Datei dsm.sys oder Befehlszeile.
compressalways „Compressalways“ auf Seite 379	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
compression „Compression“ auf Seite 380	Datei dsm.sys innerhalb einer Serverzeilengruppe oder Befehlszeile.
detail „Detail“ auf Seite 398	Nur in der Befehlszeile.
diffsnapshot „Diffsnapshot“ auf Seite 400	Nur in der Befehlszeile.
dirsonly „Dirsonly“ auf Seite 403	Nur in der Befehlszeile.
domain „Domain“ auf Seite 407	Datei dsm.sys, Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
encryptiontype „Encryptiontype“ auf Seite 431	Systemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe.
encryptkey „Encryptkey“ auf Seite 431	Systemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe.
filelist „Filelist“ auf Seite 453	Nur in der Befehlszeile.
filesonly „Filesonly“ auf Seite 457	Nur in der Befehlszeile.
incrbydate „Incrbydate“ auf Seite 490	Nur in der Befehlszeile.
memoryefficientbackup „Memoryefficientbackup“ auf Seite 507	Clientbenutzeroptionsdatei (dsm.opt), Clientsystemoptionsdatei (dsm.sys), Server oder Befehlszeile.
nojournal „Nojournal“ auf Seite 519	Nur in der Befehlszeile.
preserverlastaccessdate „Preserverlastaccessdate“ auf Seite 536	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
removeoperandlimit „Removeoperandlimit“ auf Seite 546	Nur in der Befehlszeile.
snapdiff „Snapdiff“ auf Seite 581	Nur in der Befehlszeile.
snapshotcachesize „Snapshotcachesize“ auf Seite 590	Clientoptionsdatei (dsm.opt) oder mit der Option include.fs .
snapshotproviderfs „Snapshotproviderfs“ auf Seite 591	Systemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe oder mit der Option include.fs .
snapshotroot „Snapshotroot“ auf Seite 593	Nur in der Befehlszeile.
subdir „Subdir“ auf Seite 605	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
tapeprompt „Tapeprompt“ auf Seite 607	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.

Beispiele

Task Eine Teilsicherung der Clientdomäne ausführen, die in Ihrer Clientbenutzeroptionsdatei (dsm.opt) angegeben ist.

```
Incremental
```

Eine Teilsicherung ausführen, bei der alle Dateien in der Domäne gesichert werden, unabhängig davon, ob sie sich seit der letzten Sicherung geändert haben.

`Incremental -absolute`

Task Eine Teilsicherung für die Dateisysteme /home, /usr und /proj ausführen.

`Incremental /home /usr /proj`

Task Eine Teilsicherung für das Verzeichnis /proj/test ausführen.

`Incremental /proj/test/`

Task Eine Teilsicherung nach Datum für das Dateisystem /home ausführen.

`Incremental -incrbydate /home`

Task Eine Teilsicherung der Datei abc im Verzeichnis /fs/dir1 ausführen.

`Incremental -subdir=yes /fs/dir1/abc`

Task Eine Teilsicherung des Verzeichnisobjekts /fs/dir1, aber nicht für die Dateien im Verzeichnis /fs/dir1 ausführen.

`Incremental /fs/dir1`

Task Eine Teilsicherung des Verzeichnisobjekts /fs/dir1, aller Dateien im Verzeichnis /fs/dir1 und aller Dateien und Unterverzeichnisse unter /fs/dir1 ausführen.

`Incremental -subdir=yes /fs/dir1/`

Task Angenommen, Sie haben eine Momentaufnahme des Dateisystems /usr gestartet und die Momentaufnahme als /snapshot/day1 angehängt. Führen Sie eine Teilsicherung aller Dateien und Verzeichnisse unter der lokalen Momentaufnahme aus und verwalten Sie sie auf dem IBM Spectrum Protect-Server unter dem Dateibereichsnamen /usr.

`dsmc inc /usr -snapshotroot=/snapshot/day1`

Task Eine Teilsicherung des Dateisystems /home unter Verwendung der Option **snappdiff** ausführen und die Option zum Erstellen der Differenzmomentaufnahme angeben. Im folgenden Beispiel ist /home der NFS-Mountpunkt für den Datenträger eines NAS/N-Series-Dateiservers.

`incremental /home -snappdiff -diffsnapshot=create`

Task Eine Teilsicherung des Dateisystems /proj unter Verwendung der Option **snappdiff** ausführen. Die Option zum Verwenden der letzten Momentaufnahme auf dem Dateiserver als Differenzmomentaufnahme angeben. Im folgenden Beispiel ist /proj der NFS-Mountpunkt für den Datenträger eines NAS/N-Series-Dateiservers.

`incremental /proj -snappdiff -diffsnapshot=latest`

Zugehörige Informationen

„Absolute“ auf Seite 355

„Journalgestützte Sicherung“ auf Seite 737

„Selective“ auf Seite 810

„Include-Optionen“ auf Seite 473

Journalgestützte Sicherung

Eine Sicherung für ein bestimmtes Dateisystem ist journalgestützt, wenn der IBM Spectrum Protect-Journaldämon installiert und zum Aufzeichnen des Dateisystems konfiguriert ist und ein gültiges Journal erstellt wurde.

Die journalgestützte Sicherung wird auf dem AIX-Client für Sichern/Archivieren auf JFS- und JFS2-Dateisystemen unterstützt.

Die journalgestützte Sicherung wird auf dem Linux-Client für Sichern/Archivieren für Ext2, Ext3, Ext4, XFS, ReiserFS, JFS, VxFS und NSS unterstützt. GPFS wird für journalgestützte Sicherungen unter Linux nicht unterstützt.

Wenn der Journaldämon installiert und aktiv ist, führt der Befehl **incremental** standardmäßig eine journalgestützte Sicherung für Dateisysteme aus, die vom Dämon der Journalsteuerkomponente überwacht werden. Die folgenden Bedingungen müssen erfüllt sein, damit eine journalgestützte Sicherung erfolgreich ausgeführt werden kann:

- Der Journaldämon muss zum Überwachen des Dateisystems konfiguriert sein, das die Dateien und Verzeichnisse enthält, die gesichert werden.
- Für das Dateisystem, das gesichert wird, muss mindestens eine erfolgreiche vollständige Teilsicherung ausgeführt worden sein.
- Das Dateibereichimage des Dateisystems auf dem Server darf nach der letzten vollständigen Teilsicherung nicht durch einen Verwaltungsbefehl geändert worden sein.
- Die Speicherverwaltungsmaßnahme für die Dateien, die gesichert werden, darf nach der letzten vollständigen Teilsicherung nicht aktualisiert worden sein.

Der Journaldämon zeichnet Änderungen an einem Objekt oder seinen Attributen in einer Journaldatenbank auf. Während einer journalgestützten Sicherung ruft der Client eine Liste der Dateien, die für eine Sicherung ausgewählt werden können, aus der Journaldatenbank ab. Die journalgestützte Sicherung kann die Leistung beim Sichern verbessern, da der Client nicht das lokale Dateisystem durchsuchen oder den Server kontaktieren muss, um festzustellen, welche Dateien verarbeitet werden müssen. Die journalgestützte Sicherung verringert auch den Datenaustausch im Netz zwischen dem Client und dem Server.

Der Client für Sichern/Archivieren filtert die Liste auf der Basis der aktuellen Einschluss-/Ausschlussliste und verarbeitet und aktualisiert die Ergebnisdateien gemäß Maßnahmenvorgaben, wie z. B. der Serialisierung, und lässt sie gemäß dieser Vorgaben verfallen. Der Client ignoriert jedoch das Häufigkeitsattribut des Servers während einer journalgestützten Sicherung. Der Grund hierfür ist, dass eine journalgestützte Sicherung die Abfrage der Sicherungsversion beim Server überflüssig macht; daher weiß der Client nicht, wie viele Tage seit der letzten Sicherung der Datei vergangen sind.

Der Journaldämon zeichnet keine Änderungen in speziellen UNIX-Dateien auf.

Der Journaldämon schließt bestimmte Dateien von der Aufzeichnung ihrer Änderungen im Journal aus. Da Änderungen dieser Dateien nicht im Journal aufgezeichnet werden, werden diese Dateien vom Client nicht gesichert. Suchen Sie in der Konfigurationsdatei des Journaldämons, `tsmjbbd.ini`, im Installationsverzeichnis des Clients für Sichern/Archivieren nach bestimmten ausgeschlossenen Systemdateien.

Anmerkung:

1. Wird Antivirensoftware verwendet, unterliegt die journalgestützte Sicherung gewissen Einschränkungen. Bestimmte Antivirensoftware kann fälschlicherweise Änderungsbenachrichtigungen für den IBM Spectrum Protect-JournalSERVICE generieren. Dies hat zur Folge, dass Dateien, die sich nicht geändert haben, bei einer journalbasierten Sicherung fälschlicherweise gesichert werden. Verwenden Sie Norton Anti-Virus Corporate Edition 8.0 oder höher, um diese Probleme zu vermeiden.
2. Eine journalgestützte Sicherung wird möglicherweise nicht wieder durch die traditionelle Teilsicherung ersetzt, wenn die Maßnahmendomäne Ihres Knotens auf dem Server geändert wird. Dies ist vom Zeitpunkt der letzten Aktualisierung der Maßnahmengruppe in der Domäne und vom Datum der letzten Teilsicherung abhängig. In diesem Fall müssen Sie eine traditionelle vollständige Teilsicherung erzwingen, um die Dateien erneut an die neue Domäne zu binden. Verwenden Sie die Option `nojournal` im Befehl **incremental**, um anzugeben, dass statt der standardmäßigen journalgestützten Sicherung eine traditionelle vollständige Teilsicherung ausgeführt werden soll.

Fügen Sie unter AIX 6.1 oder höher der Datei `tsmjbbd.ini` eine Anweisung `exclude snapshot` hinzu, um zu vermeiden, dass interne JFS2-Momentaufnahmeverzeichnisse vom journalgestützten Sicherungsdaemon überwacht werden. Wenn Sie die Momentaufnahmeverzeichnisse nicht ausschließen, werden die darin enthaltenen Dateien gesichert. Die Sicherung der Momentaufnahmeverzeichnisse ist eine redundante Sicherung, mit der Serverspeicherbereich verschwendet wird.

Unter den folgenden Bedingungen wird die Journaldatenbank als ungültig betrachtet und der Client kehrt zur traditionellen vollständigen Teilsicherung zurück:

- Der Name eines Journaldateibereichs wurde geändert.
- Der Name des Clientknotens wurde geändert.
- Der Client nimmt Kontakt zu einem anderen Server auf, um die Sicherung durchzuführen.
- Es sind Maßnahmenänderungen aufgetreten (Aktivierung einer neuen Maßnahmengruppe).
- Das Journal ist beschädigt (Bedingungen 'Kein Speicher mehr', Plattenfehler).
- Das Journal ist nicht aktiv.

Die journalgestützte Sicherung unterscheidet sich von der traditionellen vollständigen Teilsicherung auf folgende Weise:

- IBM Spectrum Protect erzwingt keine nicht standardmäßigen Kopienhäufigkeiten (außer 0).
- Änderungen in speziellen UNIX-Dateien werden nicht festgestellt.

Sie können die Option `nojournal` im Befehl **incremental** verwenden, um anstelle der standardmäßigen journalgestützten Sicherung eine traditionelle vollständige Teilsicherung auszuführen.

Teilsicherung nach Datum

Bei einer Teilsicherung nach Datum werden neue und geänderte Dateien mit einem Änderungsdatum gesichert, das nach dem Datum der letzten auf dem Server gespeicherten Teilsicherung liegt, sofern die Dateien nicht durch eine **Exclude**-Anweisung von der Sicherung ausgeschlossen sind.

Wird eine Teilsicherung nach Datum nur für einen Teil eines Dateisystems ausgeführt, wird das Datum der letzten vollständigen Teilsicherung nicht aktualisiert; bei der nächsten Teilsicherung nach Datum werden die Dateien dann wieder gesichert.

Änderungen der Zugriffssteuerungslisten (ACL) oder der erweiterten Attribute bewirken nicht, dass die Dateien während einer Teilsicherung nach Datum gesichert werden. Das Datum und die Zeit der letzten Teilsicherung des gesamten Dateisystems können mit dem Befehl **query filespace** bestimmt werden.

Für eine Teilsicherung nach Datum geben Sie die Option **incrbydate** im Befehl **incremental** an.

Anders als eine vollständige Teilsicherung hält die Teilsicherung nach Datum den Serverspeicher nicht auf dem aktuellen Stand *aller* Workstationdateien, weil:

- Sicherungsversionen von Dateien, die aus der Workstation gelöscht wurden, hierbei nicht verfallen.
- Sicherungsversionen nicht erneut an eine neue Verwaltungsklasse gebunden werden, wenn sich die Verwaltungsklasse geändert hat.
- Dateien mit geänderten Attributen nur dann gesichert werden, wenn sich auch das Änderungsdatum und die Änderungszeit geändert haben.
- Das Attribut 'Häufigkeit' der Kopiengruppe in den Verwaltungsklassen ignoriert wird.

Aus diesen Gründen sollten bei Zeitmangel für die Ausführung von Sicherungen während der Woche Teilsicherungen nach Datum ausgeführt werden. Am Wochenende, wenn mehr Zeit zur Verfügung steht, kann dann eine vollständige Teilsicherung erfolgen, um den Serverspeicher auf den aktuellen Stand Ihrer Workstationdateien zu bringen.

Wenn der Befehl **incremental** wegen eines Übertragungs- oder Sitzungsfehlers wiederholt wird, zeigen die Übertragungsstatistiken die Anzahl Bytes an, die der Client während aller Befehlswiederholungen zu übertragen versucht hat. Daher entsprechen die Statistiken für die übertragenen Bytes möglicherweise nicht den Dateistatistiken, z. B. für die Dateigröße.

Lokale Momentaufnahme einem Serverdateibereich zuordnen

Wenn Sie eine Anwendung eines anderen Anbieters zur Erstellung einer Momentaufnahme eines logischen Datenträgers benutzen, verwenden Sie die Option **snapshotroot** im Befehl **incremental**, um die Daten der lokalen Momentaufnahme den originalen Dateibereichsdaten zuzuordnen, die auf dem IBM Spectrum Protect-Server gespeichert sind.

Die Option **snapshotroot** bietet keine Funktionen zur Erstellung einer Datenträgermomentaufnahme, sondern ausschließlich Funktionen zur Verwaltung von Daten, die durch Erstellen einer Datenträgermomentaufnahme generiert werden.

Loop

Der Befehl **loop** startet eine interaktive Befehlszeilensitzung, die aktiv ist, bis Sie **quit** eingeben.

Wenn für Sie ein Kennwort erforderlich ist, werden Sie zur Eingabe dieses Kennworts aufgefordert, bevor die Eingabeaufforderung für den Schleifenmodus angezeigt wird.

Anmerkung: Es ist nicht möglich, den Schleifenmodus zu aktivieren, ohne dass eine Verbindung zu einem gültigen Server besteht. Eine der Folgen dieses Sachver-

halts ist, dass bestimmte Befehle wie beispielsweise `restore backupset -location=file` nur dann in der Anfangsbefehlszeile akzeptiert werden, wenn ein gültiger Server nicht verfügbar ist.

Bei einer interaktiven Befehlszeilensitzung müssen Sie den einzelnen Befehlsnamen nicht die Zeichenfolge **dsmc** und das Kennwort (falls ein Kennwort erforderlich ist) voranstellen.

Im interaktiven Modus überschreiben die Optionen, die Sie in der Anfangsbefehlszeile eingeben, den Wert, den Sie in Ihrer Clientbenutzeroptionsdatei (`dsm.opt`) oder in der Datei `dsm.sys` angegeben haben. Dieser Wert bleibt für die gesamte interaktive Sitzung aktiv, solange er nicht durch einen anderen Wert in einem angegebenen interaktiven Befehl überschrieben wird. Beispiel: Wenn Sie die Option `subdir` in Ihrer Clientbenutzeroptionsdatei (`dsm.opt`) auf *yes* setzen und in der Anfangsbefehlszeile `subdir=no` angeben, bleibt die Einstellung `subdir=no` während der gesamten interaktiven Sitzung aktiv, wenn sie nicht durch den Wert `subdir=yes` in einem angegebenen interaktiven Befehl überschrieben wird. Der Wert `subdir=yes` betrifft jedoch nur den Befehl, in dem er eingegeben wird. Wenn dieser Befehl beendet ist, wird der Wert auf `subdir=no` zurückgesetzt, d. h. auf den Wert, den die Option zu Beginn der interaktiven Sitzung hatte.

Sie können alle gültigen Befehle im interaktiven Modus eingeben, *mit Ausnahme* der Befehle **schedule** und **loop**.

Einige Optionen können Sie in der vom Befehl **loop** erstellten interaktiven Sitzung nicht verwenden; diese werden in der Optionsbeschreibung durch die folgende Anweisung identifiziert: *Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktiven Modus ist sie nicht gültig.*

Anmerkung:

1. Im Schleifenmodus wird der Mountpunkt nach einer Zurückschreibungsoperation direkt vom Band nicht freigegeben, falls weitere Zurückschreibungsanforderungen an den Datenträger gestellt werden. Wenn Sie eine Sicherungsoperation in derselben Sitzung anfordern und dieser Mountpunkt der einzig verfügbare ist, stoppt die Sicherungsoperation mit der folgenden Nachricht:

Auf Laden von Offlinedatenträger warten

In diesem Fall wird der Mountpunkt erst freigegeben, wenn eine der folgenden Bedingungen erfüllt ist:

- Der Grenzwert der Einheitenklasse MOUNTRETENTION ist erreicht.
 - Das Clientinaktivitätszeitlimit ist erreicht.
 - Die Sitzung `dsmc loop` wird geschlossen, nachdem die Zurückschreibungsoperation beendet ist. Dies ermöglicht Ihnen den Start einer nachfolgenden Sitzung im Schleifenmodus, um die Sicherungsoperation auszuführen.
2. Im interaktiven Modus können Sie keine Dateispezifikation eingeben, die Sonderzeichen in der Landessprache enthält. Wenn ein Befehl nationale Sonderzeichen enthält, müssen Sie ihn im Stapelbetrieb verarbeiten, indem Sie dem Befehl den Namen des ausführbaren Programms **dsmc** voranstellen.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

►—LOOP—◄

Parameter

Für diesen Befehl gibt es keine Parameter.

Beispiele

Task Eine interaktive Befehlszeilensitzung starten.

Befehl: `dsmc`

Geben Sie bei der Eingabeaufforderung `Protect>` einen Befehl ein.

Es gibt zwei Methoden zum Beenden einer interaktiven Sitzung:

- Geben Sie `quit` ein.
- Wenn Sie `editor=yes` definiert haben, können Sie wie folgt vorgehen:
 1. Drücken Sie die Abbruchtaste (Esc).
 2. Geben Sie `Q` ein und drücken Sie die Eingabetaste.

Anmerkung: Die Standardeinstellung ist `editor=yes`.

Anmerkung: Soll ein `dsmc`-Befehl abgebrochen werden, bevor die Clientverarbeitung abgeschlossen ist, geben Sie **QQ** an der IBM Spectrum Protect-Konsole ein. In vielen Fällen, jedoch nicht in allen Fällen, wird der Befehl dadurch abgebrochen.

Zugehörige Informationen

Kapitel 10, „Verarbeitungsoptionen“, auf Seite 323 enthält Informationen zu Optionen, die Sie im interaktiven Modus nicht verwenden können.

Macro

Der Befehl **macro** führt eine Serie von Befehlen aus, die Sie in einer Makrodatei angeben.

Wenn Sie den Befehl **macro** in einer Makrodatei angeben, können Sie bis zu 10 Befehlsebenen verschachteln.

Kommentarzeilen werden innerhalb der Makrodatei, die Sie für den Befehl **macro** angeben, nicht unterstützt.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

►—Macro— *Makroname* —◄

Parameter

Makroname

Gibt den vollständig qualifizierten Namen der Datei an, in der sich die Befehle befinden.

Beispiele

Das folgende Beispiel zeigt die Verwendung des Befehls **macro**.

Task Dateien in den folgenden Verzeichnissen selektiv sichern:

- /devel/project/proja
- /devel/project/projb
- /devel/project/projc

Befehl: macro backabc.mac

Dabei enthält backabc.mac die folgenden Anweisungen:

```
Selective /devel/project/proja/  
Selective /devel/project/projb/  
Selective /devel/project/projc/
```

Monitor Process

Der Befehl **monitor process** zeigt (sofern die NDMP-Unterstützung aktiviert ist) eine Liste der aktuellen NAS-Imagesicherungs- und -zurückschreibungsprozesse an, für die der Benutzer mit Verwaltungsaufgaben die Berechtigung hat. Sie werden zur Eingabe der IBM Spectrum Protect-Administrator-ID aufgefordert.

Der Benutzer mit Verwaltungsaufgaben kann dann einen Prozess für die Überwachung auswählen. Die Clienteneignerberechtigung ist als Berechtigung ausreichend, um die ausgewählten NAS-Imagesicherungs- oder -zurückschreibungsprozesse zu überwachen.

Unterstützte Clients

Dieser Befehl ist nur für AIX-, Linux- und Solaris-Clients gültig.

Syntax

►►—MONitor Process—◄◄

Parameter

Für diesen Befehl gibt es keine Parameter.

Beispiele

Task Die aktuellen NAS-Imagesicherungs- oder -zurückschreibungsprozesse überwachen.

Befehl: monitor process

Preview Archive

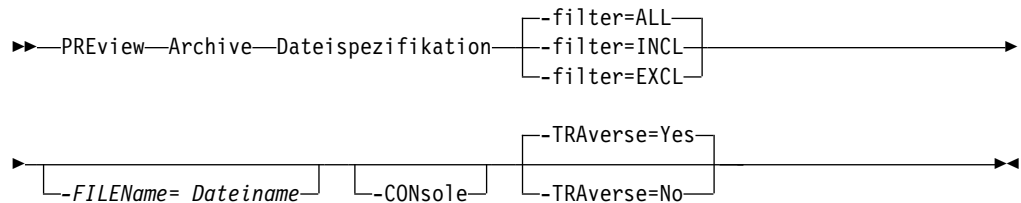
Der Befehl **preview archive** simuliert einen Archivierungsbefehl, ohne Daten an den Server zu senden.

Der Befehl **preview archive** generiert eine tabulatorbegrenzte Textdatei, die in ein Tabellenkalkulationsprogramm importiert werden kann. Die Voranzeige enthält Informationen wie z. B., ob die Datei ausgeschlossen oder eingeschlossen ist. Ist die Datei ausgeschlossen, wird das Muster oder die Ursache für den Ausschluss der Datei zusammen mit der Quelle für das Muster aufgeführt.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax



Parameter

Dateispezifikation

Gibt den Pfad und den Namen der Datei an, die archiviert werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis auszuwählen.

-filter Gibt die anzuzeigende Ausgabe an. Sie können eingeschlossene Objekte, ausgeschlossene Objekte oder beides anzeigen.

ALL Ausgabe für eingeschlossene und ausgeschlossene Objekte anzeigen. Dies ist der Standardwert.

INCLuded

Nur Ausgabe für eingeschlossene Objekte anzeigen.

EXCLuded

Nur Ausgabe für ausgeschlossene Objekte anzeigen.

-FILENAME=

Gibt den Namen der Datei an, in die die durch Tabulatoren getrennte Ausgabe geschrieben werden soll. Der Standardwert ist dsmprev.txt.

-CONsole

Die Ausgabe wird auf die Konsole und in die Datei geschrieben.

-TRAverse

Die Voranzeige für die aktuellen Verzeichnisse und ihre Unterverzeichnisse anzeigen.

Yes Die Voranzeige für die aktuellen Verzeichnisse und ihre Unterverzeichnisse anzeigen. Dies ist der Standardwert.

No Die Voranzeige nur für die aktuellen Verzeichnisse und nicht für ihre Unterverzeichnisse anzeigen.

Wichtig: Bei der Angabe von **-traverse** wird keine Voranzeige für Verzeichnisse angezeigt, die mit der Option `exclude.dir` ausgeschlossen wurden.

Preview Backup

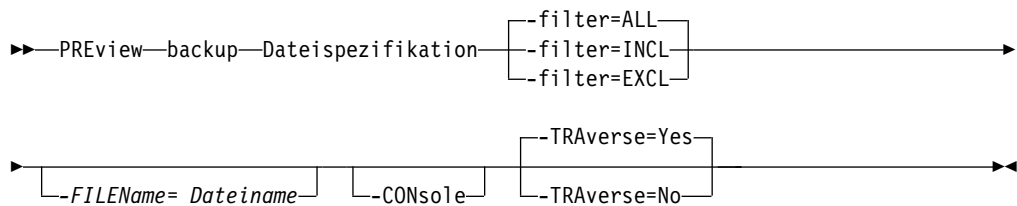
Der Befehl **preview backup** simuliert einen Sicherungsbefehl, ohne Daten an den Server zu senden.

Der Befehl **preview backup** generiert eine tabulatorbegrenzte Textdatei, die in ein Tabellenkalkulationsprogramm importiert werden kann. Die Voranzeige enthält Informationen wie z. B., ob die Datei ausgeschlossen oder eingeschlossen ist. Ist die Datei ausgeschlossen, wird das Muster oder die Ursache für den Ausschluss der Datei zusammen mit der Quelle für das Muster aufgeführt.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax



Parameter

Dateispezifikation

Gibt den Pfad und den Namen der Datei an, die gesichert werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis auszuwählen.

-filter Gibt die anzuzeigende Ausgabe an. Sie können eingeschlossene Objekte, ausgeschlossene Objekte oder beides anzeigen.

ALL Ausgabe für eingeschlossene und ausgeschlossene Objekte anzeigen. Dies ist der Standardwert.

INCLuded

Nur Ausgabe für eingeschlossene Objekte anzeigen.

EXCLuded

Nur Ausgabe für ausgeschlossene Objekte anzeigen.

-FILENAME=

Gibt den Namen der Datei an, in die die durch Tabulatoren getrennte Ausgabe geschrieben werden soll. Der Standardwert ist `dsmprev.txt`.

-CONSOLE

Die Ausgabe wird auf die Konsole und in die Datei geschrieben.

-TRaverse

Die Voranzeige für die aktuellen Verzeichnisse und ihre Unterverzeichnisse anzeigen.

Yes Die Voranzeige für die aktuellen Verzeichnisse und ihre Unterverzeichnisse anzeigen. Dies ist der Standardwert.

No Die Voranzeige nur für die aktuellen Verzeichnisse und nicht für ihre Unterverzeichnisse anzeigen.

Wichtig: Bei der Angabe von **-traverse** wird keine Voranzeige für Verzeichnisse angezeigt, die mit der Option `exclude.dir` ausgeschlossen wurden.

Query Access

Der Befehl **query access** zeigt an, welchen Benutzern Zugriff auf Sicherungsversionen und Archivierungskopien bestimmter Dateien erteilt wurde.

Der Client für Sichern/Archivieren zeigt eine Liste der Berechtigungsregeln an, die Sie mit dem Befehl **set access** oder über die Menüoption **Dienstprogramme > Knotenzugriffsliste** in der grafischen Benutzerschnittstelle (Graphical User Interface, GUI) des Clients für Sichern/Archivieren definiert haben.

Die folgenden Informationen sind enthalten.

- Die einem Benutzer erteilte Berechtigung zum Zurückschreiben von Sicherungsversionen oder zum Abrufen von Archivierungskopien.
- Der Knotenname des Benutzers, dem die Berechtigung erteilt wurde.
- Die ID des Benutzers auf dem Knoten, dem die Berechtigung erteilt wurde.
- Die Dateien, auf die der Benutzer Zugriff hat.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

►—Query Access—◄

Parameter

Für diesen Befehl gibt es keine Parameter.

Beispiele

Task Eine Liste der Benutzer anzeigen, die Zugriff auf Ihre Dateien haben.

Befehl: `query access`

Query Archive

Der Befehl **query archive** zeigt eine Liste Ihrer archivierten Dateien und folgende Informationen zu jeder Datei an: Dateigröße, Archivierungsdatum, Dateispezifikation, Verfallsdatum und Archivierungsbeschreibung.

Wenn Sie die Option `detail` im Befehl **query archive** verwenden, zeigt der Client die folgenden zusätzlichen Informationen an:

- Datum der letzten Änderung
- Datum des letzten Zugriffs
- Letztes Änderungsdatum der Dateiattribute (Dateiindex)
- Komprimierungstyp
- Verschlüsselungstyp
- Clientseitige Deduplizierung von Daten
- Initiierung des Aufbewahrungszeitraums
- Ob die Datei gesperrt ist
- Größe der ACL-Metadaten (IBM Spectrum Scale) für AIX- und Linux-Clients

- Serverspeicherinformationen (Datenträgerklasse, Datenträger-ID und Zurückschreibungsreihenfolge) für AIX- und Linux-Clients

Das folgende Beispiel zeigt Beispielausgaben, wenn der Befehl **query archive** mit der Option **detail** ausgegeben wird:

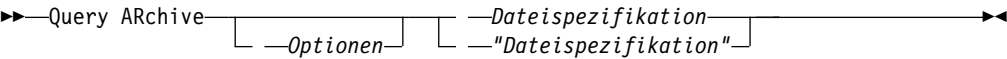
```
Größe Archiv.-Datum/-Zeit   Datei - Verfällt am - Beschreibung
-----
219 B 08/15/2016 09:32:13 /Volumes/Data/info.txt 08/16/2016
Archivierungsdatum: 08/16/2016
RetInit:STARTED Obj
Held:NO
Geändert: 03/02/2016 19:43:00 Zugriffen: 03/03/2016 09:31:23 Dateindex geändert: 03/02/2016 19:43:00
Komprimierungstyp: LZ4 Verschlüsselungstyp: None Vom Client dedupliziert: YES
ACL-Größe: 0 Datenträgerklasse: Fest Datenträger-ID: 0008 Zurückschreibungsreihenfolge: 00000000-0000001F-00000000-00000000
```

Weitere Informationen zum Komprimierungstyp finden Sie in „Compression“ auf Seite 380.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax



Parameter

Dateispezifikation

Gibt den Pfad und den Namen der Datei an, die abgefragt werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis anzugeben. Werden Platzhalterzeichen verwendet, muss die Dateispezifikation in Anführungszeichen eingeschlossen werden. Durch Eingabe eines Sterns (*) können alle archivierten Dateien im aktuellen Verzeichnis abgefragt werden.

Tabelle 94. Befehl 'Query Archive': Zugehörige Optionen

Option	Verwendung
dateformat „Dateformat“ auf Seite 389	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
description „Description“ auf Seite 397	Nur in der Befehlszeile.
detail „Detail“ auf Seite 398	Nur in der Befehlszeile.
dirsonly „Dirsonly“ auf Seite 403	Nur in der Befehlszeile.
filelist „Filelist“ auf Seite 453	Nur in der Befehlszeile.
filesonly „Filesonly“ auf Seite 457	Nur in der Befehlszeile.
fromdate „Fromdate“ auf Seite 461	Nur in der Befehlszeile.
fromnode „Fromnode“ auf Seite 461	Nur in der Befehlszeile.

Tabelle 94. Befehl 'Query Archive': Zugehörige Optionen (Forts.)

Option	Verwendung
fromowner „Fromowner“ auf Seite 462	Nur in der Befehlszeile.
fromtime „Fromtime“ auf Seite 463	Nur in der Befehlszeile.
numberformat „Numberformat“ auf Seite 521	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
querysummary „Querysummary“ auf Seite 542	Nur in der Befehlszeile.
scrolllines „Scrolllines“ auf Seite 572	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
scrollprompt „Scrollprompt“ auf Seite 573	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
subdir „Subdir“ auf Seite 605	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
timeformat „Timeformat“ auf Seite 616	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
todate „Todate“ auf Seite 621	Nur in der Befehlszeile.
totime „Totime“ auf Seite 622	Nur in der Befehlszeile.

Beispiele

Task Eine Liste aller archivierten Dateien im aktuellen Arbeitsverzeichnis anzeigen.

Befehl: q archive "*"

Task Eine Liste aller archivierten Dateien im Verzeichnis /devel und in allen zugehörigen Unterverzeichnissen anzeigen.

Befehl: query archive "/devel/*" -subdir=yes

Task Eine Liste aller archivierten Dateien im aktuellen Verzeichnis anzeigen. Die Datums- und Zeitformate mithilfe der Optionen dateformat und timeformat neu formatieren.

Befehl: q ar -date=5 -time=1 "*"

Task Eine Liste aller archivierten Dateien im aktuellen Verzeichnis anzeigen. Die Option detail verwenden, um das Datum der letzten Änderung und das Datum des letzten Zugriffs jeder Datei anzuzeigen.

Befehl: q ar -detail "*"

Task Eine Liste der archivierten Dateien im Verzeichnis /home/proj anzeigen, deren Dateiname mit den vier Zeichen proj beginnt.

Befehl: q ar "/home/proj/proj*"

Query Backup

Der Befehl **query backup** zeigt eine Liste der Sicherungsversionen Ihrer Dateien an, die auf dem IBM Spectrum Protect-Server gespeichert sind oder sich in einem Sicherungssatz auf dem Server befinden, wenn die Option `backupsetname` angegeben ist.

Der Befehl zeigt die folgenden Dateiinformationen an:

- Dateispezifikation
- Dateigröße
- Sicherungsdatum
- Ob die Datei aktiv oder inaktiv ist.
- Die der Datei zugeordnete Verwaltungsklasse. Es werden nur die ersten 10 Zeichen des Verwaltungsklassennamens angezeigt.

Wenn Sie die Option `detail` im Befehl **query backup** verwenden, zeigt der Client die folgenden zusätzlichen Informationen an:

- Datum der letzten Änderung
- Datum des letzten Zugriffs
- Letztes Änderungsdatum der Dateiattribute (Dateiindex)
- Komprimierungstyp
- Verschlüsselungstyp
- Clientseitige Deduplizierung von Daten
- Ob die Datei umgelagert oder vorumgelagert wird. Der Wert Yes bedeutet, dass die Datei umgelagert oder vorumgelagert wird. Der Wert No bedeutet, dass die Datei nicht umgelagert oder vorumgelagert wird.
- Dateiindexnummer (für AIX- und Linux-Clients)
- Größe der ACL-Metadaten (IBM Spectrum Scale) (für AIX- und Linux-Clients)
- Serverspeicherinformationen (Datenträgerklasse, Datenträger-ID und Zurückschreibungsreihenfolge (für AIX- und Linux-Clients)

Das folgende Beispiel zeigt Beispielausgaben, wenn der Befehl **query backup** mit der Option `detail` ausgegeben wird:

Größe	Sicher.-Datum	Verw.-Kl.	A/I Datei
----	-----	-----	-----
1,500,000 B	08/15/2016 16:01:25	DEFAULT	A /home/test/mydir/myfile1.txt

Geändert: 08/15/2016 16:00:10 Zugriffen: 08/16/2016 15:31:23 Dateiindex geändert: 08/15/2016 16:00:10
Komprimierungstyp: LZ4 Verschlüsselungstyp: None Vom Client dedupliziert: YES Umgelagert: NO Dateiindexnr.: 22691
ACL-Größe: 0 Datenträgerklasse: Fest Datenträger-ID: 0008 Zurückschreibungsreihenfolge: 00000000-0000001F-00000000-00

Weitere Informationen zum Komprimierungstyp finden Sie in „Compression“ auf Seite 380.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

►► Query Backup ————— —Dateispezifikation—►
 └—Optionen—┐ └—"Dateispezifikation"—┐

Parameter

Dateispezifikation

Gibt den Pfad und den Namen der Datei an, die abgefragt werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis anzugeben. Werden Platzhalterzeichen verwendet, muss die Dateispezifikation in Anführungszeichen eingeschlossen werden. Durch Eingabe eines Sterns (*) können Informationen zu den Sicherungsversionen aller Dateien im aktuellen Verzeichnis angezeigt werden. Verwenden Sie keine Platzhalterzeichen, wenn Sie NAS-Dateisystemimages mit der Optionseinstellung `-class=nas` abfragen.

Tabelle 95. Befehl 'Query Backup': Zugehörige Optionen

Option	Verwendung
backupsetname „Backupsetname“ auf Seite 370	Nur in der Befehlszeile.
class „Class“ auf Seite 374	Nur in der Befehlszeile.
dateformat „Dateformat“ auf Seite 389	Clientsystemoptionsdatei (dsm.sys) oder Befehlszeile.
detail „Detail“ auf Seite 398	Nur in der Befehlszeile.
dirsonly „Dirsonly“ auf Seite 403	Nur in der Befehlszeile.
filelist „Filelist“ auf Seite 453	Nur in der Befehlszeile.
filesonly „Filesonly“ auf Seite 457	Nur in der Befehlszeile.
fromdate „Fromdate“ auf Seite 461	Nur in der Befehlszeile.
fromowner „Fromnode“ auf Seite 461	Nur in der Befehlszeile.
fromowner „Fromowner“ auf Seite 462	Nur in der Befehlszeile.
fromtime „Fromtime“ auf Seite 463	Nur in der Befehlszeile.
inactive „Inactive“ auf Seite 471	Nur in der Befehlszeile.
nasnodename „Nasnodename“ auf Seite 515	Clientsystemoptionsdatei (dsm.sys) oder Befehlszeile.
numberformat „Numberformat“ auf Seite 521	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
pitdate „Pitdate“ auf Seite 529	Nur in der Befehlszeile.
pittime „Pittime“ auf Seite 530	Nur in der Befehlszeile.
querysummary „Querysummary“ auf Seite 542	Nur in der Befehlszeile.

Tabelle 95. Befehl 'Query Backup': Zugehörige Optionen (Forts.)

Option	Verwendung
scrolllines „Scrolllines“ auf Seite 572	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
scrollprompt „Scrollprompt“ auf Seite 573	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
subdir „Subdir“ auf Seite 605	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
timeformat „Timeformat“ auf Seite 616	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
todate „Todate“ auf Seite 621	Nur in der Befehlszeile.
totime „Totime“ auf Seite 622	Nur in der Befehlszeile.

Beispiele

Task Eine Liste aller aktiven und inaktiven Sicherungsversionen der Benutzerdateien im aktuellen Verzeichnis anzeigen.

```
dsmc query backup -inactive "*"
```

Task Eine Liste aller Ihrer Sicherungen im aktuellen Verzeichnis anzeigen. Die Option detail verwenden, um das Datum der letzten Änderung und das Datum des letzten Zugriffs jeder Datei anzuzeigen.

```
dsmc q backup -detail "*"
```

Task Eine Liste der Dateien anzeigen, die aus dem Verzeichnis /home/proj gesichert wurden und deren Dateiname mit proj beginnt.

```
dsmc q b "/home/proj/proj*"
```

Task Eine Liste der aktiven und inaktiven Sicherungsdateiversionen im Dateisystem /home anzeigen.

```
dsmc q b -ina -su=yes /home/
```

Task Dateisystemimages auf dem NAS-Dateiserver 'nas2' abfragen.

```
dsmc query backup -nasnodename=nas2 -class=nas
```

Zugehörige Informationen

„Daten aus einem Sicherungssatz zurückschreiben“ auf Seite 250

NAS-Dateisystemimages abfragen

Mit dem Befehl **query backup** können Sie Informationen zu Dateisystemimages, die für einen NAS-Dateiserver gesichert wurden, anzeigen. Der Client fordert Sie zur Eingabe einer Administrator-ID auf.

Falls unterstützt, verwenden Sie die Option nasnodename, um den abzufragenden NAS-Dateiserver anzugeben. Fügen Sie die Option nasnodename in Ihre Clientsystemoptionsdatei (dsm.sys) ein. Der Wert in der Clientsystemoptionsdatei ist der Standardwert, dieser Wert kann jedoch in der Befehlszeile überschrieben werden.

Mit der Option `class` können Sie die Klasse des abzufragenden Dateibereichs angeben. Verwenden Sie die Option `-class=nas`, um eine Liste der Images anzuzeigen, die zu einem NAS-Knoten gehören.

Zugehörige Verweise:

„Class“ auf Seite 374

„Nasnodename“ auf Seite 515

Query Backupset

Der Befehl **query backupset** fragt einen Sicherungssatz von einer lokalen Datei, von einer Bandeinheit (falls anwendbar) oder vom IBM Spectrum Protect-Server ab.

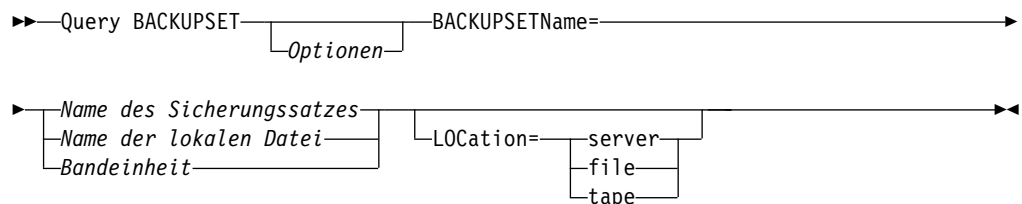
Dieser Befehl zeigt den Namen des Sicherungssatzes, das Erstellungsdatum, den Aufbewahrungszeitraum (für einen Sicherungssatz auf dem IBM Spectrum Protect-Server) und die vom Benutzer bereitgestellte Beschreibung an.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Bandunterstützung ist nur für AIX- und Oracle Solaris-Clients verfügbar.

Syntax



Parameter

BACKUPSETName=

Gibt den Namen des Sicherungssatzes an, der abgefragt werden soll. Den Namen des Sicherungssatzes können Sie mithilfe von Platzhalterzeichen angeben. Wenn Sie Platzhalterzeichen verwenden oder keinen Sicherungssatznamen angeben, werden alle Sicherungssätze angezeigt, deren Eigner Sie sind. Dieser Parameter ist erforderlich.

Wenn ein Sicherungssatz erstellt wird, ordnet der Server Root als Eigner des Sicherungssatzes zu. Bei der Abfrage eines Sicherungssatzes auf dem Server wird der Sicherungssatz für andere Benutzer als Root nicht angezeigt, selbst wenn ihnen der Name des Sicherungssatzes bekannt ist und sie ihn in der Abfrage angeben.

Der Wert von **backupsetname** ist von der Position des Sicherungssatzes abhängig und entspricht einer der folgenden drei Auswahlmöglichkeiten:

backupsetname

Gibt den Namen des Sicherungssatzes auf dem Server an. Wird der Parameter **location** angegeben, müssen Sie `-location=server` angeben.

Name der lokalen Datei

Gibt den Dateinamen des ersten Datenträgers des Sicherungssatzes an. Sie müssen `-location=file` angeben.

Bandeinheit

Gibt den Namen der Bandeinheit an, die den Datenträger des Sicherungssatzes enthält. Sie müssen einen nativen Windows-Einheitentreiber und nicht den von IBM bereitgestellten Einheitentreiber verwenden. Sie müssen `-location=tape` angeben.

LOCation=

Gibt an, wo der Client für Sichern/Archivieren nach dem Sicherungssatz sucht. Wenn Sie den Parameter `location` nicht angeben, sucht der Client auf dem IBM Spectrum Protect-Server nach Sicherungssätzen.

Server Gibt an, dass der Client den Sicherungssatz auf dem Server sucht. Diese Position ist der Standardwert.

file Gibt an, dass der Client den Sicherungssatz in einer lokalen Datei sucht.

tape Gibt an, dass der Client den Sicherungssatz auf einer lokalen Bandeinheit sucht.

Tabelle 96. Befehl `Query Backupset`: Zugehörige Optionen

Option	Verwendung
<code>description</code> „Description“ auf Seite 397	Nur in der Befehlszeile.
<code>scrolllines</code> „Scrolllines“ auf Seite 572	Clientbenutzeroptionsdatei (<code>dsm.opt</code>) oder Befehlszeile.
<code>scrollprompt</code> „Scrollprompt“ auf Seite 573	Clientbenutzeroptionsdatei (<code>dsm.opt</code>) oder Befehlszeile.

Beispiele

Task Alle Sicherungssätze auf dem IBM Spectrum Protect-Server abfragen.

Befehl: `query backupset -backupsetname=*`

Task Einen Sicherungssatz mit dem Namen `monthly_financial_data` auf dem IBM Spectrum Protect-Server abfragen.

Befehl: `query backupset
-backupsetname=monthly_financial_data.12345678`

Task Den Sicherungssatz in der Datei `/home/budget/weekly_budget_data.ost` abfragen.

Befehl: `dsmc query backupset -backupsetname="/home/budget/
weekly_budget_data.ost" -loc=file`

Task Den Sicherungssatz auf der Bandeinheit `/dev/rmt0` abfragen.

Befehl: `dsmc query backupset -backupsetname=/dev/rmt0 -loc=tape`

Zugehörige Informationen

„Daten aus einem Sicherungssatz zurückschreiben“ auf Seite 250

Query Backupset ohne Parameter backupsetname

Der Befehl **query backupset** kann ohne den Parameter **backupsetname** verwendet werden.

Die bevorzugte Syntax für den Befehl **query backupset** erfordert den Parameter **backupsetname**. Vor der Einführung des Parameters **backupsetname** hat der Client für Sichern/Archivieren beim Abfragen von Sicherungssätzen eine andere Syntax verwendet.

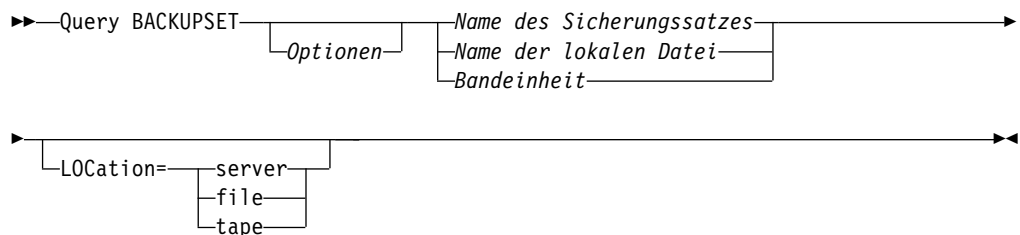
Sie können zwar die Syntax früherer Releases für diesen Befehl verwenden, diese Syntax sollte jedoch nur verwendet werden, wenn bestimmte Anforderungen vorliegen und die alte Syntax nicht durch die Syntax in Tivoli Storage Manager Version 6.1 ersetzt werden kann. Die besten Ergebnisse erzielen Sie, wenn Sie den Parameter **backupsetname** verwenden.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Bandunterstützung ist nur für AIX- und Oracle Solaris-Clients verfügbar.

Syntax



Parameter

backupsetname

Gibt den Namen des Sicherungssatzes auf dem IBM Spectrum Protect-Server an. Wird der Parameter **location** angegeben, müssen Sie **-location=server** angeben.

Name der lokalen Datei

Gibt den Dateinamen des ersten Datenträgers des Sicherungssatzes an. Sie müssen **-location=file** angeben.

Bandeinheit

Gibt den Namen der Bandeinheit an, die den Datenträger des Sicherungssatzes enthält. Sie müssen einen nativen Windows-Einheitentreiber und nicht den von IBM bereitgestellten Einheitentreiber verwenden. Sie müssen **-location=tape** angeben.

LOCation=

Gibt an, wo der Client nach dem Sicherungssatz sucht. Wenn Sie den Parameter **location** nicht angeben, sucht der Client auf dem IBM Spectrum Protect-Server nach Sicherungssätzen.

Server Gibt an, dass der Client den Sicherungssatz auf dem Server sucht. Dies ist der Standardwert.

- file** Gibt an, dass der Client den Sicherungssatz in einer lokalen Datei sucht.
- tape** Gibt an, dass der Client den Sicherungssatz auf einer lokalen Bandeinheit sucht.

Tabelle 97. Befehl Query Backupset: Zugehörige Optionen

Option	Verwendung
description „Description“ auf Seite 397	Nur in der Befehlszeile.
scrolllines „Scrolllines“ auf Seite 572	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
scrollprompt „Scrollprompt“ auf Seite 573	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.

Beispiele

Task Alle Sicherungssätze auf dem IBM Spectrum Protect-Server abfragen.

Befehl: query backupset

Task Einen Sicherungssatz mit dem Namen monthly_financial_data auf dem IBM Spectrum Protect-Server abfragen.

Befehl: query backupset monthly_financial_data.12345678

Task Den Sicherungssatz in der Datei /home/budget/weekly_budget_data.ost abfragen.

Befehl: dsmc query backupset /home/budget/weekly_budget_data.ost
-loc=file

Task Den Sicherungssatz auf der Bandeinheit /dev/rmt0 abfragen.

Befehl: dsmc query backupset /dev/rmt0 -loc=tape

Zugehörige Informationen

„Daten aus einem Sicherungssatz zurückschreiben“ auf Seite 250

Query Filespace

Der Befehl **query filespace** zeigt eine Liste der Dateibereiche für einen Knoten an. Die Dateibereiche sind auf dem IBM Spectrum Protect-Server gespeichert oder befinden sich in einem Sicherungssatz auf dem Server, wenn die Option backupsetname angegeben wird. Sie können auch einen einzelnen Dateibereich für die Abfrage angeben.

Ein *Dateibereich* ist ein logischer Speicherbereich auf dem Server, der die gesicherten oder archivierten Dateien enthält. Auf dem Server wird jedem Knoten Ihrer Workstation, von dem Sie Dateien sichern oder archivieren, ein separater Dateibereich zugeordnet.

Auf dem Server wird jedem Dateisystem Ihrer Workstation, von dem Sie Dateien sichern oder archivieren, ein separater Dateibereich zugeordnet. Der Dateibereichsname entspricht dem Namen des Dateisystems.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
►► Query Filespace [—Dateibereichsname] [—Optionen] ►►
```

Parameter

Dateibereichsname

Gibt eine optionale Zeichenfolge an, die Platzhalterzeichen enthalten kann. Mit diesem Argument können Sie eine Untergruppe von Dateibereichen angeben. Standardmäßig werden alle Dateibereiche angezeigt.

Tabelle 98. Befehl Query Filespace: Zugehörige Optionen

Option	Verwendung
backupsetname „Backupsetname“ auf Seite 370	Nur in der Befehlszeile.
class „Class“ auf Seite 374	Nur in der Befehlszeile.
dateformat „Dateformat“ auf Seite 389	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
detail „Detail“ auf Seite 398	Nur in der Befehlszeile.
fromnode „Fromnode“ auf Seite 461	Nur in der Befehlszeile.
fromowner „Fromowner“ auf Seite 462	Nur in der Befehlszeile.
nasnodename „Nasnodename“ auf Seite 515	Clientsystemoptionsdatei (dsm.sys) oder Befehlszeile.
scrolllines „Scrolllines“ auf Seite 572	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
scrollprompt „Scrollprompt“ auf Seite 573	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
timeformat „Timeformat“ auf Seite 616	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.

Beispiele

Eigene Dateibereiche anzeigen. Die Datums- und Zeitformate mit Hilfe der Optionen dateformat und timeformat neu formatieren.

```
query filesystem -date=5 -time=4
```

Den Dateibereich /home anzeigen.

```
query filesystem /home
```

Dateibereichsnamen anzeigen, die das Muster smith enthalten.

```
query filespace "*smith"
```

Einen Dateibereich vom NAS-Dateiserver nas2 abfragen.

```
query filespace -nasnodename=nas2 -class=nas
```

Detaillierte Dateibereichsinformationen anzeigen, die den Replikationsstatus während einer Übernahme zeigen.

Befehl:

```
query filespace -detail
```

Ausgabe:

Nr.	Datum ltzt	Teilsich.	Typ	FSID	Unicode	Replikation	Dateibereichsname
1	00.00.0000	00:00:00	HFS	3	Yes	Current	/
<div><div>Letztes Speicherdatum</div><div>Server</div><div>Lokal</div><div>Sicherungsdaten: 29.04.2013 16:49:55 Archivierungsdaten: Kein Datum verfügbar</div><div>29.04.2013 16:49:55 Kein Datum verfügbar</div></div>							

Zugehörige Konzepte:

„Daten aus einem Sicherungssatz zurückschreiben“ auf Seite 250

„Automatisierte Clientübernahme - Übersicht“ auf Seite 98

Zugehörige Tasks:

„Status replizierter Clientdaten bestimmen“ auf Seite 104

Zugehörige Verweise:

„Nasnodename“ auf Seite 515

„Class“ auf Seite 374

„Nrtablepath“ auf Seite 520

NAS-Dateibereiche abfragen

Mit der Option nasnodename identifizieren Sie den abzufragenden NAS-Dateiserver. Bei Verwendung einer interaktiven Befehlszeilensitzung mit einer ID ohne Verwaltungsberechtigung fordert der Client Sie zur Eingabe einer Administrator-ID auf.

Fügen Sie die Option nasnodename in Ihre Clientsystemoptionsdatei (dsm.sys) ein. Der Wert in der Clientsystemoptionsdatei ist der Standardwert, dieser Wert kann jedoch in der Befehlszeile überschrieben werden. Wird die Option nasnodename nicht in der Clientsystemoptionsdatei angegeben, muss sie bei der Verarbeitung von NAS-Dateisystemen in der Befehlszeile angegeben werden.

Mit der Option class können Sie die Klasse des abzufragenden Objekts angeben. Verwenden Sie die Option -class=nas, um eine Liste der Dateibereiche anzuzeigen, die zu einem NAS-Knoten gehören.

Query Group

Verwenden Sie den Befehl **query group**, um Informationen zu einer Gruppensicherung und ihren Mitgliedern anzuzeigen.

Anmerkung:

1. Verwenden Sie die Option **showmembers**, um einzelne Member anzuzeigen und auszuwählen, die abgefragt werden sollen. Die Option **showmembers** ist mit der Option **inactive** nicht gültig. Um Member in einer Gruppe anzuzeigen, die zurzeit nicht aktiv sind, die Optionen **pitdate** und **pittime** verwenden, um das Sicherungsdatum und die Sicherungszeit für das abzufragende Member anzugeben.
2. Verwenden Sie den Befehl **query filesystem**, um virtuelle Dateibereichsnamen für Ihren Knoten, die auf dem IBM Spectrum Protect-Server gespeichert sind, anzuzeigen.
3. Führen Sie eine vollständige und eine differenzielle Gruppensicherung und anschließend eine Abfrage dieser Gruppe mit der Option **inactive** aus, werden zwei aktive Sicherungen mit demselben Namen angezeigt, wobei eine den Typ FULL und die andere den Typ DIFF hat.

```
Protect> q group {/fs}/v1 -inactive
```

Größe	Sicher.-Datum	Verw.-kl.	A/I	Gruppe
978 B	06/02/2007 11:57:04	DEFAULT	A	FULL /fs/v1
32 B	06/05/2007 13:52:04	DEFAULT	A	DIFF /fs/v1

Fragen Sie eine Gruppensicherung ohne die Option **-inactive** ab, wird nur die letzte Gruppensicherung angezeigt, die den Typ FULL oder DIFF haben kann:

```
Protect> q group {/fs}/v1
```

Größe	Sicher.-Datum	Verw.-kl.	A/I	Gruppe
32 B	06/05/2007 13:52:04	DEFAULT	A	DIFF /fs/v1

Unterstützte Clients

Dieser Befehl ist für alle Clients außer Mac OS X gültig.

Syntax

```

>> Query Group — Dateispezifikation —————>
                                   |
                                   | —Optionen—

```

Parameter

Dateispezifikation

Gibt den Namen des virtuellen Dateibereichs und den Namen der Gruppe auf dem Server für die Abfrage an.

Tabelle 99. Befehl Query Group: Zugehörige Optionen

Option	Verwendung
fromnode „Fromnode“ auf Seite 461	Nur in der Befehlszeile.
fromowner „Fromowner“ auf Seite 462	Nur in der Befehlszeile.
inactive „Inactive“ auf Seite 471	Nur in der Befehlszeile.
pitdate „Pitdate“ auf Seite 529	Nur in der Befehlszeile.
pittime „Pittime“ auf Seite 530	Nur in der Befehlszeile.

Tabelle 99. Befehl Query Group: Zugehörige Optionen (Forts.)

Option	Verwendung
showmembers „Showmembers“ auf Seite 579 (gilt nicht für Mac OS X)	Nur in der Befehlszeile.

Beispiele

Task Alle Gruppen im Dateibereich /virtfs anzeigen.

Befehl:

```
query group /virtfs/*
```

Task Aktive und inaktive Versionen des Dateibereichs /virtfs/group1 anzeigen.

Befehl:

```
query group /virtfs/group1 -inactive
```

Task Den Dateibereich /virtfs/group1 anzeigen. Die Option showmembers verwenden, um eine Liste der Gruppenmember anzuzeigen, aus der Sie abzufragende Member auswählen können.

Befehl:

```
query group /virtfs/group1 -showmembers
```

Zugehörige Informationen

„Query Filespace“ auf Seite 754

Query Image

Der Befehl **query image** zeigt Informationen zu Dateisystemimages an, die auf dem IBM Spectrum Protect-Server gespeichert sind oder sich in einem Sicherungssatz auf dem IBM Spectrum Protect-Server befinden, wenn die Option backupsetname angegeben wurde.

Die folgenden Informationen zu Dateisystemimages werden angezeigt:

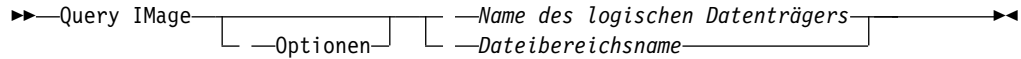
- Imagegröße - Die Größe des Datenträgers, der gesichert wurde.
- Gespeicherte Größe - Die tatsächliche Größe des Images, das auf dem Server gespeichert wurde. Das auf dem IBM Spectrum Protect-Server gespeicherte Image hat dieselbe Größe wie der Datenträger. Bei Online-Imagesicherungen auf Momentaufnahmebasis kann das gespeicherte Image aufgrund der Größe der Cachedateien größer als das Dateisystem sein. Das auf dem Server gespeicherte Image hat dieselbe Größe wie der Datenträger.
- Dateisystemtyp
- Sicherungsdatum und -zeit
- Die der Imagesicherung zugeordnete Verwaltungsklasse
- Ob die Imagesicherung eine aktive oder inaktive Kopie ist
- Der Imagenname

Anmerkung: Die IBM Spectrum Protect-API muss installiert sein, um den Befehl **query image** verwenden zu können.

Unterstützte Clients

Diese Option ist für AIX-, Linux- und Oracle Solaris-Clients gültig.

Syntax



Parameter

Name des logischen Datenträgers

Der Name eines logischen Datenträgers, der abgefragt werden soll. Sie müssen den exakten Namen des Images angeben. Platzhalterzeichen sind nicht zulässig. Standardwert ist alle aktiven Images (sofern nicht durch eine oder mehrere Optionen eingeschränkt).

Dateibereichsname

Der Name des Dateisystems, das abgefragt werden soll.

Werden der *Name des logischen Datenträgers* und *Dateibereichsname* nicht angegeben, werden alle Images angezeigt.

Tabelle 100. Befehl Query Image: Zugehörige Optionen

Option	Verwendung
backupsetname „Backupsetname“ auf Seite 370	Nur in der Befehlszeile.
dateformat „Dateformat“ auf Seite 389	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
fromnode „Fromnode“ auf Seite 461	Nur in der Befehlszeile.
fromowner „Fromowner“ auf Seite 462	Nur in der Befehlszeile.
inactive „Inactive“ auf Seite 471	Nur in der Befehlszeile.
numberformat „Numberformat“ auf Seite 521	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
pitdate „Pitdate“ auf Seite 529	Nur in der Befehlszeile.
pittime „Pittime“ auf Seite 530	Nur in der Befehlszeile.
scrolllines „Scrolllines“ auf Seite 572	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
scrollprompt „Scrollprompt“ auf Seite 573	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
timeformat „Timeformat“ auf Seite 616	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.

Beispiele

Task Alle gesicherten Images anzeigen.

Befehl: q image

Task Alle gesicherten Images anzeigen, deren Eigner kutras auf dem Knoten avalon ist.

Befehl: query image -fromnode=avalon -fromowner=kutras

Task Aktive und inaktive Versionen des Images /usr anzeigen.

Befehl: q i /usr -inactive

Task Alle Images anzeigen, die sich im Sicherungssatz weekly_backup_data.32145678 befinden.

Befehl: query image -backupsetname=weekly_backup_data.32145678

Zugehörige Informationen

„Daten aus einem Sicherungssatz zurückschreiben“ auf Seite 250

Query Inclexcl

Mit dem Befehl **query inclexcl** wird eine Liste der Include/Exclude-Anweisungen in der Reihenfolge angezeigt, in der sie bei Sicherungs- und Archivierungsoperationen verarbeitet werden. Die Liste zeigt die Optionsart, den Optionsbereich (archive, all, etc.) und den Namen der Quellendatei.

Der Client für Sichern/Archivieren schließt einige Dateien von Dateisystemsicherungs- und -zurückschreibungsoperationen aus. Sie können eine Liste dieser Dateien mit dem Befehl **query inclexcl** anzeigen. In der Ausgabe des Befehls steht bei diesen Dateien Betriebssystem neben dem Pfad.

Sie können die Gültigkeit der gewünschten Muster für die Einschluss-/Ausschlussliste testen, bevor Sie sie tatsächlich in Ihre Optionsdatei einfügen. Siehe die Erläuterung bei *Testmuster*.

Verwenden Sie die Option **detail**, um die Verwaltungsklasse anzuzeigen, die einer Include/Exclude-Anweisung zugeordnet ist.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

►► Query INClexcl — Testmuster -DEtail ►►

Parameter

Testmuster

Dient zum Testen der Gültigkeit der Muster, die Sie in Ihrer Einschluss-/Ausschlussliste verwenden wollen. Wenn Sie ein Testmuster in diesem Befehl verwenden, geschieht Folgendes:

- Die interne Einschluss-/Ausschlussliste wird nicht angezeigt

- Das Muster wird so verarbeitet, als ob es aus einer Einschluss-/Ausschlussanweisung stammte, einschließlich der gesamten üblichen Fehlerprüfung
- Das Muster wird so angezeigt, wie es in der Einschluss-/Ausschlussliste erscheinen würde

Wenn das Testmuster fehlerfrei ist, ist das Ergebnis des kompilierten Musters mit dem Testmuster identisch.

-DETail

Zeigt die Verwaltungsklasse an, die der Include/Exclude-Anweisung zugeordnet ist.

Beispiele

Task Eine Datei durch Ausschluss in der Clientoptionsdatei von der Deduplizierung ausschließen:

```
Exclude Dedup *\...\file2
```

Task Eine allgemeine Liste der Include/Exclude-Anweisungen anzeigen. Befehl:
query inclexcl

Task Eine Liste der Include/Exclude-Anweisungen anzeigen. Die Verwaltungsklasse anzeigen, die jeder Anweisung zugeordnet ist.

```
query inclexcl -detail
```

Task Die Gültigkeit des folgenden Musters testen: /.../?x?/*.log

```
query inclexcl /.../?x?/*.log
```

Query Mgmtclass

Mit dem Befehl **query mgmtclass** können Informationen zu den Verwaltungsklassen angezeigt werden, die in der aktiven Maßnahmengruppe verfügbar sind.

Ihr Administrator definiert Verwaltungsklassen. Diese enthalten Attribute, die steuern, ob eine Datei für Sicherungs- oder Archivierungsservices ausgewählt werden kann. Verwaltungsklassen bestimmen außerdem, wie Sicherungen und Archivierungen auf dem Server verwaltet werden.

Die aktive Maßnahmengruppe enthält eine Standardverwaltungs-klasse; sie kann eine beliebige Anzahl zusätzlicher Verwaltungsklassen enthalten. Sie können Dateien bestimmte Verwaltungsklassen zuordnen, indem Sie include-Optionen in der Clientbenutzeroptionsdatei (dsm.opt) verwenden. Wenn Sie einer Datei keine Verwaltungsklasse zuordnen, wird die Standardverwaltungs-klasse verwendet.

Wenn Dateien archiviert werden, kann die zugeordnete Verwaltungsklasse mit Hilfe der Option archmc überschrieben werden.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```

>> Query Mgmtclass [—Optionen]

```

Parameter

Tabelle 101. Befehl Query Mgmtclass: Zugehörige Optionen

Option	Verwendung
detail „Detail“ auf Seite 398	Nur in der Befehlszeile.
fromnode „Fromnode“ auf Seite 461	Nur in der Befehlszeile.

Beispiele

Task Standard- und verfügbare Verwaltungsklassen anzeigen.

Befehl: query mgmtclass

Query Node

Der Befehl **query node** zeigt alle Knoten an, für die eine Verwaltungsbenutzer-ID die Berechtigung zum Ausführen von Operationen hat. Sie werden zur Eingabe der IBM Spectrum Protect-Administrator-ID aufgefordert.

Die Verwaltungsbenutzer-ID sollte mindestens über die Clienteignerberechtigung für den Client-Workstation-Knoten verfügen, der entweder von der Befehlszeile oder vom Web aus verwendet wird.

Sie können mit der Option type die Knotenart angeben, mit der gefiltert werden soll. Die folgenden Werte sind gültig:

- nas
- Client
- Server
- any

Der Standardwert ist **any**.

Anmerkung: Wenn die IBM Spectrum Protect for Virtual Environments: Data Protection for VMware-Lizenzdatei auf einem vStorage-Sicherungsserver installiert ist, wird die auf dem IBM Spectrum Protect-Server gespeicherte Plattformzeichenfolge für jeden Knotennamen, der auf dieser Maschine verwendet wird, auf „TDP VMware“ gesetzt. Die Plattformzeichenfolge kann im Kontext von PVU-Berechnungen verwendet werden. Wird ein Knotenname für die Sicherung der Maschine mit Standardfunktionen des Clients für Sichern/Archivieren verwendet (beispielsweise Sicherung auf Dateiebene oder Imagesicherung), wird diese Plattformzeichenfolge für die Zwecke der PVU-Berechnungen als „client“ interpretiert.

Weitere Informationen zu Prozessor-Value-Units finden Sie im Abschnitt *Prozessor-Value-Units schätzen* in der IBM Spectrum Protect-Serverdokumentation.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

►► Query Node —Optionen— ►►

Parameter

Tabelle 102. Befehl Query Node: Zugehörige Optionen

Option	Verwendung
type „Type“ auf Seite 624	Nur in der Befehlszeile.
scrolllines „Scrolllines“ auf Seite 572	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
scrollprompt „Scrollprompt“ auf Seite 573	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.

Beispiele

Task Alle NAS-Knoten anzeigen.

Befehl: query node -type=nas

Task Alle Clientknoten anzeigen, die Clients für Sichern/Archivieren sind.

Befehl: query node -type=client

Zugehörige Informationen

„Type“ auf Seite 624

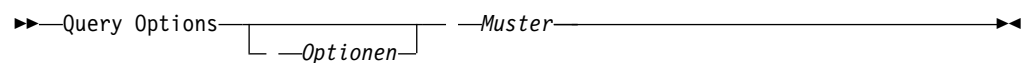
Query Options

Verwenden Sie den Befehl **query options**, um alle Optionen oder einen Teil Ihrer Optionen und ihre aktuelle Einstellung in Bezug auf den Befehlszeilenclient anzuzeigen.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax



Parameter

Muster

Eine optionale Zeichenfolge, die Platzhalterzeichen enthalten kann. Mit diesem Argument können Sie eine Untergruppe von Optionen angeben. Standardmäßig werden alle Optionen angezeigt.

Tabelle 103. Befehl Query Options: Zugehörige Optionen

Option	Verwendung
scrolllines „Scrolllines“ auf Seite 572	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.

Tabelle 103. Befehl `Query Options`: Zugehörige Optionen (Forts.)

Option	Verwendung
<code>scrollprompt</code> „Scrollprompt“ auf Seite 573	Clientbenutzeroptionsdatei (<code>dsm.opt</code>) oder Befehlszeile.

Beispiele

Task Alle Optionen und ihre Werte anzeigen.

```
query options
```

Task Nur Optionen anzeigen, die mit der Zeichenfolge `comm` beginnen.

```
query options comm*
```

Task Den Wert der Option **replace** anzeigen.

```
query options replace
```

Task Geben Sie den Befehl aus, mit dem alle Optionen und ihre Werte angezeigt werden. Die Übernahmestatusinformationen werden angezeigt.

```
query options
```

Ausgabe:

```
MYPRIMARYSERVERNAME: SERVER1
MYREPLICATIONSERVER: TARGET
REPLSERVERNAME: TARGET
    Address: 192.0.2.9
    Port: 1501
    SSLPort: 1502
    GUID: 39.5a.da.d1.ae.92.11.e2.82.d3.00.0c.29.2f.07.d3
    Used: yes
```

Zugehörige Konzepte:

„Konfiguration und Verwendung der automatisierten Clientübernahme“ auf Seite 98

Zugehörige Tasks:

„Status replizierter Clientdaten bestimmen“ auf Seite 104

Query Restore

Mit dem Befehl **query restore** kann eine Liste der wiederanlauffähigen Zurückschreibungssitzungen des Benutzers in der Serverdatenbank angezeigt werden. Die Liste enthält folgende Felder: Eigner, Ersetzen (Ersetz.), Unterverzeichnis (Untver), Pfad beibehalten (Pfad beibeh.), Quelle und Zielort.

Eine wiederanlauffähige Zurückschreibungssitzung wird erstellt, wenn ein Befehl zum Zurückschreiben mit Platzhalterzeichen wegen eines Netzausfalls, Clientfehlers, Serverausfalls oder wegen eines ähnlichen Fehlers fehlschlägt. Wenn ein solcher Fehler auftritt, wird der Dateibereich auf dem Server gesperrt, sodass seine Dateien nicht von den sequenziellen Datenträgern des Servers weg verschoben werden können. Zum Entsperren des Dateibereichs müssen Sie entweder die Zurückschreibung erneut starten und bis zum Ende ausführen (Befehl **query restore**) oder die Zurückschreibung abbrechen (Befehl **cancel restore**). Verwenden Sie **query restore**, um festzustellen, ob wiederanlauffähige Zurückschreibungssitzungen vorhanden sind und welche Dateien betroffen sind.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

►►—Query Restore—◄◄

Parameter

Für diesen Befehl gibt es keine Parameter.

Beispiele

Task Die wiederanlauffähigen Zurückschreibungssitzungen in der Serverdatenbank anzeigen.

Befehl: query restore

Query Schedule

Der Befehl **query schedule** zeigt die Ereignisse an, die für den Knoten geplant sind. Der Administrator kann Zeitpläne für automatische Sicherungen und Archivierungen erstellen. Zur besseren Arbeitsplanung kann mit diesem Befehl festgestellt werden, wann die nächsten geplanten Ereignisse stattfinden.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

►►—Query SChedule—◄◄

Parameter

Für diesen Befehl gibt es keine Parameter.

Beispiele

Task Geplante Ereignisse anzeigen.

Befehl: query schedule

Query Session

Mit dem Befehl **query session** können Informationen zur Sitzung angezeigt werden, z. B. der aktuelle Knotenname, die Angabe, wann die Sitzung aufgebaut wurde, Serverinformationen und Serververbindungsdaten.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

►►—Query SSession—◄◄

Parameter

Für diesen Befehl gibt es keine Parameter.

Beispiele

Task Die Sitzungsinformationen anzeigen.

Befehl: query session

Eine Beispielanzeige des Befehls **query session**:

```
Servername.....: HALLEY_SERVER1
Servertyp.....: Windows
Schutz der Archivaufbewahrung: "Nein"
Serverversion.....: Ver. 6, Rel. 2, Stu. 0.0
Datum des letzten Zugriffs...: 03.09.2009 09:08:13
Sicherungsdateien löschen....: "Nein"
Archivierungsdateien löschen.: "Ja"
Deduplizierung.....: "Nur Server"

Knotenname.....: HALLEY
Benutzername.....:
```

Mögliche Werte für die clientseitige Deduplizierung:

- Keine
 - Wird bei Verbindung zu einem IBM Spectrum Protect-Server mit einer niedrigeren Version als 6.1 angezeigt
- Nur Server
- Client oder Server

Task

Eine Beispielanzeige des Befehls **query session** (LAN-frei):

IBM Spectrum Protect-Serververbindungsinformationen

```
Servername.....: TEMPLAR
Servertyp.....: AIX
Schutz der Archivaufbewahrung: "Nein"
Serverversion.....: Ver. 6, Rel. 1, Stu. 4.0
Datum des letzten Zugriffs...: 12.08.10 22:10:15
Sicherungsdateien löschen....: "Nein"
Archivierungsdateien löschen.: "Ja"

Knotenname.....: LAN2
Benutzername.....: root

Speicheragentenname.....: TEMPLAR_STA
Speicheragententyp.....: AIX
Speicheragentversion.....: Ver. 6, Rel. 1, Stu. 3.3
```

Query Systeminfo

Verwenden Sie den Befehl **query systeminfo**, um Informationen zusammenzustellen und in eine Datei oder an der Konsole auszugeben.

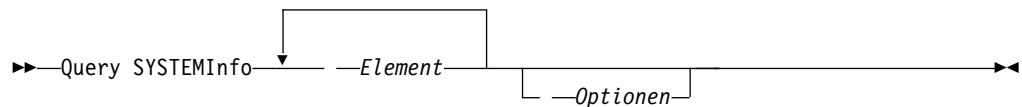
Dieser Befehl ist in erster Linie als Hilfe für die IBM Unterstützungsfunktion bei der Diagnose von Problemen gedacht. Aber Benutzer, die mit den in diesen Informationen angesprochenen Konzepten vertraut sind, finden ihn möglicherweise auch nützlich.

Wenn Sie die Option `console` verwenden, wird keine besondere Formatierung der Ausgabe ausgeführt, um die Anzeighöhe oder -breite anzupassen. Aus diesem Grund ist die Konsolaausgabe wegen ihrer Länge und dem Zeilenumbruch unter Umständen schwierig zu lesen. Wenn die Konsolaausgabe schwierig zu lesen ist, können Sie die Option `filename` mit dem Befehl **query systeminfo** verwenden. Diese Kombination ermöglicht die Ausgabe in eine Datei, die dann an die IBM Unterstützungsfunktion übergeben werden kann.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax



Parameter

Element

Gibt ein oder mehrere Elemente an, zu denen Informationen zusammengestellt und in der Datei, die Sie über die Option `filename` angegeben haben, gespeichert oder an der Konsole ausgegeben werden sollen. Standardmäßig werden Informationen zu allen Elementen zusammengestellt.

Sie können Informationen zu einem oder mehreren der folgenden Elemente zusammenstellen:

- DSMOPTFILE - Inhalt der Datei `dsm.opt`
- DSMSYSFILE - Inhalt der Datei `dsm.sys`
- ENV - Umgebungsvariablen
- ERRORLOG - Fehlerprotokoll des Clients
- FILE - Attribute für den angegebenen Dateinamen.
- INCLEXCL - Stellt eine Liste der Include/Exclude-Anweisungen in der Reihenfolge zusammen, in der sie bei Sicherungs- und Archivierungsoperationen verarbeitet werden.
- OPTIONS - Optionen
- OSINFO - Name und Version des Clientbetriebssystems (umfasst ULIMIT-Informationen für UNIX)
- POLICY - Speicherauszug der Maßnahmengruppe
- SCHEDLOG - Inhalt des Planungsprotokolls (normalerweise `dsmsched.log`).
- CLUSTER - AIX-Clusterinformationen
- ENCRYPT - Verfügbare Verschlüsselungsverfahren

Anmerkung:

1. Verwenden Sie die Option `filename`, um den Namen einer Datei anzugeben, in der die Informationen zu den angegebenen Elementen gespeichert werden sollen. Wenn Sie keinen Dateinamen angeben, werden die Informationen standardmäßig in der Datei `/Library/Application Support/tivoli/tsm/client/ba/bin/dsminfo.txt` (für Mac OS X) oder `dsminfo.txt` (für andere UNIX- und Linux-Systeme) gespeichert.
2. Verwenden Sie die Option `console`, wenn die Informationen an der Konsole ausgegeben werden sollen.

Tabelle 104. Befehl `Query Systeminfo`: Zugehörige Optionen

Option	Verwendung
<code>console</code> „Console“ auf Seite 382	Nur in der Befehlszeile.
<code>filename</code> „Filename“ auf Seite 456	Nur in der Befehlszeile.

Beispiele

Task Den Inhalt der Datei `dsm.opt` und der IBM Spectrum Protect-Fehlerprotokolldatei zusammenstellen und in der Datei `tsminfo.txt` speichern.

Befehl: `query systeminfo dsmoptfile errorlog -filename=tsminfo.txt`

Zugehörige Informationen

„Filename“ auf Seite 456

„Console“ auf Seite 382

Query VM

Verwenden Sie den Befehl **query VM**, um die erfolgreichen Sicherungen von virtuellen Maschinen (VMs) aufzulisten und zu verifizieren.

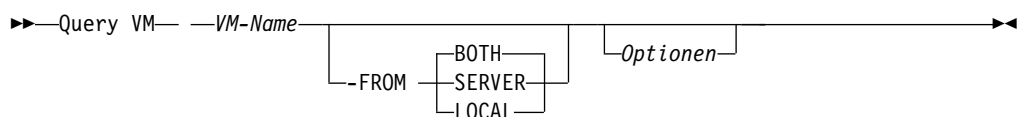
Query VM für virtuelle VMware-Maschinen

Verwenden Sie den Befehl **query vm**, um festzustellen, welche virtuellen VMware-Maschinen gesichert wurden.

Unterstützte Clients

Dieser Befehl ist auf Linux-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind.

Syntax



Parameter

VM-Name

Gibt den Hostnamen der virtuellen Maschine an, die abgefragt werden soll.

Wenn Sie den Namen der virtuellen Maschine nicht angeben, zeigt der Befehl alle VM-Sicherungen auf dem IBM Spectrum Protect-Server an.

-FROM

Gibt die Sicherungsposition oder -positionen an, die abgefragt werden sollen. Sie können einen der folgenden Werte angeben:

SERVER

Die Abfrage ist auf Sicherungen beschränkt, die sich auf dem IBM Spectrum Protect-Server befinden.

LOCAL

Die Abfrage ist auf gespeicherte Momentaufnahmen beschränkt, die sich im Hardwarespeicher befinden.

BOTH Mit der Abfrage werden sowohl Informationen für Sicherungen, die sich auf dem IBM Spectrum Protect-Server befinden, als auch Informationen für Sicherungen, die sich im Hardwarespeicher befinden, aufgelistet. Dies ist der Standardwert.

Tabelle 105. Befehl Query VM: Zugehörige Optionen für Abfragen virtueller VMware-Maschinen

Option	Verwendung
detail „Detail“ auf Seite 398	Befehlszeile
Gültig für vmbackuptype=fullvm	
inactive „Inactive“ auf Seite 471	Befehlszeile
Gültig für vmbackuptype=fullvm	
pitdate „Pitdate“ auf Seite 529	Befehlszeile
Gültig für vmbackuptype=fullvm	
pittime „Pittime“ auf Seite 530	Befehlszeile
Gültig für vmbackuptype=fullvm	
vmbackuptype „Vmbackuptype“ auf Seite 636	Befehlszeile oder Clientoptionsdatei
vmchost „Vmchost“ auf Seite 637	Befehlszeile oder Clientoptionsdatei
vmcpw „Vmcpw“ auf Seite 638	Befehlszeile oder Clientoptionsdatei
vmcuser „Vmcuser“ auf Seite 640	Befehlszeile oder Clientoptionsdatei

Beispiele für Query VM (VMware)

Die folgenden Beispiele zeigen die Verwendung des Befehls **query VM** mit und ohne Angabe der Option **-detail**.

VM-Gesamtsicherung

```
q vm devesx04-24 -ina
VM-Gesamtsicherung auf virtueller Maschine abfragen
```

Nr.	Sicherungsdatum	Verw.-Klasse	Größe	Typ	A/I	Position	Virtuelle Maschine
1	07.12.2016 14:45:24	DDMGMT	47,85 GB	IFFULL	I	SERVER	devesx04-24
2	14.12.2016 17:38:05	DDMGMT	47,85 GB	IFINCR	A	SERVER	devesx04-24
3	23.01.2017 14:07:44	DDMGMT	47,85 GB	SNAPSHOT	I	LOCAL	devesx04-24
4	01.02.2017 08:59:52	DDMGMT	47,85 GB	SNAPSHOT	A	LOCAL	devesx04-24

ANS1900I Rückkehrcode ist 0.

VM-Gesamtsicherung mit der Option **-detail**

```

q vm devesx04-24 -ina -detail
VM-Gesamtsicherung auf virtueller Maschine abfragen

```

Nr.	Sicherungsdatum	Verw.-Klasse	Größe	Typ	A/I	Position	Virtuelle Maschine
1	07.12.2016 14:45:24	DDMGMT	47,85 GB	IFFULL	I	SERVER	devesx04-24
Größe dieser Teilsicherung: nicht zutreffend Anzahl Teilsicherungen seit letzter Gesamtsicherung: 0 Zusätzliches Datenvolumen: 0 IBM Spectrum Protect-Objektfragmentierung: 0 Sicherung ist dargestellt durch: 79 TSM-Objekte Art des Anwendungsschutzes: VMware Momentaufnahmeart: VMware Tools Platte[1] Kennsatz: Festplatte 1 Platte[1] Name: [TSMXIV11:vVOL_JOANNE] rfc4122.750c6a3a-9c65-4a1f-9ed7-1b531aa204 af/devesx04-24-000003.vmdk Platte[1] Status: Geschützt Platte[2] Kennsatz: Festplatte 2 Platte[2] Name: [TSMXIV11:vVOL_JOANNE] rfc4122.750c6a3a-9c65-4a1f-9ed7-1b531aa204 af/devesx04-24_1-000003.vmdk Platte[2] Status: Geschützt Platte[3] Kennsatz: Festplatte 3 Platte[3] Name: [TSMXIV11:vVOL_JOANNE] rfc4122.750c6a3a-9c65-4a1f-9ed7-1b531aa204 af/devesx04-24_2-000003.vmdk Platte[3] Status: Geschützt							
2	14.12.2016 17:38:05	DDMGMT	47,85 GB	IFINCR	A	SERVER	devesx04-24
Größe dieser Teilsicherung: 186,43 MB Anzahl Teilsicherungen seit letzter Gesamtsicherung: 1 Zusätzliches Datenvolumen: 0 IBM Spectrum Protect-Objektfragmentierung: 2 Sicherung ist dargestellt durch: 119 TSM-Objekte Art des Anwendungsschutzes: VMware Momentaufnahmeart: VMware Tools Platte[1] Kennsatz: Festplatte 1 Platte[1] Name: [TSMXIV11:vVOL_JOANNE] rfc4122.750c6a3a-9c65-4a1f-9ed7-1b531aa204 af/devesx04-24-000006.vmdk Platte[1] Status: Geschützt Platte[2] Kennsatz: Festplatte 2 Platte[2] Name: [TSMXIV11:vVOL_JOANNE] rfc4122.750c6a3a-9c65-4a1f-9ed7-1b531aa204 af/devesx04-24_1-000006.vmdk Platte[2] Status: Geschützt Platte[3] Kennsatz: Festplatte 3 Platte[3] Name: [TSMXIV11:vVOL_JOANNE] rfc4122.750c6a3a-9c65-4a1f-9ed7-1b531aa204 af/devesx04-24_2-000006.vmdk Platte[3] Status: Geschützt							
3	23.01.2017 14:07:44	DDMGMT	47,85 GB	SNAPSHOT	I	LOCAL	devesx04-24
Größe dieser Teilsicherung: nicht zutreffend Anzahl Teilsicherungen seit letzter Gesamtsicherung: 0 Zusätzliches Datenvolumen: 0 IBM Spectrum Protect-Objektfragmentierung: 0 Sicherung ist dargestellt durch: 0 TSM-Objekte Art des Anwendungsschutzes: VMware Momentaufnahmeart: VMware Tools							
4	01.02.2017 08:59:52	DDMGMT	47,85 GB	SNAPSHOT	A	LOCAL	devesx04-24
Größe dieser Teilsicherung: nicht zutreffend Anzahl Teilsicherungen seit letzter Gesamtsicherung: 0 Zusätzliches Datenvolumen: 0 IBM Spectrum Protect-Objektfragmentierung: 0 Sicherung ist dargestellt durch: 0 TSM-Objekte Art des Anwendungsschutzes: VMware Momentaufnahmeart: VMware Tools							

```

-----
Alle Durchschnittswerte werden nur für oben angezeigte immer inkrementelle Sicherungen berechnet.
Durchschnittsgröße der Teilsicherung: 186,43 MB
Durchschnittliche Anzahl Teilsicherungen seit letzter Gesamtsicherung: 1
Durchschnittsaufwand für zusätzliche Daten: 0
Durchschnittliche Objektfragmentierung: 0
Durchschnittliche Anzahl Objekte pro Sicherung: 49
ANS1900I Rückkehrcode ist 0.

```

Alle virtuellen VMware-Maschinen abfragen, die mit -vmbaktype=fullvm gesichert wurden:

```
q vm * -vmbaktype=fullvm
```

Zugehörige Tasks:

Restart Restore

Mit dem Befehl **restart restore** kann eine Liste der wiederanlauffähigen Zurückschreibungssitzungen des Benutzers in der Serverdatenbank angezeigt werden.

Sie können nur jeweils eine wiederanlauffähige Zurückschreibungssitzung erneut starten. Führen Sie den Befehl **restart restore** erneut aus, um weitere Zurückschreibungen erneut zu starten.

Bei der erneut gestarteten Zurückschreibung werden dieselben Optionen wie bei der fehlgeschlagenen Zurückschreibung verwendet. Die erneut gestartete Zurückschreibung wird an dem Punkt fortgesetzt, an dem die Zurückschreibung zuvor fehlgeschlagen ist.

Zum Abbrechen wiederanlauffähiger Zurückschreibungssitzungen den Befehl **cancel restore** verwenden. Den Befehl **restart restore** in folgenden Fällen verwenden:

- Wiederanlauffähige Zurückschreibungssitzungen sperren den Dateibereich auf dem Server, sodass Dateien nicht von den sequenziellen Serverdatenträgern weg verschoben werden können.
- Dateien, die von der wiederanlauffähigen Zurückschreibung betroffen sind, können nicht gesichert werden.

Optionen der fehlgeschlagenen Sitzung überlagern neue oder geänderte Optionen für die erneut gestartete Sitzung.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

►►—RESTArt Restore—◄◄

Parameter

Für diesen Befehl gibt es keine Parameter.

Beispiele

Task Eine Zurückschreibungssitzung erneut starten.

Befehl: restart restore

Restore

Mit dem Befehl **restore** werden Kopien der Sicherungsversionen Ihrer Dateien vom IBM Spectrum Protect-Server oder aus einem Sicherungssatz abgerufen.

Zum Zurückschreiben der Dateien müssen die Verzeichnisse oder die ausgewählten Dateien angegeben oder die Dateien aus einer Liste ausgewählt werden. Dateien können in das Verzeichnis zurückgeschrieben werden, aus dem sie gesichert

wurden, oder in ein anderes Verzeichnis. Der Client für Sichern/Archivieren verwendet die Option **preservepath** mit dem Wert **subtree** als Standardwert zum Zurückschreiben von Dateien.

Anmerkung:

1. Für UNIX- und Linux-Systeme: Wird eine symbolische Verbindung erstellt, wird ihre Änderungszeit auf die aktuelle Systemzeit gesetzt. Diese Zeit kann nicht geändert werden. Wenn eine symbolische Verbindung zurückgeschrieben wird, werden daher Datum und Uhrzeit der Zurückschreibung als ihr Änderungsdatum und ihre Änderungszeit festgelegt und nicht das Datum und die Uhrzeit der Verbindung bei ihrer Sicherung. Folglich sichert der Client die symbolische Verbindung während der nächsten Teilsicherung, weil sich ihre Änderungszeit seit der letzten Sicherung geändert hat.

Wenn Sie beim Zurückschreiben eines bestimmten Pfads und einer bestimmten Datei die Option **subdir** auf **yes** setzen, führt der Client eine rekursive Zurückschreibung aller Unterverzeichnisse unter diesem Pfad und aller Instanzen der angegebenen Datei durch, die sich unter allen diesen Unterverzeichnissen befinden.

Wenn Sie ein vollständiges Verzeichnis oder eine vollständige Verzeichnisstruktur zurückschreiben und nicht die Option **inactive**, **latest**, **pick**, **todate** und **fromdate** im Befehl **restore** angeben, verfolgt der Client, welche Objekte zurückgeschrieben werden. Wird der Zurückschreibungsprozess unterbrochen, kann er mit Hilfe des Befehls **restart restore** am Unterbrechungspunkt erneut gestartet werden. Es können mehrere wiederanlauffähige Zurückschreibungssitzungen erstellt werden. Zurückschreibungssitzungen können nur dann erneut gestartet werden, wenn die Dateispezifikation ausschließlich aus Platzhalterzeichen besteht. Für eine wiederanlauffähige Zurückschreibungssitzung kann beispielsweise Folgendes eingegeben werden:

```
dsmc rest /home/* -sub=yes
```

Die Eingabe für eine nicht wiederanlauffähige Zurückschreibungssitzung sieht wie folgt aus:

```
dsmc rest "/Users/user1/file?.c" -sub=yes
```

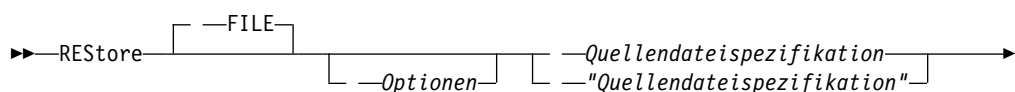
Mit dem Befehl **query restore** wird eine Liste der wiederanlauffähigen Zurückschreibungssitzungen des Benutzers in der Serverdatenbank angezeigt. Es können keine weiteren Sicherungen des Dateisystems ausgeführt werden, bis die wiederanlauffähige Zurückschreibung mit dem Befehl **restart restore** abgeschlossen oder mit dem Befehl **cancel restore** abgebrochen wird.

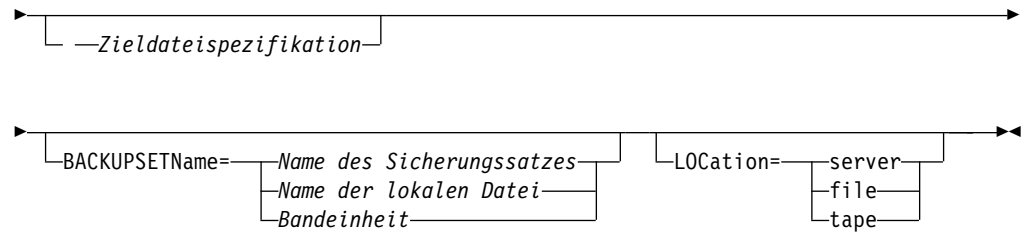
```
dsmc rest "/Users/user1/file?.c" -sub=yes
```

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax





Parameter

file

Dieser Parameter gibt an, dass die Quellendateispezifikation ein expliziter Dateiname ist. Dieser Parameter ist erforderlich, wenn ein Dateiname aus dem aktuellen Pfad zurückgeschrieben wird, kein relativer oder absoluter Pfad angegeben wird und der Dateiname mit einem der reservierten Schlüsselwörter des Befehls **restore**, wie z. B. **restore backupset**, unverträglich ist.

Quellendateispezifikation

Gibt den Pfad und den Namen der Datei im Speicher an, die zurückgeschrieben werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis anzugeben.

{Dateibereichsname}

Gibt den in geschweiften Klammern eingeschlossenen Dateibereich auf dem Server an, in dem sich die zurückzuschreibenden Dateien befinden. Dies ist der Name auf dem Workstationlaufwerk, auf dem die Dateien gesichert wurden.

Geben Sie den Dateibereichsnamen an, wenn sich die Laufwerkbezeichnung geändert hat oder wenn Sie Dateien zurückschreiben, die auf einem anderen Knoten gesichert wurden, dessen Laufwerkbezeichnungen sich von Ihren unterscheiden.

Zieldateispezifikation

Gibt den Pfad und den Dateinamen für den Zielort der zurückgeschriebenen Dateien an. Wenn Sie kein Ziel angeben, schreibt der Client die Dateien in den ursprünglichen Quellenpfad zurück.

- Wenn die *Quellendateispezifikation* eine einzelne Datei benennt, kann die *Zieldateispezifikation* eine Datei oder ein Verzeichnis sein. Wenn Sie eine einzelne Datei zurückschreiben, kann die Spezifikation wahlweise mit einem Dateinamen enden, wenn die zurückgeschriebene Datei einen neuen Namen erhalten soll.
- Wenn die *Quellendateispezifikation* Platzhalterzeichen enthält oder wenn `subdir=yes` angegeben wird, muss die *Zieldateispezifikation* ein Verzeichnis sein und mit einem Verzeichnisbegrenzer (\) enden.

Anmerkung: Falls der Zielpfad oder ein Teil davon nicht vorhanden ist, wird er vom Client erstellt.

Anmerkung: Wenn Sie kein Ziel angeben, stellt der Client fest, ob das ursprüngliche Dateisystem erreicht werden kann. Kann das ursprüngliche Dateisystem nicht erreicht werden, schreibt der Client die Datei nicht zurück. In diesem Fall können Sie einen anderen Zielort angeben und den Befehl wiederholen.

BACKUPSETName=

Gibt den Namen eines Sicherungssatzes an. Dieser Parameter ist optional. Wenn Sie den Parameter **backupsetname** im Befehl **restore** angeben, können Sie nicht die Option **pick** verwenden.

Der Wert von **backupsetname** ist von der Position des Sicherungssatzes abhängig und entspricht einer der folgenden Optionen:

backupsetname

Gibt den Namen des Sicherungssatzes auf dem IBM Spectrum Protect-Server an. Wird der Parameter **location** angegeben, müssen Sie **-location=server** angeben. Ist der Sicherungssatz im IBM Spectrum Protect-Serverspeicher gespeichert, muss der Sicherungssatz über ein Inhaltsverzeichnis verfügen.

Name der lokalen Datei

Gibt den Dateinamen des ersten Datenträgers des Sicherungssatzes an. Sie müssen **-location=file** angeben.

Bandeinheit

Gibt den Namen der Bandeinheit an, die den Datenträger des Sicherungssatzes enthält. Sie müssen einen von Windows bereitgestellten Einheitentreiber und nicht den von IBM bereitgestellten Einheitentreiber verwenden. Sie müssen **-location=tape** angeben.

LOCation=

Gibt an, wo der Client nach dem Sicherungssatz sucht. Wenn Sie den Parameter **location** nicht angeben, sucht der Client auf dem IBM Spectrum Protect-Server nach Sicherungssätzen.

Server Gibt an, dass der Client den Sicherungssatz auf dem Server sucht. Dies ist die Standardposition.

file Gibt an, dass der Client den Sicherungssatz in einer lokalen Datei sucht.

tape Gibt an, dass der Client den Sicherungssatz auf einer lokalen Bandeinheit sucht.

Tabelle 106. Befehl Restore: Zugehörige Optionen

Option	Verwendung
dateformat „Dateformat“ auf Seite 389	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
dirsonly „Dirsonly“ auf Seite 403	Nur in der Befehlszeile.
filelist „Filelist“ auf Seite 453	Nur in der Befehlszeile.
filesonly „Filesonly“ auf Seite 457	Nur in der Befehlszeile.
followsymbolic „Followsymbolic“ auf Seite 458	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
fromdate „Fromdate“ auf Seite 461	Nur in der Befehlszeile.
fromnode „Fromnode“ auf Seite 461	Nur in der Befehlszeile.
fromowner „Fromowner“ auf Seite 462	Nur in der Befehlszeile.

Tabelle 106. Befehl Restore: Zugehörige Optionen (Forts.)

Option	Verwendung
fromtime „Fromtime“ auf Seite 463	Nur in der Befehlszeile.
ifnewer „Ifnewer“ auf Seite 468	Nur in der Befehlszeile.
inactive „Inactive“ auf Seite 471	Nur in der Befehlszeile.
latest „Latest“ auf Seite 499	Nur in der Befehlszeile.
numberformat „Numberformat“ auf Seite 521	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
pick Anmerkung: Wenn Sie den Parameter backupsetname im Befehl restore angeben, können Sie nicht die Option pick verwenden. „Pick“ auf Seite 528	Nur in der Befehlszeile.
pitdate „Pitdate“ auf Seite 529	Nur in der Befehlszeile.
pittime „Pittime“ auf Seite 530	Nur in der Befehlszeile.
preservepath „Preservepath“ auf Seite 537	Nur in der Befehlszeile.
replace „Replace“ auf Seite 547	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
subdir „Subdir“ auf Seite 605	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
tapeprompt „Tapeprompt“ auf Seite 607	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
timeformat „Timeformat“ auf Seite 616	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
todate „Todate“ auf Seite 621	Nur in der Befehlszeile.
totime „Totime“ auf Seite 622	Nur in der Befehlszeile.

Beispiele

Task Eine einzelne Datei mit dem Namen budget im Verzeichnis /Users/user1/Documents zurückschreiben.

```
restore /home/devel/projecta/budget
```

Task Eine einzelne Datei mit dem Namen budget zurückschreiben, die sich im aktuellen Verzeichnis befindet.

```
restore file budget
```

- Task** Alle Dateien mit der Dateierweiterung `.c` aus dem Verzeichnis `/home/devel/projecta` zurückschreiben.
- ```
restore "/home/devel/projecta/*.c"
```
- Task** Dateien im Verzeichnis `/user/project` zurückschreiben. Mit Hilfe der Optionen `pick` und `inactive` aktive und inaktive Sicherungsversionen auswählen.
- ```
restore "/user/project/*" -pick -inactive
```
- Task** Alle Dateien aus dem Verzeichnis `/home/devel/projecta`, deren Name auf `.c` endet, in das Verzeichnis `/home/newdevel/projectn/projecta` zurückschreiben. Ist das Verzeichnis `projectn` oder `projectn/projecta` nicht vorhanden, wird es erstellt.
- ```
restore "/home/devel/projecta/*.c" /home/newdevel/projectn/
```
- Task** Alle Dateien im Verzeichnis `/home/mydir` mit ihrem Status am 17. August 2002 um 13:00 Uhr zurückschreiben.
- ```
restore -pitd=8/17/2002 -pitt=13:00:00 /home/mydir/
```
- Task** Alle Objekte im Verzeichnis `/home/myid/` zurückschreiben. Da diese Zurückschreibungsoperation ausschließlich aus Platzhalterzeichen besteht, wird eine wiederanlauffähige Zurückschreibungssitzung erstellt, falls der Zurückschreibungsprozess unterbrochen wird.
- ```
res "/home/myid/*"
```
- Task** Alle Dateien im Verzeichnis `/home/mydir` mit ihrem Status am 17. August 2002 um 13:00 Uhr zurückschreiben.
- ```
restore -pitd=8/17/2002 -pitt=13:00:00 /home/mydir/
```

Zugehörige Informationen

„Daten aus einem Sicherungssatz zurückschreiben“ auf Seite 250

„Preservepath“ auf Seite 537

„Dateisystem- und ACL-Unterstützung“ auf Seite 174

Aus nicht Unicode-fähigen Dateibereichen zurückschreiben

Wenn Sie aus Dateibereichen zurückschreiben wollen, die nicht Unicode-fähig sind, müssen Sie die Quelle auf dem Server und ein Ziel auf dem Client angeben, bevor Sie den Client mit Unicode-Unterstützung installieren.

Anmerkung: Dieser Unicode-Abschnitt gilt nur für Mac OS X.

Beispiel: Angenommen, Jaguar ist der Name Ihrer Startplatte und Sie sichern alle `.log`-Dateien im Verzeichnis `/Users/user5/Documents`. Bevor die Sicherung stattfindet, benennt der Server den Dateibereich in `Jaguar_OLD` um. Bei der Sicherung werden die in der aktuellen Operation angegebenen Daten in den Unicode-fähigen Dateibereich mit dem Namen `/` gestellt. Der neue Unicode-fähige Dateibereich enthält nun nur das Verzeichnis `/Users/user5/Documents` und die Dateien `*.log`, die in der Operation angegeben wurden.

Wenn Sie eine Datei aus dem *umbenannten* (alten) Dateibereich an den ursprünglichen Standort zurückschreiben wollen, müssen Sie sowohl die Quelle als auch das Ziel wie folgt eingeben:

```
restore Jaguar_0LD/Users/user5/Documents  
/mylog.log /Users/user5/Documents/
```

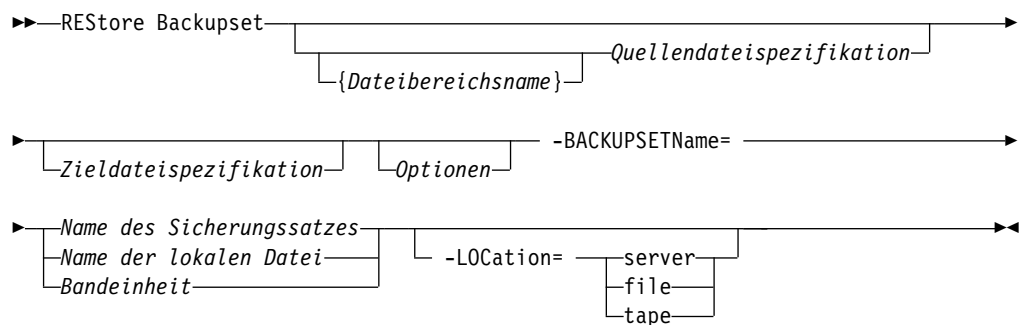
Restore Backupset

Der Befehl **restore backupset** schreibt einen Sicherungssatz vom IBM Spectrum Protect-Server, von einer lokalen Datei oder von einer lokalen Bandeinheit zurück. Sie können den vollständigen Sicherungssatz oder in einigen Fällen bestimmte Dateien in dem Sicherungssatz zurückschreiben.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax



Parameter

`{Dateibereichsname}`

Gibt den in geschweiften Klammern eingeschlossenen Dateibereich auf dem Server an, in dem sich die zurückzuschreibenden Dateien befinden. Dies ist der Name des Workstationlaufwerks, auf dem die Dateien gesichert wurden, oder der Name des virtuellen Dateibereichs für eine Gruppe.

Geben Sie einen Dateibereichsnamen an, wenn Sie einen Sicherungssatz zurückschreiben, der eine Gruppe enthält.

Geben Sie einen Dateibereichsnamen an, wenn die *Quellendateispezifikation* auf dem Zielcomputer nicht vorhanden ist. Diese Situation kann eintreten, wenn sich die Laufwerkbezeichnung geändert hat oder wenn Sie Dateien zurückschreiben, die auf einem anderen Knoten gesichert wurden, dessen Laufwerkbezeichnungen sich von Ihren unterscheiden.

Quellendateispezifikation

Gibt den Quellenpfad eines Teils des Sicherungssatzes an. Standardmäßig wird der gesamte Sicherungssatz zurückgeschrieben.

Zieldateispezifikation

Gibt den Zielpfad für die zurückgeschriebenen Dateien an. Wird keine *Quellendateispezifikation* angegeben, können Sie keine *Zieldateispezifikation* angeben. Wenn Sie kein Ziel angeben, schreibt der Client für Sichern/Archivieren die Dateien in den ursprünglichen Quellenpfad zurück. Wenn Sie mehrere Dateien zurückschreiben, muss die Dateispezifikation mit einem Verzeichnisbegrenzer (/) enden. Andernfalls geht der Client davon aus, dass der letzte Name ein Dateiname ist, und meldet einen Fehler. Wenn Sie eine einzelne Datei zurückschreiben, kann die Zieldateispezifikation optional mit einem Dateinamen en-

den, wenn die zurückgeschriebene Datei einen neuen Namen erhalten soll. Ist die *Quelldateispezifikation* nicht auf der Zielworkstation vorhanden, müssen Sie eine *Zielfdateispezifikation* angeben.

-BACKUPSETName=

Gibt den Namen des Sicherungssatzes an, mit dem eine Zurückschreibungsoperation ausgeführt werden soll. Den Namen des Sicherungssatzes können Sie nicht mit Hilfe von Platzhalterzeichen angeben. Der Wert von *backupsetname* ist von der Position des Sicherungssatzes abhängig und entspricht einer der folgenden Auswahlmöglichkeiten:

Name des Sicherungssatzes

Gibt den Namen des Sicherungssatzes auf dem Server an, von dem eine Operation zum Zurückschreiben ausgeführt werden soll. Wird die Option **location** angegeben, müssen Sie **-location=server** angeben.

Name der lokalen Datei

Gibt den Dateinamen des ersten Datenträgers des Sicherungssatzes an. Sie müssen **-location=file** angeben.

Bandeinheit

Gibt den Namen der Bandeinheit an, die den Datenträger des Sicherungssatzes enthält. Sie müssen einen von Windows bereitgestellten Einheitentreiber und nicht den von IBM bereitgestellten Einheitentreiber verwenden. Sie müssen **-location=tape** angeben.

-LOCation=

Gibt die Position des Sicherungssatzes an. Wenn Sie den Parameter *location* nicht angeben, sucht der Client auf dem IBM Spectrum Protect-Server nach Sicherungssätzen. Wenn Sie den Parameter 'location' angeben, muss der Wert einer der folgenden drei Auswahlmöglichkeiten entsprechen.

server Gibt an, dass der Sicherungssatz sich auf dem IBM Spectrum Protect-Server befindet. Server ist die Standardposition.

file Gibt an, dass der Sicherungssatz sich auf einem verfügbaren Dateisystem befindet.

tape Gibt an, dass der Sicherungssatz sich auf einer verfügbaren Bandeinheit befindet.

Tabelle 107. Befehl Restore Backupset: Zugehörige Optionen

Option	Verwendung
dirsonly „Dirsonly“ auf Seite 403	Nur in der Befehlszeile.
filesonly „Filesonly“ auf Seite 457	Nur in der Befehlszeile.
ifnewer „Ifnewer“ auf Seite 468	Nur in der Befehlszeile.
preservepath „Preservepath“ auf Seite 537	Nur in der Befehlszeile.
quiet „Quiet“ auf Seite 543	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
replace „Replace“ auf Seite 547	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
subdir „Subdir“ auf Seite 605	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.

Beispiele

Task Den gesamten Sicherungssatz mit dem Namen `monthly_financial_data.87654321` vom Server zurückschreiben.

```
dsmc restore backupset
-backupsetname=monthly_financial_data.87654321
-loc=server
```

Task Den gesamten Sicherungssatz zurückschreiben, der in der Datei `/home/budget/weekly_budget_data.ost` enthalten ist.

```
dsmc restore backupset
-backupsetname="/home/budget/weekly_budget_data.ost"
-loc=file
```

Task Den gesamten Sicherungssatz von der Einheit `/dev/rmt0` zurückschreiben.

```
dsmc restore backupset
-backupsetname=/dev/rmt0 -loc=tape
```

Task Die einzelne Datei mit dem Namen `/home/jones/budget.dev` von der Einheit `/dev/rmt0` in den ursprünglichen Quellenpfad zurückschreiben.

```
dsmc restore backupset
-backupsetname=/dev/rmt0 "/home/jones/budget.dev"
-loc=tape
```

Task Alle Dateien im Verzeichnis `budget` mit der Dateierweiterung `.txt` von den Bändern auf der Einheit `/dev/rmt0` in den ursprünglichen Quellenpfad zurückschreiben.

```
dsmc restore backupset "/home/budget/*.txt"
-backupsetname=/dev/rmt0 -loc=tape
```

Task Den gesamten Sicherungssatz zurückschreiben, der in der lokalen Datei `/home/jones/bset01.file` enthalten ist.

```
dsmc restore backupset
-backupsetname="/home/jones/bset01.file"
-loc=file
```

Task Gruppen aus dem Sicherungssatz `mybackupset.12345678` auf dem IBM Spectrum Protect-Server in das Verzeichnis `/home/devel/projectb` zurückschreiben. Der virtuelle Dateibereich der Gruppen ist `accounting`.

```
dsmc restore backupset {/accounting}/*
/home/devel/projectb/
-backupsetname=mybackupset.12345678 -loc=server
-subdir=yes
```

Task Gruppen aus dem lokalen Sicherungssatz `mybackupset.ost` in das Verzeichnis `/home/devel/projectb/` zurückschreiben. Der virtuelle Dateibereich der Gruppen ist `accounting`.

```
dsmc restore backupset {/accounting}/*
/home/devel/projectb/
-backupsetname=mybackupset.ost
-loc=server -subdir=yes
```

Sicherungssätze zurückschreiben: Hinweise und Einschränkungen

In diesem Abschnitt sind einige Hinweise und Einschränkungen aufgeführt, die Sie beim Zurückschreiben von Sicherungssätzen beachten müssen.

Hinweise für das Zurückschreiben von Sicherungssätzen

Beachten Sie beim Zurückschreiben von Sicherungssätzen die folgenden Hinweise:

- Wenn das zurückzuschreibende Objekt auf einem Clientknoten generiert wurde, dessen Name sich von Ihrem aktuellen Knotennamen unterscheidet, geben Sie in allen Zurückschreibungsbefehlen den ursprünglichen Knotennamen im Parameter **filespace** an.
- Ist das Zurückschreiben eines Sicherungssatzes von einem austauschbaren Datenträger nicht möglich, ist zusammen mit dem IBM Spectrum Protect-Administrator zu überprüfen, ob der austauschbare Datenträger auf einer Einheit erstellt wurde, auf der ein kompatibles Format verwendet wurde.
- Wenn Sie den Befehl **restore backupset** in der Anfangsbefehlszeile mit dem Parameter **-location=tape** oder **-location=file** verwenden, versucht der Client nicht, eine Verbindung zum IBM Spectrum Protect-Server herzustellen.
- Beim Zurückschreiben einer Gruppe aus einem Sicherungssatz:
 - Die gesamte Gruppe bzw. alle Gruppen im virtuellen Dateibereich werden zurückgeschrieben. Wenn sich in einem virtuellen Dateibereich mehrere Gruppen befinden, ist es nicht möglich, durch Angabe des Gruppennamens eine einzige Gruppe zurückzuschreiben. Es ist nicht möglich, durch Angabe eines Dateipfads eine Gruppe teilweise zurückzuschreiben.
 - Geben Sie eine Gruppe über einen der folgenden Werte an:
 - Geben Sie den Namen des virtuellen Dateibereichs mit dem Parameter **Dateibereichsname** an.
 - Verwenden Sie die Option **subdir**, um Unterverzeichnisse einzuschließen.
- Eine begrenzte Unterstützung wird für das Zurückschreiben von Sicherungssätzen auf Bandeinheiten bereitgestellt, die an das Clientsystem angeschlossen sind. Sie müssen immer einen nativen Einheitentreiber verwenden, der vom Hersteller der Einheit bereitgestellt wird. Der Einheitentreiber, der von IBM für die Verwendung mit dem IBM Spectrum Protect-Server bereitgestellt wird, kann nicht auf dem Clientsystem zum Zurückschreiben lokaler Sicherungssätze benutzt werden.
- Enthält ein Sicherungssatz Dateien von mehreren Eignern, ist der Sicherungssatz selbst Eigentum der Rootbenutzer-ID und er wird Benutzer-IDs ohne Rootberechtigung nicht angezeigt. In diesem Fall können Benutzer-IDs ohne Rootberechtigung ihre Dateien zurückschreiben, indem sie den Namen des Sicherungssatzes vom IBM Spectrum Protect-Administrator anfordern. Andere Benutzer als Root können nur eigene Dateien zurückschreiben.
- Soll die grafische Benutzerschnittstelle des Clients einen Sicherungssatz von einer lokalen Einheit zurückschreiben, ohne dass eine Serververbindung erforderlich ist, verwenden Sie die Option **localbackupset**.

Einschränkungen beim Zurückschreiben von Sicherungssätzen

Beachten Sie beim Zurückschreiben von Sicherungssätzen die folgenden Einschränkungen:

- Sicherungssatzdaten, die mit der API gesichert wurden, können weder zurückgeschrieben noch verwendet werden.
- Mit dem Befehl **restore backupset** können Sie keine Imagedaten aus einem Sicherungssatz zurückschreiben. Imagedaten aus einem Sicherungssatz können Sie nur mit dem Befehl **restore image** zurückschreiben.
- Sie können keine Imagedaten aus einem lokalen Sicherungssatz (`location=tape` oder `location=file`) zurückschreiben. Imagedaten aus einem Sicherungssatz können Sie nur vom IBM Spectrum Protect-Server zurückschreiben.

Zugehörige Verweise:

„Localbackupset“ auf Seite 500

„Restore“ auf Seite 771

„Restore Image“ auf Seite 786

„Restore Backupset“ auf Seite 777

Sicherungssätze in einer SAN-Umgebung zurückschreiben

Sie können Sicherungssätze auf folgende Weise in einem Speicherbereichsnetz (SNA) zurückschreiben:

- Befindet sich der Sicherungssatz auf einer an ein SAN angeschlossenen Speichereinheit, geben Sie die Einheit mit dem Parameter *filename* an und verwenden die Option `location=tape`, soweit zutreffend. Der Client für Sichern/Archivieren schreibt den Sicherungssatz direkt von der an das SAN angeschlossenen Speichereinheit zurück und erzielt bei der Zurückschreibung eine hohe Geschwindigkeit.

Anmerkung: Sie müssen sicherstellen, dass in dem an das SAN angeschlossenen Bandlaufwerk das korrekte Band geladen ist, bevor Sie den Befehl **restore** ausgeben. Der Client für Sichern/Archivieren initiiert einen SCSI-Kassettenwechsler nicht dazu, das Band automatisch zu laden.

- Befindet sich der Sicherungssatz nicht auf einem lokalen Datenträger oder auf einer an ein SAN angeschlossenen Speichereinheit, können Sie den Sicherungssatz mit der Option `backupsetname` angeben. Verwenden Sie die Option `location=server`, um den Sicherungssatz direkt vom Server mit Hilfe des LAN zurückzuschreiben.

Restore Backupset ohne Parameter backupsetname

Der Befehl **restore backupset** kann ohne den Parameter **backupsetname** verwendet werden.

Die bevorzugte Syntax für den Befehl **restore backupset** erfordert den Parameter **backupsetname**. Vor der Einführung des Parameters **backupsetname** hat der Client für Sichern/Archivieren beim Zurückschreiben von Sicherungssätzen eine andere Syntax verwendet. Die vorherige Syntax wird zwar unterstützt, es wird jedoch empfohlen, wann immer möglich die Syntax zu verwenden, die den Parameter **backupsetname** erfordert. Die vorherige Syntax wird für die Fälle dokumentiert, in denen sie nicht durch die bevorzugte Syntax ersetzt werden kann.

Name des Sicherungssatzes

Gibt den Namen des Sicherungssatzes auf dem IBM Spectrum Protect-Server an. Wird der Parameter **location** angegeben, müssen Sie **-location=server** angeben.

Name der lokalen Datei

Gibt den Dateinamen des ersten Datenträgers des Sicherungssatzes an. Sie müssen **-location=file** angeben.

Bandeinheit

Gibt den Namen der Bandeinheit an, die den Datenträger des Sicherungssatzes enthält. Sie müssen einen von Windows bereitgestellten Einheitentreiber und nicht den von IBM bereitgestellten Einheitentreiber verwenden. Sie müssen **-location=tape** angeben.

LOCation=

Gibt die Position des Sicherungssatzes an. Wenn Sie den Parameter **location** nicht angeben, sucht der Client auf dem IBM Spectrum Protect-Server nach Sicherungssätzen. Wenn Sie den Parameter **'location'** angeben, muss der Wert einer der folgenden drei Auswahlmöglichkeiten entsprechen.

server Gibt an, dass der Sicherungssatz sich auf dem Server befindet. **Server** ist die Standardposition.

file Gibt an, dass der Sicherungssatz sich auf einem verfügbaren Dateisystem befindet.

tape Gibt an, dass der Sicherungssatz sich auf einer verfügbaren Bandeinheit befindet.

Beispiele

Task Den gesamten Sicherungssatz mit dem Namen **monthly_financial_data.87654321** vom Server zurückschreiben.

```
dsmc restore backupset monthly_financial_data.87654321 -loc=server
```

Task Den gesamten Sicherungssatz zurückschreiben, der in der Datei **/home/budget/weekly_budget_data.ost** enthalten ist.

```
dsmc restore backupset "/home/budget/weekly_budget_data.ost" -loc=file
```

Task Den gesamten Sicherungssatz von der Einheit **/dev/rmt0** zurückschreiben.

```
dsmc restore backupset "/dev/rmt0" -loc=tape
```

Task Die einzelne Datei mit dem Namen **/home/jones/budget.dev** von der Einheit **/dev/rmt0** in den ursprünglichen Quellenpfad zurückschreiben.

```
dsmc restore backupset /dev/rmt0 "/home/jones/budget.dev" -loc=tape
```

Task Alle Dateien im Verzeichnis **budget** mit der Dateierweiterung **.txt** von dem Band/den Bändern auf der Einheit **/dev/rmt0** in den ursprünglichen Quellenpfad zurückschreiben.

```
dsmc restore backupset /dev/rmt0 "/home/budget/*.txt" -loc=tape
```

Task Den gesamten Sicherungssatz zurückschreiben, der in der lokalen Datei **/home/jones/bset01.file** enthalten ist.

```
dsmc restore backupset "/home/jones/bset01.file" -loc=file
```

Task Gruppen aus dem Sicherungssatz **mybackupset.12345678** auf dem IBM

Spectrum Protect-Server in das Verzeichnis /home/devel/projectb zurückschreiben. Der virtuelle Dateibereich der Gruppen ist accounting.

```
dsmc restore backupset mybackupset.12345678 {/accounting}/*  
/home/devel/projectb/ -loc=server -subdir=yes
```

Task Gruppen aus dem lokalen Sicherungssatz mybackupset.ost in das Verzeichnis /home/devel/projectb/ zurückschreiben. Der virtuelle Dateibereich der Gruppen ist accounting.

```
dsmc restore backupset mybackupset.ost {/accounting}/*  
/home/devel/projectb/ -loc=server -subdir=yes
```

Zugehörige Informationen

„Daten aus einem Sicherungssatz zurückschreiben“ auf Seite 250

Restore Group

Verwenden Sie den Befehl **restore group**, um bestimmte Member oder alle Member einer Gruppensicherung zurückzuschreiben.

Anmerkung:

1. Verwenden Sie die Option **pick**, um eine Liste der Gruppen anzuzeigen, aus der Sie eine zurückzuschreibende Gruppe auswählen können.
2. Verwenden Sie die Option **showmembers** in Verbindung mit der Option **pick**, um einzelne oder mehrere Member einer Gruppe anzuzeigen und zurückzuschreiben. In diesem Fall wählen Sie zunächst die Gruppe aus, von der Sie Member zurückschreiben wollen, und anschließend wählen Sie ein oder mehrere Member der Gruppe aus, die zurückgeschrieben werden sollen.
3. Sie können eine Gruppe aus einem Sicherungssatz zurückschreiben.

Unterstützte Clients

Dieser Befehl ist für alle Clients außer Mac OS X gültig.

Syntax

```
►► REStore GRoup [Optionen] Quelle [Ziel] ►►
```

Parameter

Quelle

Gibt den Namen des virtuellen Dateibereichs und den Gruppennamen auf dem Server für die Zurückschreibung an.

Ziel

Gibt den Pfad für den Zielort der Gruppe bzw. der Member der Gruppe an. Wird kein Zielort angegeben, schreibt der Client die Dateien an die ursprüngliche Position zurück.

Tabelle 108. Befehl Restore Group: Zugehörige Optionen

Option	Verwendung
backupsetname „Backupsetname“ auf Seite 370	Nur in der Befehlszeile.
followsymbolic „Followsymbolic“ auf Seite 458	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
fromdate „Fromdate“ auf Seite 461	Nur in der Befehlszeile.
fromnode „Fromnode“ auf Seite 461	Nur in der Befehlszeile.
fromowner „Fromowner“ auf Seite 462	Nur in der Befehlszeile.
fromtime „Fromtime“ auf Seite 463	Nur in der Befehlszeile.
ifnewer „Ifnewer“ auf Seite 468	Nur in der Befehlszeile.
inactive „Inactive“ auf Seite 471	Nur in der Befehlszeile.
latest „Latest“ auf Seite 499	Nur in der Befehlszeile.
pick „Pick“ auf Seite 528	Nur in der Befehlszeile.
pitdate „Pitdate“ auf Seite 529	Nur in der Befehlszeile.
pittime „Pittime“ auf Seite 530	Nur in der Befehlszeile.
preservepath „Preservepath“ auf Seite 537	Nur in der Befehlszeile.
replace „Replace“ auf Seite 547	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
showmembers „Showmembers“ auf Seite 579 (gilt nicht für Mac OS X)	Nur in der Befehlszeile.
subdir „Subdir“ auf Seite 605	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
tapeprompt „Tapeprompt“ auf Seite 607	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
todate „Todate“ auf Seite 621	Nur in der Befehlszeile.
totime „Totime“ auf Seite 622	Nur in der Befehlszeile.

Beispiele

Task Alle Member der Gruppensicherung /virtfs/group1 an ihre ursprüngliche Position auf dem Clientsystem zurückschreiben.

Befehl:

```
restore group /virtfs/group1
```

Task Alle Gruppen im virtuellen Dateibereich /virtfs anzeigen. Die Option **showmembers** verwenden, um eine Liste der Gruppenmember anzuzeigen, aus der Sie zurückzuschreibende Member auswählen können.

Befehl:

```
restore group /virtfs/  
* -pick -showmembers
```

Task Eine Liste der Gruppen im virtuellen Dateibereich /virtfs anzeigen, aus der Sie eine oder mehrere zurückzuschreibende Gruppen auswählen können.

Befehl:

```
restore group /virtfs/* -pick
```

Zugehörige Informationen

„**Restore Backupset**“ auf Seite 777

Restore Image

Mit dem Befehl **restore image** wird ein Dateisystemimage oder das Image eines unformatierten Datenträgers zurückgeschrieben, das mit Hilfe des Befehls **backup image** gesichert wurde.

Bei der Zurückschreibung wird das Sicherungsbild vom IBM Spectrum Protect-Server oder aus einem Sicherungssatz vom IBM Spectrum Protect-Server abgerufen, wenn die Option **backupsetname** angegeben ist. Dieser Befehl kann ein aktives Basisimage oder ein zeitpunktgesteuertes Basisimage mit zugeordneten Teilaktualisierungen zurückschreiben.

Anmerkung:

1. Die Verwendung der Option **incremental** im Befehl **restore image** zur Ausführung einer dynamischen Imagesicherung wird nicht unterstützt.
2. Wenn Sie IBM Spectrum Protect HSM for Windows oder IBM Spectrum Protect for Space Management verwenden, eine Dateisystemimagesicherung zurückschreiben und die Ausführung eines Abgleichs planen, müssen Sie die Dateien zurückschreiben, die nach der Imagesicherung gesichert wurden. Andernfalls verfallen umgelagerte Dateien, die nach der Imagesicherung erstellt wurden, im HSM-Archivierungsspeicher auf dem IBM Spectrum Protect-Server.

Sie können mit der Option **verifyimage** im Befehl **restore image** angeben, dass die Feststellung von defekten Sektoren auf dem Zieldatenträger aktiviert werden soll. Werden defekte Sektoren auf dem Zieldatenträger festgestellt, gibt der Client eine Warnung auf der Konsole und im Fehlerprotokoll aus.

Befinden sich defekte Sektoren auf dem Zieldatenträger, können Sie die Option **imagetofile** im Befehl **restore image** verwenden, um anzugeben, dass das Quellimage in eine Datei zurückgeschrieben werden soll. Später können Sie ein Datenkopierprogramm Ihrer Wahl verwenden, um das Image von der Datei auf einen Plattendatenträger zu übertragen.

Hinweise:

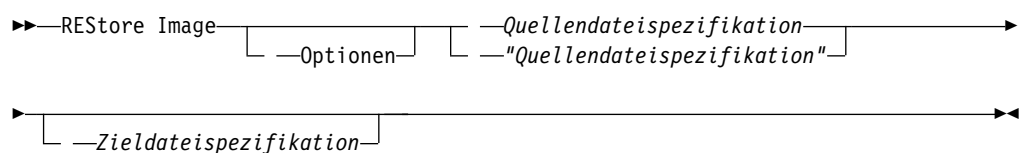
- Die API muss installiert sein, um den Befehl **restore image** verwenden zu können.
- Die Imagezurückschreibung wird für das Sun-Dateisystem QFS nicht unterstützt.

- Die Imagezurückschreibung wird für GPFS-Dateisysteme unter Linux x86_64, Linux on POWER und Linux on System z nicht unterstützt.
- Auf Linux-Systemen verwenden einige Dateisysteme (z. B. ext2, ext3, ext4, btrfs und xfs) eine UUID (Universally Unique Identifier), um sich selbst im Betriebssystem zu identifizieren. Wenn Sie eine Imagesicherung eines solchen Datenträgers erstellen und an eine andere Position zurückschreiben, kann es sein, dass es zwei Datenträger mit derselben UUID gibt. Wenn Sie Ihre Dateisysteme mit einer UUID in /etc/fstab definieren, denken Sie daran, dass der Client für Sichern/Archivieren das zurückgeschriebene Dateisystem unter Umständen wegen eines UUID-Konflikts nicht korrekt anhängen kann. Um diese Situation zu vermeiden, sollten Sie das Image an seine ursprüngliche Position zurückschreiben. Wenn Sie es an eine andere Position zurückschreiben müssen, ändern Sie die UUID des ursprünglichen oder des zurückgeschriebenen Datenträgers, bevor Sie das zurückgeschriebene Dateisystem anhängen. Informationen zur Änderung einer UUID finden Sie in der Linux-Dokumentation. Möglicherweise müssen Sie auch die Datei /etc/fstab manuell bearbeiten, damit der ursprüngliche Datenträger und/oder der zurückgeschriebene Datenträger angehängt werden können.
- Wenn Sie die Option **pick** verwenden, werden die folgenden Informationen für Dateisystemimages angezeigt, die vom Client gesichert wurden:
 - Imagegröße
 - Gespeicherte Größe - Dieser Wert ist die tatsächliche Größe des Images, das auf dem IBM Spectrum Protect-Server gespeichert ist. Das auf dem Server gespeicherte Image hat dieselbe Größe wie der Datenträger.
 - Dateisystemtyp
 - Sicherungsdatum und -zeit
 - Die den Imagesicherungen zugeordnete Verwaltungsklasse
 - Ob die Imagesicherung eine aktive oder inaktive Kopie ist
 - Der Imagenname
- Sollte ein zurückgeschriebenes Image aus irgendeinem Grund beschädigt sein, können Sie versuchen, es mit dem Tool **fsck** zu reparieren.

Unterstützte Clients

Diese Option ist für AIX-, Linux- und Oracle Solaris-Clients gültig.

Syntax



Parameter

Quellendateispezifikation

Der Name eines Quellenimagedateisystems, das zurückgeschrieben werden soll. Es kann nur ein einzelnes Quellenimage angegeben werden. Platzhalterzeichen sind nicht zulässig.

Ziellendateispezifikation

Gibt den Namen eines vorhandenen angehängten Dateisystems oder den Pfad und Dateinamen an, in das/den das Quellendateisystem zurückgeschrieben wird. Standardwert ist die ursprüngliche Position des Dateisystems.

Tabelle 109. Befehl **Restore Image**: Zugehörige Optionen

Option	Verwendung
backupsetname „Backupsetname“ auf Seite 370	Nur in der Befehlszeile.
dateformat „Dateformat“ auf Seite 389	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
deletefiles „Deletefiles“ auf Seite 396	Nur in der Befehlszeile.
fromnode „Fromnode“ auf Seite 461	Nur in der Befehlszeile.
fromowner „Fromowner“ auf Seite 462	Nur in der Befehlszeile.
imagetofile „Imagetofile“ auf Seite 470	Nur in der Befehlszeile.
inactive „Inactive“ auf Seite 471	Nur in der Befehlszeile.
incremental „Incremental“ auf Seite 492	Nur in der Befehlszeile.
noprompt „Noprompt“ auf Seite 519	Nur in der Befehlszeile.
pick „Pick“ auf Seite 528	Nur in der Befehlszeile.
pitdate „Pitdate“ auf Seite 529	Nur in der Befehlszeile.
pittime „Pittime“ auf Seite 530	Nur in der Befehlszeile.
timeformat „Timeformat“ auf Seite 616	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
verifyimage „Verifyimage“ auf Seite 629	Nur in der Befehlszeile.

Durch den Befehl **restore image** wird der Zieldateibereich nicht definiert oder angehängt. Der Zieldatenträger muss vorhanden und groß genug für die Quelle sein und wenn er ein Dateisystem enthält, muss er angehängt sein. Wenn eine Imagesicherung ein Dateisystem enthält und an eine andere Position zurückgeschrieben wird, müssen folgende Punkte beachtet werden:

- Ist der Zieldatenträger kleiner als der Quelledatenträger, schlägt die Operation fehl.
- Wenn der Zieldatenträger größer als die Quelle ist, geht die Größendifferenz nach der Zurückschreibungsoperation verloren. Der verlorene Speicherbereich kann durch Vergrößern des Datenträgers wiederhergestellt werden, wodurch sich auch der zurückgeschriebene Datenträger vergrößert.

Beispiele

Task Das Verzeichnis /home/test, über das der logische Datenträger angehängt wird, an seine ursprüngliche Position zurückschreiben.

Befehl: `dsmc rest image /home/test`

Task Das Verzeichnis `/home/proj`, über das der logische Datenträger angehängt wird, an seine ursprüngliche Position zurückschreiben und die auf dem Server aufgezeichneten Änderungen aus der letzten Teilsicherung des ursprünglichen Images anwenden. Die Änderungen schließen das Löschen von Dateien ein.

Befehl: `dsmc restore image /home/proj -incremental -deletefiles`

Task Das Dateisystem `/usr` an seine ursprüngliche Position zurückschreiben. Verwenden Sie die Option **verifyimage**, um die Feststellung von defekten Sektoren auf dem Zieldatenträger zu aktivieren.

Befehl: `dsmc restore image /usr -verifyimage`

Task Sind defekte Sektoren auf dem Zieldatenträger vorhanden, die Option **imagetofile** verwenden, um das Dateisystem `/usr` in die Datei `/home/usr.img` zurückzuschreiben, sodass Datenverlust vermieden wird.

Befehl: `dsmc restore image /usr /home/usr.img -imagetofile`

Zugehörige Informationen

„Verifyimage“ auf Seite 629

„Imagetofile“ auf Seite 470

Restore NAS

Mit dem Befehl **restore nas** wird das Image eines Dateisystems zurückgeschrieben, das zu einem NAS-Dateiserver gehört (NAS = Network Attached Storage, Netzspeicher). Wenn Sie eine interaktive Befehlszeilensitzung mit einer ID ohne Verwaltungsberechtigung verwenden, werden Sie zur Eingabe einer Administrator-ID aufgefordert.

Der NAS-Dateiserver führt die Gerätedatenversetzung aus. Ein Serverprozess führt die Zurückschreibung durch.

Wenn Sie die Option `toc` im Befehl **backup nas** oder mit der Option `include.fs.nas` verwendet haben, um Inhaltsverzeichnisangaben (TOC - Table of Contents) für jede Dateisystemsicherung zu speichern, können Sie über den Serverbefehl **QUERY TOC** den Inhalt einer Dateisystemsicherung ermitteln und über den Serverbefehl **RESTORE NODE** einzelne Dateien oder Verzeichnisbaumstrukturen zurückschreiben. Sie können auch den Web-Client verwenden, um die gesamte Baumstruktur des Dateisystems zu untersuchen und zurückzuschreibende Dateien und Verzeichnisse auszuwählen. Werden keine TOC-Angaben gespeichert, können Sie über den Befehl **RESTORE NODE** dennoch einzelne Dateien und Verzeichnisstrukturen zurückschreiben, wenn der vollständig qualifizierte Name jeder Datei bzw. jedes Verzeichnisses und das Image bekannt ist, in dem das Objekt gesichert wurde.

Verwenden Sie die Option `nasnodename`, um den Knotennamen für den NAS-Dateiserver anzugeben. Der NAS-Knotenname identifiziert den NAS-Dateiserver für den IBM Spectrum Protect-Server. Sie müssen den NAS-Knotennamen im Server registrieren. Fügen Sie die Option `nasnodename` in Ihre Clientsystemoptionsdatei (`dsm.sys`) ein. Der Wert in der Clientsystemoptionsdatei ist der Standardwert, dieser Wert kann jedoch in der Befehlszeile überschrieben werden.

Sie können mit der Option **pick** eine Liste der NAS-Images anzeigen, deren Eigner der angegebene NAS-Knoten ist. In dieser Liste können Sie Images zum Zurückschreiben auswählen. Wenn Sie mit der Option **pick** mehrere Images zum Zurückschreiben auswählen, dürfen Sie nicht die Option **monitor** verwenden; sonst werden die Zurückschreibungen serialisiert. Wenn Sie beim Zurückschreiben mehrerer Images mehrere Zurückschreibungsprozesse gleichzeitig starten wollen, dürfen Sie nicht **monitor=yes** angeben.

Mit der Option **monitor** geben Sie an, ob Sie eine NAS-Imagezurückschreibung eines Dateisystems überwachen und Verarbeitungsinformationen anzeigen wollen.

Mit dem Befehl **monitor process** können Sie eine Liste der aktuellen Zurückschreibungsprozesse für alle NAS-Knoten anzeigen, für die Ihre Verwaltungsbenutzer-ID eine Berechtigung hat. Die Verwaltungsbenutzer-ID sollte mindestens die Clienteigenerberechtigung sowohl über den NAS-Knoten als auch den Client-Workstation-Knoten besitzen, der entweder von der Befehlszeile oder vom Web aus verwendet wird.

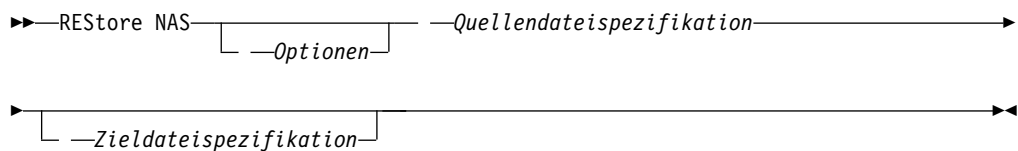
Mit dem Befehl **cancel process** können Sie die NAS-Zurückschreibungsverarbeitung stoppen.

Unabhängig von der Clientplattform wird in NAS-Dateisystemspezifikationen der Schrägstrich (/) als Trennzeichen verwendet. Zum Beispiel: /vol/vol0.

Unterstützte Clients

Dieser Befehl ist nur für AIX- und Solaris-Clients gültig.

Syntax



Parameter

Quelldateispezifikation

Gibt den Namen des NAS-Dateisystemimages an, das Sie zurückschreiben wollen. Dieser Parameter ist erforderlich, wenn Sie nicht die Option **pick** verwenden, um eine Liste der NAS-Images zur Auswahl anzuzeigen. Sie können keine Platzhalterzeichen verwenden, wenn Sie die *Quelldateispezifikation* angeben.

Zielformat

Gibt den Namen eines vorhandenen angehängten Dateisystems auf der NAS-Einheit an, über das Sie das Image zurückschreiben wollen. Dieser Parameter ist optional. Standardwert ist der ursprüngliche Standort des Dateisystems auf der NAS-Einheit.

Tabelle 110. Befehl *Restore NAS*: Zugehörige Optionen

Option	Verwendung
dateformat „Dateformat“ auf Seite 389	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.

Tabelle 110. Befehl `Restore NAS`: Zugehörige Optionen (Forts.)

Option	Verwendung
<code>inactive</code> „Inactive“ auf Seite 471	Nur in der Befehlszeile.
<code>mode</code> „Mode“ auf Seite 509	Nur in der Befehlszeile.
<code>monitor</code> „Monitor“ auf Seite 512	Nur in der Befehlszeile.
<code>nasnodename</code> „Nasnodename“ auf Seite 515	Clientsystemoptionsdatei (dsm.sys) oder Befehlszeile.
<code>numberformat</code> „Numberformat“ auf Seite 521	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
<code>pick</code> „Pick“ auf Seite 528	Nur in der Befehlszeile.
<code>pitdate</code> „Pitdate“ auf Seite 529	Nur in der Befehlszeile.
<code>pittime</code> „Pittime“ auf Seite 530	Nur in der Befehlszeile.
<code>timeformat</code> „Timeformat“ auf Seite 616	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.

Beispiele

Task Das NAS-Dateisystemimage `/vol/vol1` in das Dateisystem `/vol/vol2` auf dem NAS-Dateiserver `nas1` zurückschreiben.

Befehl: `restore nas -nasnodename=nas1 /vol/vol1 /vol/vol2`

Task Inaktive NAS-Images zurückschreiben.

Befehl: `restore nas -nasnodename=nas2 -pick -inactive`

Zugehörige Informationen

„Nasnodename“ auf Seite 515

„Monitor“ auf Seite 512

„Cancel Process“ auf Seite 719

Restore VM

Mit dem Befehl **restore vm** können Sie eine virtuelle Maschine (VM) zurückschreiben, die zuvor gesichert wurde.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Restore VM für virtuelle VMware-Maschinen

Mit dem Befehl **restore vm** können Sie virtuelle VMware-Maschinen oder Schablonen virtueller VMware-Maschinen zurückschreiben.

Wenn der Client für Sichern/Archivieren auf einem separaten System installiert ist, das als vStorage-Sicherungsserver konfiguriert ist, können Sie vollständige Sicherungen virtueller Maschinen auf den ESX- oder ESXi-Server zurückschreiben, von dem sie stammen, oder auf einen anderen Server. Soll eine vollständige Sicherung einer virtuellen Maschine auf einen anderen Server zurückgeschrieben werden, verwenden Sie den Parameter **HOST**. Der Client für Sichern/Archivieren kopiert die Daten vom IBM Spectrum Protect-Server über das LAN oder das SAN. Der Client schreibt die Daten dann direkt auf den ESX-Server, indem die in der Clientoptionsdatei angegebene Transportmethode verwendet wird.

Bei der Zurückschreibung einer vollständigen Sicherung einer virtuellen Maschine wird eine neue virtuelle Maschine erstellt. Die Konfigurationsdaten und der Inhalt der neuen Maschine sind mit den Konfigurationsdaten und dem Inhalt zum Zeitpunkt der Sicherung identisch. Alle Platten der virtuellen Maschine werden bis zum angegebenen Zeitpunkt als virtuelle Platten in der neu erstellten virtuellen Maschine zurückgeschrieben.

Zum Erstellen einer neuen virtuellen Maschine geben Sie den Parameter **vmname** und einen Namen für die neue virtuelle Maschine an. Mit dem Parameter **vmname** wird eine neue virtuelle Maschine mit einer Konfiguration erstellt, die mit der Konfiguration zum Zeitpunkt der Sicherung identisch ist.

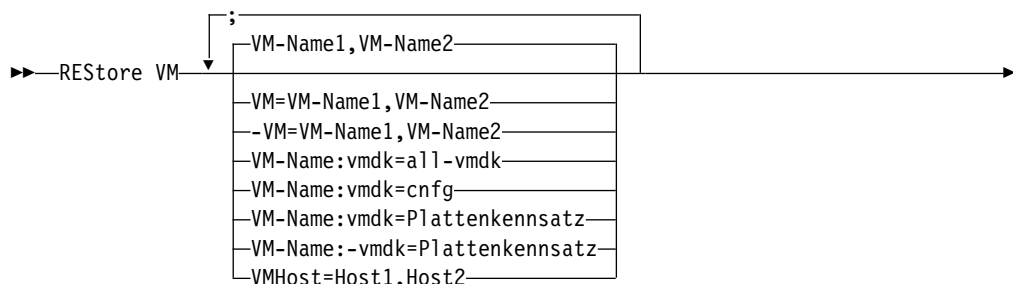
Virtuelle Maschinen werden in ihren ursprünglichen Ressourcenpool, Cluster oder Ordner zurückgeschrieben, falls die Container vorhanden sind. Wenn während einer Zurückschreibungsoperation das Ziel (ein vCenter- oder ESXi-Host) nicht die erforderlichen Container aufweist, wird die VM in die Standardposition auf der höchsten Ebene auf dem ESXi-Zielhost zurückgeschrieben. Wenn Sie eine virtuelle Maschine mithilfe des Befehlszeilenclients zurückschreiben und wenn die virtuelle Maschine nicht an ihre ursprüngliche Position zurückgeschrieben werden kann, wird eine Informationsnachricht (ANS2091I) angezeigt. Wenn Sie eine virtuelle Maschine mithilfe der Java-GUI zurückschreiben und wenn die virtuelle Maschine nicht an ihre ursprüngliche Position zurückgeschrieben werden kann, wird die Informationsnachricht nicht angezeigt. Die virtuelle Maschine wird jedoch trotzdem in die Standardposition auf der höchsten Ebene zurückgeschrieben.

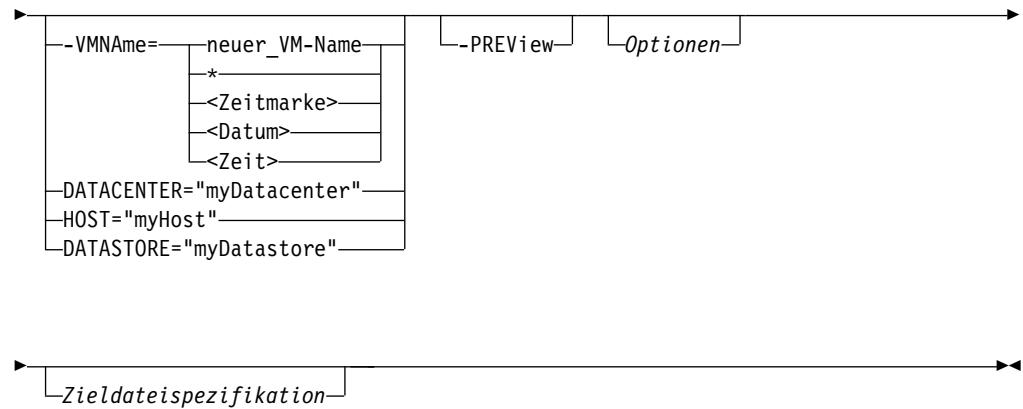
Datenschutztags, die mit dem Befehl **backup vm** gesichert wurden, werden mit der virtuellen Maschine zurückgeschrieben. Datenschutztags werden verwendet, um virtuelle Maschinen von Sicherungen auszuschließen und die Aufbewahrungsmaßnahme für Sicherungen anzugeben.

Unterstützte Clients

Dieser Befehl ist auf unterstützten Linux-Clients gültig, die auf einem vStorage-Sicherungsserver für eine virtuelle VMware-Maschine installiert sind.

Syntax





Parameter

Alle Parameter, die Leerzeichen enthalten, müssen in Anführungszeichen (" ") eingeschlossen werden.

VM-Name

Geben Sie den Namen mindestens einer virtuellen Maschine an, die zurückgeschrieben werden soll. Der Name ist der Anzeigename der virtuellen Maschine. Trennen Sie mehrere VM-Namen durch Kommas voneinander (z. B. vm1,vm2,vm5). Wenn Sie virtuelle Schablonenmaschinen gesichert haben, kann der Parameter *vmname* den Namen einer zurückzuschreibenden virtuellen Schablonenmaschine angeben.

Für die Auswahl von VM-Namen, die einem Muster entsprechen, können Platzhalterzeichen verwendet werden. Ein Stern (*) entspricht einer beliebigen Zeichenfolge. Ein Fragezeichen (?) entspricht einem beliebigen einzelnen Zeichen. Zum Beispiel:

- `restore vm VM_TEST*` schreibt alle virtuellen Maschinen zurück, deren Name mit "VM_TEST" beginnt.
- `restore vm VM??` schreibt alle virtuellen Maschinen zurück, deren Name mit den Buchstaben "VM" beginnt, gefolgt von 2 beliebigen Zeichen.

Es muss mindestens eine zurückzuschreibende virtuelle Maschine angegeben werden.

vm=VM-Name

Das Schlüsselwort `vm=` gibt an, dass die nächste Gruppe von Werten eine Liste mit Namen virtueller Maschinen ist. Das Schlüsselwort `vm=` ist der Standardwert und ist nicht erforderlich.

In den Namen virtueller Maschinen können Platzhalterzeichen verwendet werden. Die Spezifikation des Parameters *vmname* finden Sie in „VM-Name“.

In dem folgenden Beispiel ist `vm=` angegeben und zwei Maschinennamen sind durch Kommas getrennt.

```
restore vm vm=my_vm1,my_vm2
```

-vm=VM-Name

Sie können eine virtuelle Maschine von einer Zurückschreibungsoperation ausschließen, indem Sie den Ausschlussoperator (-) vor dem Schlüsselwort `vm=` angeben.

Mit der Option `-vm=` können Sie eine Liste virtueller Maschinen aus einer größeren VM-Sicherungsgruppe ausschließen, z. B. eine Gruppe virtueller Maschinen, deren Namen mit einem VM-Namensmuster beginnen. Wenn Sie beispielsweise alle virtuellen Maschinen zurückschreiben müssen, deren Namen mit `Dept99_` beginnen, aber das Zurückschreiben von `vm2` verhindern wollen, geben Sie den folgenden Befehl aus:

```
restore vm vm=Dept99_*;-vm=vm2
```

Mithilfe von Platzhalterzeichen im Schlüsselwort `-vm=` können VM-Namen ausgeschlossen werden, die einem Muster entsprechen. Zum Beispiel:

- Alle Dateien ausschließen, deren Hostname die Zeichenfolge `test` enthält:
`-vm=*test*`
- Alle virtuellen Maschinen mit Namen wie den folgenden einschließen:
`test20, test25, test29, test2A:`
`vm=test2?`

Anmerkung: Sie können mit dem Ausschlussoperator (`-`) keine VM-Hostdomäne ausschließen. Der Ausschlussoperator funktioniert nur auf der Ebene der Namen der virtuellen Maschinen.

VM-Name: vmdk=all-vmdk

Diese Option gibt an, dass alle virtuellen Platten (Dateien `*.vmdk`) bei der Zurückschreibung der virtuellen Maschine eingeschlossen werden. Dieser Parameter ist der Standardwert für vmdk-Spezifikationen.

Anmerkung: Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.

VM-Name: vmdk=cnfg

Diese Option gibt an, dass die Konfigurationsinformationen der virtuellen Maschine zurückgeschrieben werden. Die Konfigurationsinformationen werden immer zurückgeschrieben, wenn eine neue virtuelle Maschine erstellt wird. Standardmäßig wird die Konfiguration jedoch nicht zurückgeschrieben, wenn Sie eine vorhandene virtuelle Maschine mit ausgewählten virtuellen Platten aktualisieren.

Normalerweise schlägt das Zurückschreiben von Konfigurationsinformationen auf eine vorhandene virtuelle Maschine fehl, weil ein Konflikt zwischen den zurückgeschriebenen Konfigurationsinformationen und den Konfigurationsinformationen der vorhandenen virtuellen Maschine auftritt. Verwenden Sie diese Option, wenn die vorhandene Konfigurationsdatei einer virtuellen Maschine auf dem ESXi-Server gelöscht wurde und die gesicherte Konfiguration verwendet werden soll, um die Datei erneut zu erstellen.

Anmerkung: Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.

VM-Name: vmdk=Plattenkennsatz

Mit dieser Option wird der Plattenkennsatz einer virtuellen Platte angegeben, die bei der Zurückschreibungsoperation eingeschlossen werden soll. Geben Sie diese Option nur an, wenn mindestens eine bestimmte Platte, aber nicht alle Platten zurückgeschrieben werden sollen. Wiederholen Sie diese Option für jede Platte, die zurückgeschrieben werden soll.

Die folgenden Hinweise gelten für jede Platte, die zurückgeschrieben werden soll:

- Die Platte muss auf der VM vorhanden sein, bevor Sie die Zurückschreibungsoperation einleiten. Wenn die Platte nicht vorhanden ist, müssen Sie sie erstellen. Mit dem Parameter **-preview** können Sie den Kennsatz, die Kapazität und den Datenspeicher der ursprünglichen Platte ermitteln. Die Ausgabe von **-preview** umfasst keine Bereitstellungsinformationen.
- Die vorhandene Platte muss mindestens so groß wie die zurückzuschreibende Platte sein.
- Der Kennsatz der vorhandenen Platte muss mit dem Kennsatz der zurückzuschreibenden Platte übereinstimmen.
- Alle Daten auf der vorhandenen Platte werden überschrieben.

Nur die angegebenen Platten werden zurückgeschrieben. Andere Platten in der VM werden nicht geändert.

Die VM, auf die die Platte zurückgeschrieben wird, muss ausgeschaltet werden, bevor Sie die Zurückschreibungsoperation einleiten.

Erforderlich: Im Befehl **restore vm** müssen die Kennsatznamen der vmdk-Dateien, die bei einer Zurückschreibungsoperation für virtuelle Maschinen (**restore VM** mit dem Parameter **VM-Name:vmdk=Plattenkennsatz**) eingeschlossen werden sollen, als Kennsatznamen in englischer Sprache angegeben werden. Der Kennsatzname muss der Ausgabe des Kennsatznamens übereinstimmen, die vom Parameter **-preview** angezeigt wird. Beispiele für die englischen vmdk-Kennsätze sind "Hard Disk 1", "Hard Disk 2" usw.

Anmerkung: Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.

VM-Name:-vmdk=Plattenkennsatz

Mit dieser Option wird der Plattenkennsatz mindestens einer virtuellen Platte angegeben, die von der Zurückschreibungsoperation ausgeschlossen werden soll.

Erforderlich: Im Befehl **restore vm** müssen die Kennsatznamen der vmdk-Dateien, die bei einer Zurückschreibungsoperation für virtuelle Maschinen (**restore VM** mit dem Parameter **VM-Name:vmdk=Plattenkennsatz**) eingeschlossen werden sollen, als Kennsatznamen in englischer Sprache angegeben werden. Der Kennsatzname muss der Ausgabe des Kennsatznamens übereinstimmen, die vom Parameter **-preview** angezeigt wird. Beispiele für die englischen vmdk-Kennsätze sind "Hard Disk 1", "Hard Disk 2" usw.

Anmerkung: Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.

vmhost=Hostname

Mit dieser Option werden alle virtuellen Maschinen zurückgeschrieben, die für das Virtual Center oder den ESX-Server definiert sind, das bzw. der in der Option **vmhost** angegeben ist. Der angegebene Hostname muss genau mit dem vollständig qualifizierten Hostnamen oder der IP-Adresse übereinstimmen, der/die in der Ansicht des vCenter-Servers für **Hosts und Cluster** angegeben ist.

Trennen Sie mehrere Hostnamen durch Kommas voneinander (z. B. **host1,host2,host5**).

Dieser Parameter kann mehrere, durch Kommas getrennte ESX-Server umfassen.

Wenn Sie eine direkte Verbindung zu einem ESXi- oder ESX-Host herstellen, ist die Option `vmhost` nur gültig, wenn **vmhost** der Server ist, zu dem Sie eine Verbindung herstellen. Andernfalls wird eine Warnung an die Konsole gesendet und in der Datei `dserror.log` aufgezeichnet; sie wird auch als Serverereignisnachricht aufgezeichnet.

Wenn Sie Schablonen für virtuelle Maschinen gesichert haben, sind diese in der Zurückschreibungsoperation eingeschlossen.

VMName=

Gibt den neuen Namen der virtuellen Maschine nach der Zurückschreibung an, wenn nicht der mit dem Parameter `VM=` angegebene Name verwendet werden soll.

neuer_VM-Name

Geben Sie einen neuen VM-Namen für die zurückgeschriebene virtuelle Maschine an.

Die folgenden Zeichen werden in Namen zurückgeschriebener virtueller Maschinen nicht unterstützt:

: ; ' \ / " ? , < > |

Ein Zurückschreibungsbefehl, der nicht unterstützte Zeichen enthält, schlägt mit Fehlermeldung ANS9117E fehl.

VMware unterstützt keine VM-Namen mit einer Länge von mehr als 80 Zeichen.

- * Das Symbol * (Stern) können Sie als Platzhalterzeichen verwenden, um den ursprünglichen Namen der zurückzuschreibenden virtuellen Maschine darzustellen. Indem gültige Zeichen vor oder hinter dem Stern angegeben werden, wird ein Präfix oder Suffix für den Namen der zurückgeschriebenen virtuellen Maschine erstellt.

Die folgenden Zeichen werden in Namen zurückgeschriebener virtueller Maschinen nicht unterstützt:

: ; ' \ / " ? , < > |

Ein Zurückschreibungsbefehl, der nicht unterstützte Zeichen enthält, schlägt mit Fehlermeldung ANS9117E fehl.

VMware unterstützt keine VM-Namen mit einer Länge von mehr als 80 Zeichen.

Sie können das Symbol * wie folgt verwenden:

- Den ursprünglichen Namen der virtuellen Maschine durch Angabe von **vmname=*** als Namen der zurückgeschriebenen virtuellen Maschine verwenden.
- Für die zurückgeschriebene virtuelle Maschine ein Suffix an den ursprünglichen Namen der virtuellen Maschine anhängen. Lautet der ursprüngliche Name der virtuellen Maschine z. B. VM1, können Sie mit dem folgenden Befehl das Suffix "_restored" an VM1 anhängen:

```
dsmc restore vm VM1 -VMName=*_restored
```

Der Name der zurückgeschriebenen virtuellen Maschine ist VM1_restored.

- Für die zurückgeschriebene virtuelle Maschine ein Präfix vor dem ursprünglichen Namen der virtuellen Maschine anfügen. Lautet der ur-

sprüngliche Name der virtuellen Maschine z. B. VM2, können Sie mit dem folgenden Befehl das Präfix "new_" vor VM2 anfügen:

```
dsmc restore vm VM2 -vmname=new_*
```

Der Name der zurückgeschriebenen virtuellen Maschine ist new_VM2.

<Zeitmarke>

Fügt eine Zeitmarke mit dem Datum und der Uhrzeit der Zurückschreibungsoperation an den Namen der zurückgeschriebenen virtuellen Maschine an. Der Parameter <Zeitmarke> ist ein Schlüsselwort und muss zwischen spitzen Klammern ("<" und ">") stehen. Das Format der Zeitmarkenzeichenfolge wird durch die Optionen DATEFORMAT und TIMEFORMAT in der Datei dsm.opt festgelegt. In der vom Parameter <Zeitmarke> zurückgegebenen Zeitmarke wird ein Gedankenstrich als Trennzeichen verwendet.

Sollen beispielsweise zwei virtuelle Maschinen mit dem Namen VM5 und VM6 zurückgeschrieben und das Datum und die Uhrzeit der Zurückschreibung an die Namen der zurückgeschriebenen virtuellen Maschinen angehängt werden, geben Sie den folgenden Befehl aus:

```
dsmc restore vm VM5,VM6 -vmn=*_<Zeitmarke>
```

Die Namen der zurückgeschriebenen virtuellen Maschinen könnten VM5_06-22-2017_14-56-55 und VM6_06-22-2017_14-56-55 lauten.

<Datum>

Fügt das Datum der Zurückschreibungsoperation an den Namen der zurückgeschriebenen virtuellen Maschine an. Der Parameter <Datum> ist ein Schlüsselwort und muss zwischen spitzen Klammern ("<" und ">") stehen. Das Format der Datumszeichenfolge wird durch die Option DATEFORMAT der Datei dsm.opt festgelegt. In dem vom Parameter <Datum> zurückgegebenen Datum wird ein Gedankenstrich als Trennzeichen verwendet.

Soll beispielsweise das Präfix "new_" in den Namen der virtuellen Maschine VM3 eingefügt und das Zurückschreibungsdatum an den Namen der zurückgeschriebenen virtuellen Maschine angehängt werden, geben Sie den folgenden Befehl aus:

```
dsmc restore vm VM3 -vmname=new_*_<Datum>
```

Der Name der zurückgeschriebenen virtuellen Maschine könnte new_VM3_06-22-2017 lauten.

<Zeit>

Fügt die Uhrzeit der Zurückschreibungsoperation an den Namen der zurückgeschriebenen virtuellen Maschine an. Der Parameter <Zeit> ist ein Schlüsselwort und muss zwischen spitzen Klammern ("<" und ">") stehen. Das Format der Zeitzeichenfolge wird durch die Option TIMEFORMAT der Datei dsm.opt festgelegt. In der vom Parameter <Zeit> zurückgegebenen Uhrzeit wird ein Gedankenstrich als Trennzeichen verwendet.

Soll beispielsweise das Suffix "_today_" an den Namen der virtuellen Maschine VM8 angehängt und die Zurückschreibungszeit an den Namen der zurückgeschriebenen virtuellen Maschine angehängt werden, geben Sie den folgenden Befehl aus:

```
dsmc restore vm VM8 -vmn=*_today_<Zeit>
```

Der Name der zurückgeschriebenen virtuellen Maschine könnte VM8_today_14-56-55 lauten.

Anmerkung: Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, oder bei Angabe von LOCAL für den Parameter **FROM** nicht gültig.

DATACENTER

Gibt den Namen des Datacenters, in das die virtuelle Maschine zurückgeschrieben werden soll, gemäß Definition in vSphere vCenter an. Wenn das Datacenter in einem Ordner enthalten ist, müssen Sie die Option **-datacenter** angeben, wenn Sie die virtuelle Maschine zurückschreiben, und die Ordnerstruktur des Datacenters in den Datacenternamen einschließen. Die folgende Syntax ist beispielsweise gültig:

`-datacenter=Ordnername/Datacentername`

Wenn Sie eine virtuelle Maschine mithilfe der grafischen Benutzerschnittstelle zurückschreiben, müssen Sie die virtuelle Maschine an eine andere Position zurückschreiben. Erfolgt die Zurückschreibung an die ursprüngliche Position, kann der Ordnername des Datacenters nicht angegeben werden. Ohne einen Ordnernamen zum Lokalisieren des ursprünglichen Datacenters schlägt die Zurückschreibungsoperation fehl.

Anmerkung: Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.

HOST

Gibt den Domännennamen des ESX-Host-Servers an, auf den zurückgeschrieben wird (wie in vSphere vCenter definiert).

Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden und sein Wert muss mit dem Hostnamen übereinstimmen, der im VMware vSphere-Web-Client angezeigt wird. Um den Hostnamen im vSphere-Web-Client zu bestätigen, wählen Sie einen Host aus und klicken Sie auf **Verwalten > Netzbetrieb > TCP/IP-Konfiguration > DNS**.

Anmerkung: Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.

DATASTORE

Gibt den VMware-Datenspeicher an, in den die virtuelle Maschine zurückgeschrieben werden soll. Der Datenspeicher kann sich auf einer SAN-, NAS- oder iSCSI-Einheit oder auf einem virtuellen VMware-Datenträger (VVOL) befinden. Sie können nur einen Datenspeicher angeben, wenn Sie eine virtuelle Maschine zurückschreiben. Wenn Sie keinen Parameter **datastore** angeben, wird die VMDK-Datei der virtuellen Maschine in den Datenspeicher zurückgeschrieben, in dem sie sich befunden hat, als die Sicherung erstellt wurde.

Anmerkung: Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.

-PREVIEW

Mit diesem Parameter können Sie die Ergebnisse einer Zurückschreibungsoperation überprüfen, ohne virtuelle Maschinen (VMs) zurückzuschreiben. Der Parameter **-preview** stellt eine Liste der virtuellen Maschinen, die zurückgeschrieben werden, sowie Informationen zu den virtuellen Maschinen (z. B. Kennsätze der Festplatten in der virtuellen Maschine und die Verwaltungsklasse für eine virtuelle Maschine) zur Verfügung.

Wenn Sie den Parameter **-preview** mit dem Befehl **restore vm** ausgeben, wird die Zurückschreibungsoperation nicht gestartet. Die Zurückschreibungsoperation wird nur gestartet, wenn der Parameter **-preview** aus dem Befehl entfernt wird.

Weitere Informationen finden Sie in Zurückschreibungsoperationen virtueller Maschinen voranzeigen.

Tabelle 111. Befehl Restore VM: Für die Zurückschreibung virtueller VMware-Maschinen verwendete zugehörige Optionen

Option	Verwendung
datacenter	Befehlszeile oder Optionsdatei. Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.
Datastore	Befehlszeile oder Optionsdatei. Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.
host	Befehlszeile oder Optionsdatei. Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.
inactive	Befehlszeile.
pick	Befehlszeile. Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.
pitdate	Befehlszeile. Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.
pittime	Befehlszeile. Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.
vmbackdir	Befehlszeile oder Clientoptionsdatei
vmbackuplocation	Befehlszeile
vmbackuptype	Befehlszeile oder Clientoptionsdatei
vmchost	Befehlszeile oder Clientoptionsdatei
vmcpw	Befehlszeile oder Clientoptionsdatei
vmcuser	Befehlszeile oder Clientoptionsdatei
vmdefaultdvportgroup	Befehlszeile oder Clientoptionsdatei
vmdefaultdvswitch	Befehlszeile oder Clientoptionsdatei
vmdefaultnetwork	Befehlszeile oder Clientoptionsdatei
vmdiskprovision	Befehlszeile oder Clientoptionsdatei
Dieser Parameter ist nur gültig, wenn instantrestore als Wert für vmrestoretype angegeben wird.	

Tabelle 111. Befehl Restore VM: Für die Zurückschreibung virtueller VMware-Maschinen verwendete zugehörige Optionen (Forts.)

Option	Verwendung
vmexpireprotect Dieser Parameter ist nur gültig, wenn instantaccess oder instantrestore als Wert für vmrestoretype angegeben wird.	Befehlszeile oder Clientoptionsdatei
vmiscsiadapter Dieser Parameter ist nur gültig, wenn instantaccess oder instantrestore als Wert für vmrestoretype angegeben wird.	Befehlszeile oder Clientoptionsdatei
vmmaxrestoresessions	Befehlszeile oder Clientoptionsdatei
vmmaxrestoreparalleldisks	Befehlszeile oder Clientoptionsdatei
vmmaxrestoreparallelvms	Befehlszeile oder Clientoptionsdatei
vmmountage	Befehlszeile.
vmnoprdmdisks	Befehlszeile oder Clientoptionsdatei
vmnovrdmdisks	Befehlszeile oder Clientoptionsdatei
vmstoragetype Dieser Parameter ist nur gültig, wenn instantaccess oder instantrestore als Wert für vmrestoretype angegeben wird.	Befehlszeile oder Clientoptionsdatei
vmstortransport	Befehlszeile oder Clientoptionsdatei Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.

Beispiele

Task Die neueste Sicherungsversion von *eigene_VM* mit dem ursprünglichen Namen zurückschreiben. Die VMware-Verwaltungsschnittstelle verwenden, um die ursprüngliche virtuelle Maschine zu löschen, bevor sie mit dieser Syntax zurückgeschrieben wird.

```
dsmc restore vm eigene_VM
```

Task Die neueste Sicherungsversion von *myvm* auf eine neue virtuelle Maschine zurückschreiben, die mit dem Namen „Test Machine“ erstellt wird. Im Befehl sind für das Zurückschreibungsziel das Datacenter, der ESX-Host und der Datenspeicher angegeben.

```
dsmc restore vm eigene_VM -vmname="Testmaschine"
-datacenter="eigenes_Datacenter" -host="eigener_Host"
-datastore="eigener_Datenspeicher"
```

Task Die neueste Sicherungsversion von *eigene_VM* mit dem neuen Namen *eigene_VM_nach_Zurückschreibung* zurückschreiben.

```
dsmc restore vm eigene_VM -vmname="* nach Zurückschreibung"
-datacenter="eigenes_Datacenter" -host="eigener_Host"
-datastore="eigener_Datenspeicher"
```

Task Die neueste Sicherungsversion von *eigene_VM* mit einem neuen Namen zurückschreiben, der Datum und Uhrzeit ähnlich wie in dem Beispiel *eigene_VM_03-22-2017_14-41-24* anzeigt.

```
dsmc restore vm eigene_VM -vmname="* <Zeitmarke>"
-datacenter="eigenes_Datacenter" -host="eigener_Host"
-datastore="eigener_Datenspeicher"
```

- Task** Die neueste Sicherungsversion von *eigene_VM* zurückschreiben. Die Zurückschreibung in ein Datacenter mit dem Namen *eigenes_Datacenter* ausführen. Das Datacenter befindet sich in vCenter; der relative Pfad in vCenter lautet *dirA/datacenters/*.

```
dsmc restore vm eigene_VM -vmname="Testmaschine"
-datacenter="dirA/datacenters/eigenes_Datacenter"
-host="eigener_Host" -datastore="eigener_Datenspeicher"
```

- Task** Eine Schablone für virtuelle Maschinen an dieselbe Position und mit demselben Namen zurückschreiben.

```
dsmc restore vm VM-Schablonenname
```

- Task** Eine Schablone für virtuelle Maschinen an eine andere Position zurückschreiben.

```
dsmc restore vm VM-Schablonenname -vmname=neuer_Name
-datastore=neuer_Datenspeicher -host=neuer_Host
-datacenter=neues_Datacenter
```

- Task** Nur Festplatte 2 und Festplatte 3 auf die vorhandene virtuelle Maschine mit dem Namen *vm1* zurückschreiben.

```
dsmc restore vm "vm1:vmdk=Festplatte 2:vmdk=Festplatte 3"
```

- Task** Alle Platten auf die vorhandene virtuelle Maschine mit dem Namen *vm1* zurückschreiben, aber die Daten von Festplatte 4 nicht zurückschreiben.

```
dsmc restore vm "vm1:-vmdk=Festplatte 4"
```

- Task** Nur die Daten von Festplatte 1 auf die vorhandene virtuelle Maschine *vm1* zurückschreiben; die Konfigurationsinformationen sollen nicht aktualisiert werden.

Anmerkung: Wenn Sie eine vorhandene virtuelle Maschine zurückschreiben, ist das Standardverhalten, die Konfigurationsinformationen nicht zu aktualisieren.

```
dsmc restore vm "vm1:vmdk=Festplatte 1:-vmdk=cnfg"
```

- Task** Alle Platten auf die vorhandene virtuelle Maschine mit dem Namen *vm1* zurückschreiben.

```
dsmc restore vm "vm1:vmdk=all-vmdk"
```

Dieser Befehl aktualisiert alle virtuellen Platten auf einer vorhandenen virtuellen Maschine mit dem Namen *vm1*. Hierbei besteht ein Unterschied zu der mit `dsmc restore vm vm1` ausgeführten Aktion, bei der eine neue virtuelle Maschine mit dem Namen *vm1* erstellt wird (*vm1* darf nicht vorhanden sein, damit `dsmc restore vm vm1` erfolgreich ist).

- Task** Maximal drei Sitzungen für Zurückschreibungsoperationen für virtuelle Platten in der VM *vm1* festlegen:

```
dsmc restore vm vm1 -vmmxrestoresessions=3
```

- Task** Die virtuelle Maschine mit dem Namen 'Accounts' und alle virtuellen Maschinen, deren Namen mit *Dept99* beginnen, zurückschreiben:

```
dsmc restore vm Accounts,Dept99*
```

- Task** Alle virtuellen Maschinen zurückschreiben, deren Name mit dem Wort "Payroll" beginnt, und alle virtuellen Maschinen ausschließen, deren Name das Wort "temp" enthält:

```
dsmc restore vm vm=Payroll*;-vm=*temp*
```

Task Die virtuellen Maschinen VM1, VM2 und VM3 mit neuen VM-Namen zurückschreiben, die auf den ursprünglichen VM-Namen basieren. Das Suffix "_restored_" und das Datum und die Uhrzeit der Zurückschreibungsoperation an den Namen der virtuellen Maschine anfügen:

```
dsmc restore vm vm=VM1,VM2,VM3 -vmname=*_restored_<Zeitmarke>
```

Die Namen der zurückgeschriebenen virtuellen Maschinen könnten VM1_restored_07-28-2017_13-28-00, VM2_restored_07-28-2017_13-28-00 und VM2_restored_07-28-2017_13-28-00 lauten.

Task Alle virtuellen Maschinen von Host esx03 zurückschreiben, die auf dem IBM Spectrum Protect-Server gesichert wurden, und aus allen virtuellen Maschinen, die zurückgeschrieben werden, die virtuelle Maschine mit dem Namen esx03-02 ohne die VM-Platte Hard Disk 1 zurückschreiben:

```
dsmc restore vm VMHOST=esx03.example.com;esx03-2:-vmdk=Hard Disk 1
```

Task Alle virtuellen Maschinen auf den ESXi-Hosts mit den Namen brovar, doomzoo und kepler zurückschreiben:

```
dsmc restore vm  
vmhost=brovar.example.com,doomzoo.example.com,kepler.example.com
```

Task Überprüfen, ob die virtuelle Maschine mit dem Namen Dept99_VM1 korrekt zurückgeschrieben wird, ohne die virtuelle Maschine tatsächlich zurückzuschreiben:

```
dsmc restore vm VM=Dept99_VM1 -vmname=*_restored -preview
```

Wichtig: Für virtuelle Windows-Maschinen: Wenn Sie versuchen, eine vollständige VM-Zurückschreibung einer Sicherung mit Anwendungsschutz auszuführen, die mit zwei oder mehr Versuchen zur Erstellung einer Momentaufnahme erstellt wurde, ist die Momentaufnahme des Systemproviders auf der zurückgeschriebenen virtuellen Maschine (VM) vorhanden. Während die Anwendung Daten auf die Platte schreibt, wächst der Schattenspeicherbereich, bis nicht mehr genügend Plattenspeicher verfügbar ist.

Im Allgemeinen darf, wenn während einer Sicherung Anwendungsschutz verwendet wurde, nur die Zurückschreibung mit Anwendungsschutz verwendet werden. Wenn Sie die Anwendung zurückschreiben, wird der Datenträger automatisch zurückgesetzt. Wenn Sie jedoch die vollständige virtuelle Maschine zurückschreiben müssen, müssen Sie die Schattenkopie zurücksetzen oder löschen.

Stellen Sie nach der Zurückschreibung der gesamten virtuellen Maschine sicher, dass die Zurückschreibung erfolgreich war und die Daten nicht beschädigt sind. Wenn die Daten nicht beschädigt sind, löschen Sie die Schattenkopie. Wenn die Daten beschädigt sind, setzen Sie die Schattenkopie zurück, um die Datenintegrität wiederherzustellen.

Sie können die Schattenkopie, die gelöscht oder zurückgesetzt werden soll, mithilfe der Datei dsmShadowCopyID.txt im Stammverzeichnis jedes zurückgeschriebenen Datenträgers bestimmen. Diese Datei enthält die Momentaufnahme-IDs der Schattenkopien, die während der Versuche zur Erstellung einer Momentaufnahme erstellt wurden. Mit dem **diskshadow-Befehl delete shadows** können Sie diese IDs löschen; mit dem Befehl **revert** können Sie die Schattenkopie zurücksetzen. Nachdem das Löschen oder Zurücksetzen abgeschlossen ist, können Sie auch die Datei dsmShadowCopyID.txt löschen.

Weitere Informationen finden Sie in „INCLUDE.VMSNAPSHOTATTEMPTS“ auf Seite 485.

Zugehörige Informationen:

Umgebung für Gesamtsicherungen virtueller VMware-Maschinen vorbereiten

Exclude-Optionen für virtuelle Maschinen

Include-Optionen für virtuelle Maschinen

Zurückschreibungsoperationen virtueller Maschinen voranzeigen

Mit dem Parameter `-preview` können Sie die Ergebnisse einer Zurückschreibungsoperation überprüfen, ohne virtuelle Maschinen (VMs) zurückzuschreiben. Der Parameter `-preview` liefert eine Liste der virtuellen Maschinen, die zurückgeschrieben werden, sowie Informationen zu den virtuellen Maschinen. Informationen zur Verwendung des Parameters `-preview` im Befehl **restore vm** finden Sie in den Informationen zu den angezeigten Optionen und in den Beispielen des Befehls **restore vm -preview**.

Mit dem Parameter `-preview` werden Optionen und ihre Werte nur angezeigt, wenn die Optionen die Standardwerte überschreiben oder wenn kein Standardwert vorhanden ist.

Welche Optionen angezeigt werden, ist von verschiedenen Faktoren abhängig:

- Die folgenden Optionen sind für alle Zurückschreibungsoperationen für virtuelle Maschinen gültig:

VMNAME
DATACENTER
DATASTORE
HOST

- Die folgenden Optionen werden angezeigt, wenn sie in der Clientoptionsdatei definiert sind:

VMDEFAULTDVPORTGROUP
VMDEFAULTDVSWITCH
VMDEFAULTNETWORK

- Die folgende Option wird nur während der Voranzeige von Operationen, die keine Sofortzurückschreibungsoperationen (Non-Instant Restore) sind, immer angezeigt:

VMBACKDIR

Der für diese Option zurückgegebene Wert sind die Verzeichnis-CTL-Dateien, die sowohl für Sicherungs- als auch für Zurückschreibungsoperationen im Cache gespeichert werden.

- Die folgenden Optionen werden angezeigt, wenn sie während Voranzeigen von Zurückschreibungsoperationen mit Sofortzugriff (Instant Access) definiert sind:

VMDISKPROVISION
VMAUTOSTARTVM

Wenn Sie den Parameter `-preview` mit dem Befehl **restore vm** ausgeben, wird die Zurückschreibungsoperation nicht gestartet. Die Zurückschreibungsoperation wird nur gestartet, wenn der Parameter `-preview` aus dem Befehl entfernt wird.

Beispiele

Task Die Operation zur Zurückschreibung der virtuellen Maschine VM8 voranzeigen und die Platte Hard Disk 1 ausschließen. Die virtuelle Maschine wird mit einem neuen VM-Namen, der mit `-restore` endet, auf den ESXi-Host-Server esx03 zurückgeschrieben.

Der Befehl zeigt außerdem die zu verwendende Portgruppe für die NICs, den verteilten virtuellen Switch (dvSwitch), der die Portgruppe enthält, und das Netz, das die NICs während der Zurückschreibungsoperation verwenden sollen, an.

```
dsmc restore vm "VM8:-vmdk:Hard Disk 1" -vmname="*" -restore"  
-vmdefaultdvportgroup=portgroup1 -vmdefaultdvswitch=switch1  
-vmdefaultnetwork=network1 -host=esx03.example.com -preview
```

Befehlsausgabe:

Zurückschreibungsfunktion aufgerufen.

Befehl 'Restore VM' gestartet. Gesamtzahl zu verarbeitender VMs: 1

```
1.      VM-Name: 'VM8'  
        Modus: 'Immer inkrementell - Vollständig'  
        Sicherungszeit: IFFULL 05/22/2017 11:08:33  
  
        Platte 1 Kennsatz:      'Hard Disk 1'  
        Platte 1 Name:         '[TSMV5K2:DS1_VMDData (26TB)] VM8/TestVM8.vmdk'  
        Platte 1 Status:       Von Benutzer ausgeschlossen  
        Platte 1 Kapazität:     42,949,672,960  
        Platte 1 Daten zu senden: 42,878,369,792  
  
        Platte 2 Kennsatz:     'Hard Disk 2'  
        Platte 2 Name:         '[TSMV5K2:DS1_VMDData (26TB)] VM8/TestVM8_1.vmdk'  
        Platte 2 Status:       Ausgewählt  
        Platte 2 Kapazität:     10,737,418,240  
        Platte 2 Daten zu senden: 10,737,418,240  
  
        Zielname:              'VM8 -restore'  
        Zielhost:              'esx03.example.com'  
        Virtuelle Zielportgruppe: 'portgroup1'  
        Virtueller Zielswitch:  'switch1'  
        Zielnetz:              'network1'  
        Ziel-CTL-Ordner:       'C:\mnt\tsmvmbackup'
```

Task Die Sofortzurückschreibungsoperation (Instant Restore) der virtuellen Maschine VM8 voranzeigen, bei der auch die Platte Hard Disk 1 ausgeschlossen wird. Die virtuelle Maschine wird mit einem neuen VM-Namen, der mit -restore endet, auf den ESXi-Host-Server esx03 zurückgeschrieben.

Der Befehl zeigt außerdem die zu verwendende Portgruppe für die NICs, den verteilten virtuellen Switch (dvSwitch), der die Portgruppe enthält, und das Netz, das die NICs während der Zurückschreibungsoperation verwenden sollen, an. Die neue virtuelle Maschine wird als virtuelle Platte mit Thick Provisioning bereitgestellt und sie wird nach der Zurückschreibungsoperation automatisch erneut gestartet.

```
restore vm "VM8:-vmdk:Hard Disk 1" -vmname="*" -restore"  
-vmdefaultdvportgroup=portgroup1 -vmdefaultdvswitch=switch1  
-vmdefaultnetwork=network1 -host=esx03.storage.example.com  
-vmrestoretype=instantrestore -vmdiskprovision=thick  
-vmautostartvm=yes -preview
```

Befehlsausgabe:


```

1.  VM-Name: 'VM8'
    Modus: 'Immer inkrementell - Vollständig'
    Sicherungszeit: IFFULL 05/22/2017 11:08:33

    Platte 1 Kennsatz:      'Hard Disk 1'
    Platte 1 Name:         '[TSMV5K2:DS1_VMDa (26TB)] VM8/TestVM8.vmdk'
    Platte 1 Status:       Von Benutzer ausgeschlossen
    Platte 1 Kapazität:    42,949,672,960
    Platte 1 Daten zu senden: 42,878,369,792

    Platte 2 Kennsatz:      'Hard Disk 2'
    Platte 2 Name:         '[TSMV5K2:DS1_VMDa (26TB)] VM8/TestVM8_1.vmdk'
    Platte 2 Status:       Ausgewählt
    Platte 2 Kapazität:    10,737,418,240
    Platte 2 Daten zu senden: 10,737,418,240

    Zielname:              'VM8 -restore'
    Zielhost:              'esx03.example.com'
    Virtuelle Zielportgruppe: 'portgroup1'
    Virtueller Zielswitch:  'switch1'
    Zielnetz:              'network1'
    Zielbereitstellung:     'THICK'
    Automatisches Starten des Ziels: Ja

```

Zugehörige Verweise:

„Restore VM“ auf Seite 791

Retrieve

Mit dem Befehl **retrieve** können Kopien archivierter Dateien vom IBM Spectrum Protect-Server abgerufen werden. Es können bestimmte Dateien oder vollständige Verzeichnisse abgerufen werden.

Mit der Option **description** können die Beschreibungen angegeben werden, die den abzurufenden Dateien zugeordnet sind.

Verwenden Sie die Option **pick**, um eine Liste Ihrer Archivierungen anzuzeigen, aus der Sie eine Archivierung zum Abrufen auswählen können.

Rufen Sie die Dateien in dasselbe Verzeichnis ab, in dem sie archiviert wurden, oder in ein anderes Verzeichnis. Der Client für Sichern/Archivieren verwendet die Option **preservepath** mit dem Wert **subtree** als Standardwert für das Zurückschreiben von Dateien.

Anmerkung: Wird ein Verzeichnis abgerufen, werden das Datum und die Uhrzeit des Abrufs als Änderungsdatum und Änderungszeit festgelegt und nicht das Datum und die Uhrzeit des Verzeichnisses bei seiner Archivierung. Die Ursache dafür ist, dass der Client für Sichern/Archivieren zuerst die Verzeichnisse abruft und anschließend die Dateien zu den Verzeichnissen hinzufügt.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```

>> RETrieve [—Optionen] [—Quellendateispezifikation]

```

Parameter

Quellendateispezifikation

Gibt den Pfad und den Namen der Datei an, die abgerufen werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis anzugeben.

Zieldateispezifikation

Gibt den Pfad und Dateinamen an, in dem die Dateien gespeichert werden sollen. Wenn Sie kein Ziel angeben, schreibt der Client die Dateien in den ursprünglichen Quellenpfad zurück.

Anmerkung: Wenn Sie kein Ziel angeben, stellt der Client für Sichern/Archivieren fest, ob das ursprüngliche Dateisystem erreicht werden kann. Kann das ursprüngliche Dateisystem nicht erreicht werden, schreibt der Client die Datei nicht zurück.

Dieser Fehler kann auch auftreten, wenn Sie die Option **virtualmountpoint** aus der Datei dsm.sys entfernen. In diesem Fall können Sie einen anderen Zielort angeben oder die ursprüngliche Option **virtualmountpoint** in die Datei dsm.sys zurückschreiben, den Client erneut starten und den Befehl wiederholen.

Tabelle 112. Befehl Retrieve: Zugehörige Optionen

Option	Verwendung
dateformat „Dateformat“ auf Seite 389	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
description „Description“ auf Seite 397	Nur in der Befehlszeile.
dironly „Dironly“ auf Seite 403	Nur in der Befehlszeile.
filelist „Filelist“ auf Seite 453	Nur in der Befehlszeile.
filesonly „Filesonly“ auf Seite 457	Nur in der Befehlszeile.
followsymbolic „Followsymbolic“ auf Seite 458	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
fromdate „Fromdate“ auf Seite 461	Nur in der Befehlszeile.
fromnode „Fromnode“ auf Seite 461	Nur in der Befehlszeile.
fromowner „Fromowner“ auf Seite 462	Nur in der Befehlszeile.
fromtime „Fromtime“ auf Seite 463	Nur in der Befehlszeile.
ifnewer „Ifnewer“ auf Seite 468	Nur in der Befehlszeile.
pick „Pick“ auf Seite 528	Nur in der Befehlszeile.

Tabelle 112. Befehl *Retrieve*: Zugehörige Optionen (Forts.)

Option	Verwendung
preservepath „Preservepath“ auf Seite 537	Nur in der Befehlszeile.
replace „Replace“ auf Seite 547	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
subdir „Subdir“ auf Seite 605	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
tapeprompt „Tapeprompt“ auf Seite 607	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
timeformat „Timeformat“ auf Seite 616	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
todate „Todate“ auf Seite 621	Nur in der Befehlszeile.
totime „Totime“ auf Seite 622	Nur in der Befehlszeile.

Beispiele

Task Eine einzelne Datei mit dem Namen *budget* abrufen.

```
retrieve /home/devel/projecta/budget
```

Task Alle Dateien mit der Erweiterung *.c* aus dem Verzeichnis */home/devel/projecta* abrufen.

```
retrieve "/home/devel/projecta/*.c"
```

Task Alle Dateien im Verzeichnis */home* abrufen.

```
retrieve /home/
```

Task Alle Dateien mit der Dateierweiterung *.c* aus dem Verzeichnis */home/devel/projecta* in das Verzeichnis */home/newdevel/projectn/projecta* abrufen. Ist das Verzeichnis */projectn* oder */projectn/projecta* nicht vorhanden, wird es erstellt.

```
retrieve "/home/devel/projecta/*.c" /home/newdevel/projectn/
```

Task Dateien im Verzeichnis */user/project* abrufen. Die Option **pick** verwenden.

```
ret "/user/project/*" -pick
```

Task Alle Dateien abrufen, die aus dem Verzeichnis */proj* mit der Beschreibung „2012 survey results“ archiviert wurden.

```
retrieve "/proj/*" -desc="2012 survey results"
```

Task Die archivierte Datei */home/devel/budget* mit der Beschreibung "my budget" auf das Bandlaufwerk */dev/rmt1* abrufen.

```
mkfifo fifo
dd if=fifo of=/dev/rmt1&
dsmc retrieve -replace=yes -description="mybudget"
/home/devel/budget fifo
```

Task Eine Datei aus dem umbenannten Dateibereich *Jaguar_OLD* an ihren ursprünglichen Standort abrufen. Geben Sie sowohl die Quelle als auch das Ziel wie folgt ein:

```
ret Jaguar_OLD/user5/Documents/myresume.doc /Users/user5/Documents/
```

Zugehörige Informationen

„Clientoptionsreferenz“ auf Seite 355

Archivierungen aus nicht Unicode-fähigen Dateibereichen abrufen

Wenn Sie Archivierungen aus Dateibereichen abrufen wollen, die vom Unicode-fähigen Client umbenannt wurden, müssen Sie die Quelle auf dem Server und ein Ziel auf dem Client angeben.

Dieser Abschnitt gilt nur für Mac OS X. Beispiel: Angenommen, Jaguar ist der Name Ihrer Startplatte und Sie archivieren alle .log-Dateien im Verzeichnis /Users/user5/Documents. Bevor die Archivierung stattfindet, benennt der Server den Dateibereich in Jaguar_OLD um. Bei der Archivierung werden die in der aktuellen Operation angegebenen Daten in den Unicode-fähigen Dateibereich mit dem Namen / gestellt. Der neue Unicode-fähige Dateibereich enthält jetzt nur das Verzeichnis Users/user5/Documents und die Dateien *.log, die in der Operation angegeben wurden.

Wenn Sie eine Datei aus dem *umbenannten* (alten) Dateibereich an den ursprünglichen Standort abrufen wollen, müssen Sie sowohl die Quelle als auch das Ziel wie folgt eingeben:

```
retrieve Jaguar_OLD/Users/user5/Documents/mylog.log /Users/user5/Documents/
```

Schedule

Mit dem Befehl **schedule** kann der Client-Scheduler auf Ihrer Workstation gestartet werden. Der Client-Scheduler muss aktiv sein, damit geplante Arbeit gestartet werden kann.

Berechtigter Benutzer: Der Befehl **schedule** startet den Client-Scheduler auf Ihrer Workstation. Der Client-Scheduler muss aktiv sein, damit geplante Arbeit gestartet werden kann.

Anmerkung:

1. Der Befehl **schedule** kann nicht verwendet werden, wenn die Option `managedservices` auf `schedule` gesetzt ist. .
2. Nur für Mac OS X: Geben Sie zur Verwendung des Befehls **schedule** die Option `managedservices none` in der Datei `dsm.sys` an.
3. Dieser Befehl ist nur in der Anfangsbefehlszeile gültig. Im interaktive Modus oder in einer Makrodatei ist er nicht gültig.

Ist die Option `schedmode` auf "polling" (Sendeaufruf) gesetzt, fragt der Client-Scheduler den Server nach der Anzahl Stunden, die Sie mit der Option `querschedperiod` in Ihrer Clientbenutzeroptionsdatei (`dsm.opt`) angegeben haben, nach geplanten Ereignissen ab. Wird die Option `querschedperiod` vom Administrator für alle Knoten definiert, überschreibt diese Einstellung die Einstellung des Clients.

Wird TCP/IP-Übertragung verwendet, kann der Server der Workstation auch mitteilen, wann ein geplantes Ereignis ausgeführt werden muss. In diesem Fall müssen Sie die Option `schedmode` in der Clientbenutzeroptionsdatei (`dsm.opt`) oder im Befehl **schedule** auf *prompted* setzen.

Sie können die Option `sessioninitiation` im Befehl **schedule** verwenden, um zu steuern, ob der Server oder der Client Sitzungen durch eine Firewall einleiten soll.

Nach dem Starten des Client-Schedulers bleibt dieser so lange aktiv und startet geplante Ereignisse, bis Sie die Tastenkombination **Strg+C** drücken, den Schedulerprozess mit dem UNIX-Befehl **kill** stoppen oder die Workstation erneut starten bzw. ausschalten, um ihn zu beenden.

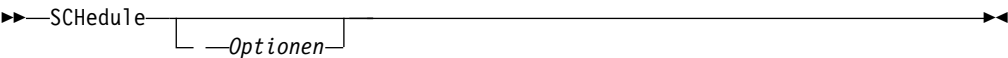
Nach dem Starten des Client-Schedulers bleibt dieser so lange aktiv und startet geplante Ereignisse, bis die Sie die Tastenkombination **Strg+C** drücken, die Taste **Q** zweimal drücken oder die Workstation erneut starten bzw. ausschalten, um ihn zu beenden.

Anmerkung: Dieser Befehl kann *nicht* im interaktiven Modus eingegeben werden.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax



Parameter

Tabelle 113. Befehl Schedule: Zugehörige Optionen

Option	Verwendung
maxcmdretries „Maxcmdretries“ auf Seite 504	Clientsystemoptionsdatei (<code>dsm.sys</code>) oder Befehlszeile.
password „Password“ auf Seite 524	Clientbenutzeroptionsdatei (<code>dsm.opt</code>)
querschedperiod „Querschedperiod“ auf Seite 541	Clientsystemoptionsdatei (<code>dsm.sys</code>) oder Befehlszeile.
retryperiod „Retryperiod“ auf Seite 560	Clientsystemoptionsdatei (<code>dsm.sys</code>) oder Befehlszeile.
schedlogname „Schedlogname“ auf Seite 567	Clientsystemoptionsdatei (<code>dsm.sys</code>) oder Befehlszeile.
schedmode „Schedmode“ auf Seite 570	Clientsystemoptionsdatei (<code>dsm.sys</code>) oder Befehlszeile.
sessioninitiation „Sessioninitiation“ auf Seite 576	Clientsystemoptionsdatei (<code>dsm.sys</code>) oder Befehlszeile.

Tabelle 113. Befehl *Schedule*: Zugehörige Optionen (Forts.)

Option	Verwendung
tcpclientport „Tcpclientport“ auf Seite 612	Clientsystemoptionsdatei (dsm.sys) oder Befehlszeile.

Beispiele

Task Den Client-Scheduler starten.

Befehl: `dsmc sch -password=notell`

Task Für AIX: Den Scheduler beim Systemstart starten, indem Sie den folgenden Befehl in die Datei `/etc/inittab` eingeben. Stellen Sie sicher, dass die Option *passwordaccess* auf *generate* gesetzt ist.

Befehl: `tsm::once:/usr/bin/dsmc sched > /dev/null 2>&1 #TSM`

Task Den Scheduler interaktiv starten und im Hintergrund ausführen.

Befehl: `nohup dsmc sched 2> /dev/null &`

Wenn Sie den Befehl **schedule** ausführen, werden alle Nachrichten zu geplanter Arbeit an die Datei `dsmsched.log` gesendet oder an die Datei, die Sie mit der Option `schedlogname` in Ihrer Clientsystemoptionsdatei (`dsm.sys`) angeben. Wenn Sie für den Dateinamen in der Option `schedlogname` keinen Verzeichnispfad angeben, wird die Datei `dsmsched.log` im aktuellen Arbeitsverzeichnis gespeichert. Dies gilt jedoch nicht für Mac OS X. Bei Mac OS X befindet sich die Datei `dsmsched.log` im Verzeichnis `/Library/Logs/tivoli/tsm/`.

Wichtig: Geben Sie in der Umgebungsvariablen `DSM_LOG` den Namen eines Verzeichnisses an, in dem die Standardberechtigungen den erforderlichen Zugriff gestatten, um Fehler bei Protokollschreiboperationen und den Verarbeitungsabbruch in bestimmten Fällen zu vermeiden.

Zugehörige Informationen

„Sessioninitiation“ auf Seite 576

Selective

Der Befehl **selective** sichert vom Benutzer angegebene Dateien. Werden diese Dateien beschädigt oder gehen sie verloren, können sie durch Sicherungsversionen vom Server ersetzt werden.

Wenn Sie eine selektive Sicherung ausführen, sind alle Dateien Sicherungskandidaten, sofern Sie sie nicht von der Sicherung ausschließen oder sie nicht den Anforderungen der Verwaltungsklasse in Bezug auf die Durchnummerierung entsprechen.

Während einer selektiven Sicherung werden Kopien der Dateien an den Server gesendet, auch wenn sie sich seit der letzten Sicherung nicht geändert haben. Aus diesem Grund können mehrere Kopien derselben Datei auf dem Server vorhanden sein. In diesem Fall sind möglicherweise nicht so viele verschiedene Versionen der Datei auf dem Server vorhanden, wie beabsichtigt war. Das Versionslimit könnte

durch identische Dateien erreicht worden sein. Um dieses Problem zu vermeiden, können Sie mit Hilfe des Befehls **incremental** ausschließlich neue und geänderte Dateien sichern.

Sie können einzelne Dateien oder Verzeichnisse selektiv sichern. Zum Sichern von Gruppen zusammengehöriger Dateien können außerdem Platzhalterzeichen verwendet werden.

Wenn Sie beim Sichern eines bestimmten Pfads und einer bestimmten Datei die Option `subdir` auf `yes` setzen, sichert der Client rekursiv alle Unterverzeichnisse unter diesem Pfad und alle Instanzen der angegebenen Datei, die sich unter allen diesen Unterverzeichnissen befinden.

Während einer selektiven Sicherung kann ein Verzeichnispfad gesichert werden, auch wenn die spezifische Datei für die Sicherung nicht gefunden wird. Beispielsweise sichert der folgende Befehl `dir1` und `dir2`, auch wenn die Datei `bogus.txt` nicht vorhanden ist.

```
selective /Users/user1/Documents/dir1/bogus.txt  
selective "/dir1/dir2/bogus.txt"
```

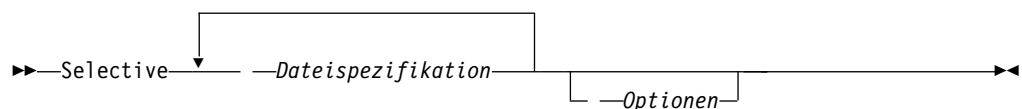
Wenn der Befehl **selective** wegen eines Übertragungs- oder Sitzungsfehlers wiederholt wird, zeigen die Übertragungsstatistiken die Anzahl Byte an, die der Client während *aller* Befehlswiederholungen zu übertragen versucht. Daher entsprechen die Statistiken für die übertragenen Byte möglicherweise nicht den Dateistatistiken, z. B. für die Dateigröße.

Sie können mit der Option `removeoperandlimit` angeben, dass die Beschränkung auf 20 Operanden entfernt wird. Geben Sie die Option `removeoperandlimit` mit dem Befehl **selective** an, wird die Beschränkung auf 20 Operanden nicht umgesetzt und nur durch die verfügbaren Ressourcen oder andere Begrenzungen des Betriebssystems eingeschränkt.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax



Parameter

Dateispezifikation

Gibt den Pfad und den Namen der Datei an, die gesichert werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis anzugeben.

Sollen mehrere Dateispezifikationen angegeben werden, trennen Sie die einzelnen Spezifikationen durch ein Leerzeichen voneinander. Werden mehrere Dateispezifikationen angegeben und haben mindestens zwei der Spezifikationen gemeinsame übergeordnete Verzeichnisse, kann es vorkommen, dass die gemeinsamen Verzeichnisobjekte mehrmals gesichert werden. Die Bedingungen, unter denen dieses Verhalten auftritt, sind laufzeitabhängig; das Verhalten

selbst hat jedoch keine nachteiligen Auswirkungen.

Lautet die Dateispezifikation beispielsweise `/home/amr/ice.doc /home/amr/fire.doc`, könnten `/home` und `/home/amr` zweimal gesichert werden. Die Dateiobjekte, `ice.doc` und `fire.doc`, werden nur einmal gesichert.

Wenn Sie verhindern wollen, dass das gemeinsame übergeordnete Verzeichnis mehrmals angegeben wird, verwenden Sie separate, nicht überlappende **selective**-Befehle, um jede Dateispezifikation zu sichern.

Wenn Sie ein Dateisystem sichern, geben Sie einen abschließenden Schrägstrich an (`/home/`).

Es gilt eine Begrenzung auf 20 Operanden. Diese Begrenzung verhindert, dass sehr viele Sitzungen geöffnet werden, wenn die Platzhalterzeichen vom Befehlsprozessor der UNIX-Shell erweitert werden. Sie können verhindern, dass aufgrund der Shellerweiterung der Grenzwert von 20 Operanden überschritten wird, indem Sie am Anfang und am Ende der Dateispezifikationen, die Platzhalterzeichen enthalten ("`home/docs/*`"), Anführungszeichen eingeben.

Sie können mit der Option **removeoperandlimit** angeben, dass die Beschränkung auf 20 Operanden entfernt wird. Wenn Sie die Option **removeoperandlimit** angeben, wird die Beschränkung auf 20 Operanden nicht umgesetzt und nur durch die verfügbaren Ressourcen oder andere Begrenzungen des Betriebssystems eingeschränkt. Entfernen Sie beispielsweise die Begrenzung auf 20 Operanden, um 21 Dateispezifikationen zu sichern:

```
selective -removeoperandlimit filespec1 filespec2 ... filespec21
```

Sie können die Option **filelist** anstelle von Dateispezifikationen verwenden, um anzugeben, welche Dateien bei dieser Operation berücksichtigt werden sollen. Diese beiden Methoden schließen sich jedoch gegenseitig aus. Sie können nicht sowohl Dateispezifikationsparameter angeben als auch die Option **filelist** verwenden. Wenn die Option **filelist** angegeben wird, werden alle angegebenen Dateispezifikationen ignoriert.

Tabelle 114. Befehl Selective: Zugehörige Optionen

Option	Verwendung
changingretries „Changingretries“ auf Seite 373	Clientsystemoptionsdatei (dsm.sys) oder Befehlszeile.
compressalways „Compressalways“ auf Seite 379	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
compression „Compression“ auf Seite 380	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
dironly „Dironly“ auf Seite 403	Nur in der Befehlszeile.
filelist „Filelist“ auf Seite 453	Nur in der Befehlszeile.
filesonly „Filesonly“ auf Seite 457	Nur in der Befehlszeile.
presavelastaccessdate „Presavelastaccessdate“ auf Seite 536	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.

Tabelle 114. Befehl *Selective*: Zugehörige Optionen (Forts.)

Option	Verwendung
removeoperandlimit „Removeoperandlimit“ auf Seite 546	Nur in der Befehlszeile.
snapshotcachesize „Snapshotcachesize“ auf Seite 590	Clientoptionsdatei (dsm.opt) oder mit der Option include.fs.
snapshotproviderfs „Snapshotproviderfs“ auf Seite 591	Systemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe oder mit der Option include.fs.
snapshotroot „Snapshotroot“ auf Seite 593	Nur in der Befehlszeile.
subdir „Subdir“ auf Seite 605	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
tapeprompt „Tapeprompt“ auf Seite 607	Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.

Beispiele

Task Die Datei proja im Verzeichnis /home/devel sichern.

Befehl: selective /home/devel/proja

Task Alle Dateien im Verzeichnis /home/devel sichern, deren Dateiname mit proj beginnt.

Befehl: selective "/home/devel/proj*"

Task Alle Dateien im Verzeichnis /home/devel sichern, deren Dateiname mit proj beginnt. Die einzelne Datei mit dem Namen budget im Verzeichnis /user/home sichern.

Befehl: selective "/home/devel/proj*" /user/home/budget

Task Das Dateisystem /home sichern.

Befehl: selective /home/ -subdir=yes

Task Angenommen, Sie haben eine Momentaufnahme des Dateisystems /usr gestartet und die Momentaufnahme als /snapshot/day1 angehängt. Führen Sie eine selektive Sicherung der Verzeichnisbaumstruktur /usr/dir1/sub1 aus der lokalen Momentaufnahme durch und verwalten Sie sie auf dem IBM Spectrum Protect-Server unter dem Dateibereichsnamen /usr.

Befehl: dsmc sel "/usr/dir1/sub1/*" -subdir=yes -snapshotroot=/snapshot/day1

Lokale Momentaufnahme einem Serverdateibereich zuordnen

Wenn Sie eine Anwendung eines unabhängigen Softwareanbieters zur Erstellung einer Momentaufnahme eines logischen Datenträgers benutzen, verwenden Sie die Option snapshotroot im Befehl **selective**, um die Daten der lokalen Momentaufnahme den originalen Dateibereichsdaten zuzuordnen, die auf dem IBM Spectrum Protect-Server gespeichert sind. Die Option snapshotroot bietet keine Funktionen zur Erstellung einer Datenträgermomentaufnahme, sondern ausschließlich Funktionen zur Verwaltung von Daten, die durch Erstellen einer Datenträgermomentaufnahme generiert werden.

Nur für AIX: Sie können eine selektive Sicherung auf Momentaufnahmebasis ausführen, indem Sie die Option `snapshotproviderfs=JFS2` angeben.

Set Access

Der Befehl **set access** erteilt Benutzern an anderen Knoten Zugriff auf Ihre Sicherungsversionen und Archivierungskopien.

Sie können den Befehl **set access** auch verwenden, um Benutzern an anderen Knoten Zugriff auf Ihre Sicherungsbilder zu erteilen.

Sie können einem anderen Benutzer Zugriff auf eine bestimmte Datei oder ein bestimmtes Image, auf mehrere Dateien oder Images oder auf alle Dateien in einem Verzeichnis erteilen. Erteilen Sie einem anderen Benutzer die Zugriffsberechtigung, kann dieser Benutzer Ihre Objekte zurückschreiben oder abrufen. In dem Befehl muss angegeben werden, ob der Zugriff auf Archivierungskopien oder auf Sicherungsversionen erteilt wird.

Bei virtuellen VMware-Maschinen können Sie einem Benutzer auf einem anderen Knoten Zugriff auf die Sicherungen einer bestimmten virtuellen Maschine erteilen.

Wenn ein Knoten auf einen anderen IBM Spectrum Protect-Server exportiert wird, können sich die Zugriffsregeln auf dem importierenden Server ändern. Wird eine Zugriffsregel auf alle Dateibereiche auf dem exportierenden Server angewendet, wird die Zugriffsregel auf dem importierenden Server auf die importierten Dateibereiche beschränkt. Die Dateibereiche in der Zugriffsregel auf dem importierenden Server werden aus Sicherheitsgründen beschränkt. Darüber hinaus erkennen die Zugriffsregeln das erste Auftreten eines Platzhalterzeichens in der Dateispezifikation beim Zurückschreiben oder beim Abruf nicht. Dies bedeutet, dass Unterverzeichnisse ignoriert werden, wenn Sie in der Dateispezifikation für eine Zurückschreibung oder einen Abruf ein Platzhalterzeichen verwenden.

Tipp: Wenn Sie einen Knoten auf einen anderen IBM Spectrum Protect-Server exportieren, dürfen Sie kein einzelnes Platzhalterzeichen als Dateispezifikation in der Zugriffsregel verwenden. Erstellen Sie stattdessen eine Zugriffsregel für jeden Dateibereich.

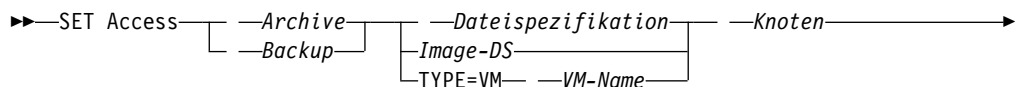
Anmerkung: Es ist nicht möglich, mit einem einzigen Befehl die Zugriffsberechtigung für Sicherungen und Archivierungen zu erteilen.

Wenn ein vorhandener Dateibereich während der Unicode-Konvertierung umbenannt wird, gelten die für den Dateibereich definierten Zugriffsregeln weiterhin für den ursprünglichen Dateibereich. Für den neuen Unicode-Dateibereich müssen jedoch neue Zugriffsregeln definiert werden.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax





Parameter

Archive

Erteilt Zugriff auf archivierte Dateien oder Images.

Backup

Erteilt Zugriff auf Sicherungsversionen von Dateien oder Images.

Dateispezifikation

Gibt den Pfad, die Datei, das Image oder das Verzeichnis an, für den/die/das Sie dem anderen Knoten oder Benutzer Zugriff erteilen. Verwenden Sie Platzhalterzeichen, um Gruppen von Dateien oder Images oder alle Dateien in einem Verzeichnis, alle Objekte in einer Verzeichnisverzweigung oder alle Objekte in einem Dateisystem anzugeben. Mit einem einzelnen Stern "*" als Dateispezifikation können Sie die Zugriffsberechtigung für alle Dateien oder Images erteilen, deren Eigner Sie sind und die auf dem Server gesichert wurden. Wenn der Befehl `set access backup "*" Knoten` eingegeben wird, erfolgt keine Überprüfung auf dem Server; es wird davon ausgegangen, dass mindestens ein Objekt gesichert wurde.

Wird die Zugriffsberechtigung für eine Ebene des aktuellen Arbeitsverzeichnisses erteilt, muss nur die Ebene angegeben werden. Wird die Zugriffsberechtigung für Objekte erteilt, die sich nicht in einer Verzeichnisebene des aktuellen Arbeitsverzeichnisses befinden, müssen Sie den vollständigen Pfad angeben. Für die Dateispezifikation, für die eine Zugriffsberechtigung erteilt wurde, muss mindestens eine Sicherungsversion oder eine Archivierungskopie (Datei oder Verzeichnis) auf dem Server vorhanden sein.

Sollen alle Dateien in einem bestimmten Verzeichnis angegeben werden, geben Sie `/home/mine/proj1/*` in die Befehlszeile ein.

Um die Zugriffsberechtigung für alle Objekte unter einer bestimmten Ebene zu erteilen, geben Sie einen Stern, ein Verzeichnisbegrenzungszeichen und einen Stern am Ende der Dateispezifikation an. Soll beispielsweise Zugriff auf alle Objekte unter `home/test` erteilt werden, verwenden Sie die Dateispezifikation `home/test/*/*`.

Wichtig: Durch die Verwendung des Formats `/*/*` alleine erteilen Sie keinen Zugriff auf Objekte in dem angegebenen Verzeichnis, sondern nur auf Objekte in den Verzeichnissen unter dem angegebenen Verzeichnis.

Für das Stammverzeichnis sind die Regeln im Wesentlichen identisch. Geben Sie `/*` in einem Befehl `set access` und `/*/*` in einem weiteren Befehl `set access` an, wenn ein anderer Benutzer Zugriff auf alle Dateien und Verzeichnisse in und unter dem Stammverzeichnis haben soll. Die erste Angabe `/*` erteilt Zugriff auf alle Verzeichnisse und alle Dateien im Stammverzeichnis. Die zweite Angabe `/*` erteilt Zugriff auf alle Verzeichnisse und Dateien unter dem Stammverzeichnis.

Beispiel:

- Ihre Verzeichnisstruktur besteht aus mehreren Ebenen: `/home/sub1/subsub1`.
- Das Verzeichnis `/home` enthält die Dateien `h1.txt` und `h2.txt`.
- Das Verzeichnis `/home/sub1` enthält die Datei `s1.htm`.
- Das Verzeichnis `/home/sub1/sub2` enthält die Datei `ss1.cpp`.

Soll Zugriff auf alle Dateien im Verzeichnis /home/sub1/sub2 erteilt werden, geben Sie Folgendes ein:

```
set access backup /home/sub1/sub2/* * *
```

Soll Zugriff nur auf die Dateien im Verzeichnis /home erteilt werden, geben Sie Folgendes ein:

```
set access backup /home/* * *
```

Soll Zugriff auf alle Dateien in allen Verzeichnissen in und unter dem Verzeichnis /home erteilt werden, geben Sie Folgendes ein:

```
set access backup /home/* * *  
set access backup /home/*/* * *
```

Image-DS

Der Name des Imagedateisystems, das gemeinsam benutzt werden soll. Durch die Angabe eines Sterns (*) wird der Zugriff auf alle Images des Eigners ermöglicht, der die Zugriffsberechtigung erteilt.

-TYPE=VM VM-Name

Dieser Parameter ist erforderlich, wenn Sie diesen Befehl verwenden, um einem anderen Benutzer Zugriff auf Sicherungen der virtuellen VMware-Maschine zu erteilen. Die Option *VM-Name* kann nur verwendet werden, wenn -TYPE=VM angegeben wird; *VM-Name* ist der Name der virtuellen VMware-Maschine, der Sie Zugriff erteilen.

Knoten

Gibt den Clientknoten des Benutzers an, dem der Zugriff erteilt werden soll. Es können Platzhalterzeichen verwendet werden, wenn der Zugriff für mehrere Knoten mit ähnlichen Knotennamen erteilt werden soll. Mit einem Stern (*) wird allen Knoten der Zugriff erteilt.

Benutzer

Dieser optionale Parameter schränkt den Zugriff auf den benannten Benutzer auf dem angegebenen Knoten ein. Soll jeder berechtigte Benutzer Zugriff auf Ihre gesicherten oder archivierten Daten erhalten, geben Sie **root** als Benutzer an.

Beispiele

Task Dem Benutzer an node_2 die Berechtigung zum Zurückschreiben der Datei budget aus dem Verzeichnis /home/user erteilen.

```
set access backup /home/user/budget node_2
```

Task Dem Knoten node_3 die Berechtigung zum Abrufen aller Dateien im Verzeichnis /home/devel/proja erteilen.

```
set ac archive /home/devel/proja/ node_3
```

Task Allen Knoten, deren Name mit bldgb endet, die Berechtigung zum Zurückschreiben aller Sicherungsversionen aus Verzeichnissen mit dem Dateibereichsnamen project erteilen.

```
set ac b "{project}/*" "*bldgb"
```

Task Jedem berechtigten Benutzer auf node1 die Berechtigung zum Abrufen aller Dateien im Verzeichnis /home/devel/projb erteilen.

```
set access archive /home/devel/projb/ node1 root
```

Task Benutzer serena auf node_5 die Berechtigung zum Zurückschreiben aller Images des im Verzeichnis /home/devel/proja angehängten Dateibereichs erteilen.

```
set acc backup "home/devel/proja/*/*" node_5 serena
```

Task Dem Knoten **myOtherNode** die Berechtigung zum Zurückschreiben von Dateien erteilen, die von der virtuellen VMware-Maschine **myTestVM** gesichert wurden.

```
set access backup -TYPE=VM myTestVM myOtherNode
```

Set Event

Mit dem Befehl **set event** können Sie die Umstände für das Löschen archivierter Daten angeben.

Den Befehl **set event** können Sie für folgende Aktionen verwenden:

- Die Löschung von Daten am Ende ihrer zugeordneten Aufbewahrungsdauer verhindern (Löschen unzulässig)
- Den Verfall wie von der Archivierungskopiengruppe definiert zulassen (eine Löschsperre freigeben)
- Die Uhr für den Verfall starten, wenn ein bestimmtes Ereignis eintritt (den Server benachrichtigen, dass ein Ereignis eingetreten ist)

Betroffene Objekte können wie folgt angegeben werden: über eine Standarddateispezifikation (einschließlich Platzhalterzeichen), über eine Liste von Dateien, deren Namen in der mit der Option `filelist` angegebenen Datei stehen, oder über eine Gruppe archivierter Dateien, deren Beschreibung mit der Option `description` angegeben ist.

Anmerkung: Wird nur eine <Dateispezifikation> verwendet, sind alle archivierten Kopien von Dateien oder Ordnern betroffen, die mit der Dateispezifikation übereinstimmen. Wenn Sie bestimmte Versionen einer Datei berücksichtigen wollen, verwenden Sie die Option `-pick` und wählen Sie aus der angezeigten Liste aus.

Interaktion mit Servern einer älteren Version

Wird der Befehl **set event** auf einem Client mit Verbindung zu einem Server ausgegeben, der keine ereignisgesteuerten Maßnahmen unterstützt (vor IBM Spectrum Protect 5.2.2), wird der Befehl mit einer Fehlermeldung zurückgewiesen, die besagt, dass der aktuelle Server keine ereignisgesteuerten Maßnahmen unterstützt.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
➤ SET Event -TYPE= Hold | Release | Activateretention -<Dateispezifikation> ➤
➤ -filelist=<Dateispezifikation> -description=-pick ➤
```

Parameter

`TYPE=`

Gibt die Einstellung des Ereignistyps an. Dieser Parameter muss angegeben werden.

hold

Verhindert, dass das Objekt gelöscht wird (unabhängig von der Verfallsmaßnahme).

release

Ermöglicht einen normalen ereignisgesteuerten Verfall.

activateretention

Sendet ein Signal an den Server, dass das steuernde Ereignis eingetreten ist, und startet die Uhr für den Verfall.

-pick

Stellt eine Liste von Objekten zur Verfügung, die der Benutzer auswählen kann, um das Ereignis auf sie anzuwenden.

Die folgenden Optionen können ebenfalls verwendet werden; sie dienen ihrem üblichen Zweck:

- Dateformat
- Numberformat
- Noprompt
- Subdir
- Timeformat

Beispiele

Task Das folgende Beispiel zeigt die ausführliche Ausgabe und Statistikausgabe des Befehls **set event** für **set event type=hold /home/accounting/ledgers/*05.books** bei erneut gebundenen Objekten an (im Gegensatz zu archivierten oder anderen Objekten).

```
Erneut binden--> 274 /home/accounting/ledgers/
                 jan05.books
Erneut binden--> 290 /home/accounting/ledgers/
                 feb05.books
```

```
Gesamtzahl archivierter Objekte:          0
Gesamtzahl fehlgeschlagener Objekte:      0
Gesamtzahl erneut gebundener Objekte:     2
Gesamtzahl übertragener Byte:            0 B
Datenübertragungszeit:                   0,00 Sek.
Datenübertragungsgeschwindigkeit im Netz: 0,00 KB/Sek.
Datenübertragungsgeschwindigkeit Gesamt: 0,00 KB/Sek.
Objekte komprimiert um:                  0%
Verarbeitungszeit:                       00:00:02
```

Task Die Option **-pick** in dem 'set event'-Befehl **set event type=activate /user/tsm521/common/unix** zeigt den Ereignistyp anstelle des Befehlsnamens:

Fenster PICK mit Blätterfunktion - Aufbewahrungsereignis: ACTIVATE

Nr.	Archiv.-Datum/-Zeit	Dateigröße	Datei
1.	05.08.2003 08:47:46	766 B	/user/tsm521 /common/unix
2.	01.08.2003 10:38:11	766 B	/user/tsm521 /common/unix
3.	05.08.2003 08:47:46	5,79 KB	/user/tsm521

4.	01.08.2003 10:38:11	5,79 KB	/common/unix /user/tsm521
5.	05.08.2003 08:47:46	10,18 KB	/common/unix /user/tsm521 /common/unix

Zugehörige Informationen

„Dateformat“ auf Seite 389

„Numberformat“ auf Seite 521

„Noprompt“ auf Seite 519

„Subdir“ auf Seite 605

„Timeformat“ auf Seite 616

Set Netappsvm

Der Befehl **set netappsvm** ordnet die Berechtigungsnachweise für Anmeldung eines Cluster-Management-Servers, die im Befehl **set password** angegeben werden, einer NetApp Storage Virtual Machine und dem Daten-SVM-Namen (Data Vserver) zu (SVM = Storage Virtual Machine). Sie müssen diesen Befehl eingeben, bevor Sie eine Momentaufnahmedifferenzteilsicherung eines NetApp-Clusterdatenträgers erstellen können.

Dieser Befehl wird normalerweise nur einmal eingegeben. Die Parameter werden gespeichert und bei der nächsten Sicherung eines Clusterdatenträgers, der von der Storage Virtual Machine verwaltet wird, wiederverwendet. Wenn Sie eine Storage Virtual Machine zu einem anderen Cluster-Management-Server verschieben, müssen Sie diesen Befehl erneut eingeben und den neuen Cluster-Management-Server angeben. Falls erforderlich, ändern Sie die Berechtigungsnachweise für Anmeldung mit dem Befehl **set password**.

Unterstützte Clients

Dieser Befehl ist für Linux-Clients für Sichern/Archivieren gültig, die Momentaufnahmedifferenzsicherungen von Clustered Data ONTAP-C-Mode-Dateiserverdatenträgern ausführen.

Syntax

```

>>—SET NETAPPSVM—SVM-Hostname—CMS-Hostname—SVM-Name—>>
                    |
                    |—-remove—SVM-Hostname—
  
```

Parameter

SVM-Hostname

Gibt für die Datenträger, die Sie schützen wollen, den Hostnamen oder die IP-Adresse der Storage Virtual Machine an, die die Datenträger und logischen Schnittstellen (LIFs) verwaltet.

CMS-Hostname

Gibt den Hostnamen oder die IP-Adresse des Cluster-Management-Servers an. Geben Sie denselben Hostnamen an, den Sie bei Verwendung des Befehls **set**

password für die Erstellung der Berechtigungsnachweise für Anmeldung für diesen Cluster-Management-Server angegeben haben.

SVM-Name

Gibt den Namen der Daten-SVM an, die den angehängten Datenträger verwaltet. Wenden Sie sich an den NetApp SVM-Administrator, um den Namen der Daten-SVM, die der virtuellen Maschinen zugeordnet ist, zu erhalten.

-remove SVM-Hostname

Hebt die Zuordnung zwischen der SVM und dem Cluster-Management-Server, dem sie zuvor zugeordnet war, auf. Geben Sie einen SVM-Hostnamen an.

Sie können diesen Parameter angeben, wenn Sie eine Storage Virtual Machine versehentlich einem 7-Mode-Dateiserver zugeordnet haben. Wenn Sie einen 7-Mode-Dateiserver entfernen und anschließend einen Cluster-Management-Server zuordnen, definieren Sie die Anmeldeberechtigungsnachweise für den Cluster-Management-Server mit dem Befehl **set password**.

Beispiele

Die Berechtigungsnachweise und den Zugriff auf eine Storage Virtual Machine konfigurieren:

```
set netappsvm svm_example.com cms_filer1.example.com svm_2
dsmc set password cms_filer1.example.com user_name password
```

Für die Storage Virtual Machine erstellte Zuordnungen entfernen:

```
set netappsvm -remove svm_example.com
```

Zugehörige Tasks:

„Clustered Data ONTAP NetApp-Dateiserverdatenträger schützen“ auf Seite 121

Set Password

Mit dem Befehl **set password** können Sie das IBM Spectrum Protect-Kennwort für Ihre Workstation ändern oder die Berechtigungsnachweise definieren, mit denen auf einen anderen Server zugegriffen wird.

Wenn Sie das alte und das neue Kennwort bei der Eingabe des Befehls **set password** weglassen, werden Sie einmal zur Eingabe des alten Kennworts und zweimal zur Eingabe des neuen Kennworts aufgefordert.

Die maximale Kennwortlänge beträgt 63 Zeichen. Kennwortbedingungen variieren, abhängig davon, wo die Kennwörter gespeichert und verwaltet werden, und abhängig von der Version des IBM Spectrum Protect-Servers, zu dem Ihr Client die Verbindung herstellt.

Wenn Ihr IBM Spectrum Protect-Server die Version 6.3.3 oder höher aufweist und Sie einen LDAP-Verzeichnisserver zum Authentifizieren von Kennwörtern verwenden

Verwenden Sie die folgenden Zeichen, um ein Kennwort zu erstellen:

```
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 . ! @ # $ % ^ & * _ - + = ` ( )
| { } [ ] : ; < > , ? / ~
```

Bei den Kennwörtern muss die Groß-/Kleinschreibung beachtet werden. Außerdem können die Kennwörter weiteren Einschränkungen aufgrund von LDAP-Richtlinien unterliegen.

Wenn Ihr IBM Spectrum Protect-Server die Version 6.3.3 oder höher aufweist und Sie keinen LDAP-Verzeichnisserver zum Authentifizieren von Kennwörtern verwenden

Verwenden Sie die folgenden Zeichen, um ein Kennwort zu erstellen:

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 werden in der IBM Spectrum Protect-Serverdatenbank gespeichert. Bei diesen Kennwörtern muss die Groß-/Kleinschreibung nicht beachtet werden.

Hinweis:

Schließen Sie in der Befehlszeile alle Parameter, die mindestens ein Sonderzeichen enthalten, in Anführungszeichen ein. Ohne Anführungszeichen können die Sonderzeichen als Shell-Escapezeichen, als Dateiumleitungszeichen oder als andere Zeichen, die eine Bedeutung für das Betriebssystem haben, interpretiert werden.

Auf AIX-, Linux- und Solaris-Systemen:

Schließen Sie die Befehlsparameter in Hochkommas (') ein.

Beispiel für die Befehlszeile:

```
dsmc set password -type=vmguest 'Win 2012 SQL'  
'tsml2dag\administrator' '7@#$$^&7'
```

Anführungszeichen sind nicht erforderlich, wenn Sie ein Kennwort mit Sonderzeichen in einer Optionsdatei eingeben.

Einschränkung: Der Befehl **set password** unterstützt nicht die für FIPS (Federal Information Processing Standard) aktivierte Betriebssystemumgebung für lokal gespeicherte Kennwörter.

Weitere Informationen zur FIPS-Unterstützung finden Sie in Technote 2007756.

Diese Einschränkung gilt für AIX-, Linux- und Solaris-Clients.

Unterstützte Clients

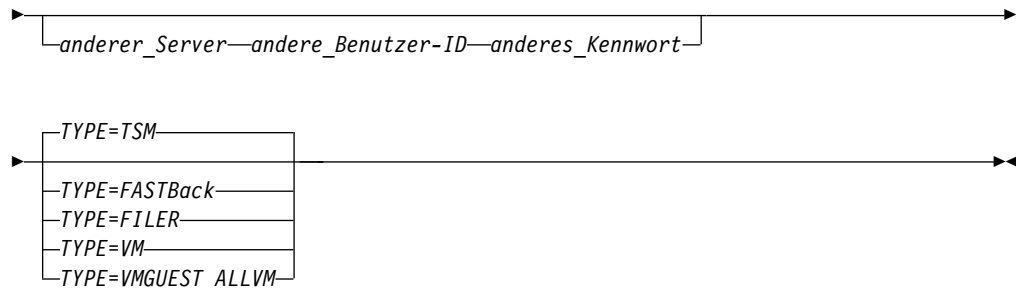
Dieser Befehl ist für alle Clients gültig.

Die folgenden Parameter gelten für VMware-Operationen, die nur verfügbar sind, wenn Sie den Client als eine Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware verwenden.

- TYPE=DOMAIN
- TYPE=VM
- TYPE=VMGUEST

Syntax

►►—SET Password—
└──altes_Kennwort—neues_Kennwort──┘



Parameter

altes_Kennwort

Gibt das aktuelle Kennwort für die Workstation an.

neues_Kennwort

Gibt das neue Kennwort für die Workstation an.

anderer_Server andere_Benutzer-ID anderes_Kennwort

Diese drei Parameter geben die Attribute an, mit denen der Client auf einen anderen Server, wie beispielsweise einen Dateiserver oder einen ESXi-Host, zugreift.

anderer_Server

Gibt den Hostnamen oder die IP-Adresse des Servers an, auf den der Client zum Schutz von Dateien zugreifen kann.

andere_Benutzer-ID

Die Benutzer-ID eines Kontos auf dem Server, mit der sich der Client bei dem anderen Server anmeldet. Das Konto muss über die erforderlichen Berechtigungen für die Operationen verfügen, die ausgeführt werden, sobald der Benutzer am anderen Server angemeldet ist.

anderes_Kennwort

Das Kennwort, das der Benutzer-ID auf dem anderen Server zugeordnet ist.

TYPE

Gibt an, ob dieses Kennwort für den Client für Sichern/Archivieren oder für einen anderen Servertyp gilt.

Verwenden Sie TYPE=TSM, um das Kennwort für Ihren Client für Sichern/Archivieren anzugeben. Der Standardtyp ist TYPE=TSM.

Verwenden Sie TYPE=FastBack auf Linux- und Windows-Clients, um die Tivoli Storage Manager FastBack-Berechtigungsnachweise zu speichern, die für das Bereitstellen und das Aufheben der Bereitstellung der FastBack-Datenträger auf dem Windows FastBack Disaster Recovery Hub-Server erforderlich sind.

Die Kennwortdatei auf dem vStorage-Sicherungsserver muss entweder über die Windows-Administrator-ID für das VMware Virtual Center-System oder über die UNIX-Benutzer-ID für einen bestimmten ESX-Server verfügen. Für eine Proxy-Sicherung für FastBack muss die Kennwortdatei die FastBack-Administrator-ID und das zugehörige Kennwort enthalten. Hier einige Beispiele:

```
dsmc set password 192.0.2.24 admin admin 123 -type=fastback
```

```
dsmc set password 192.0.2.24 WORKGROUP:admin admin 123 -type=fastback
```

```
dsmc set password windserv administrator windpass4 -type=fastback
```

Wichtig: Sie müssen die Benutzerberechtigungsnachweise, die für das Bereitstellen und das Aufheben der Bereitstellung von FastBack-Datenträgern in

einem Repository erforderlich sind, für den Client für Sichern/Archivieren definieren, bevor Sie den FastBack-Unterbefehl für die Sicherung/Archivierung eingeben. Verwenden Sie die Option fbserver zum Definieren der Berechtigungsnachweise.

Es folgt eine Kurzbeschreibung der verschiedenen Konfigurationen und der erforderlichen Berechtigungsnachweise:

- Der Client für Sichern/Archivieren ist auf einem dedizierten vStorage-Sicherungsserver installiert. Der Client auf dem vStorage-Sicherungsserver muss eine Verbindung zu mehreren gemeinsam genutzten Repositories im Netz herstellen.

Führen Sie die folgenden Schritte für jedes der gemeinsam genutzten Repositories im Netz aus, mit denen der Client verbunden ist:

1. Konfigurieren Sie das Repository mit FastBack Manager für den fernen Netzzugriff. Siehe die Tivoli Storage Manager FastBack-Produktdokumentation im IBM Knowledge Center unter <http://www.ibm.com/support/knowledgecenter/SS9NU9/welcome>.

Bei dieser Prozedur wird ein Domänenname und eine Benutzer-ID sowie ein Kennwort für die gemeinsame Nutzung im Netz erstellt, sodass eine ferne Verbindung zu dem Repository hergestellt werden kann.

2. Geben Sie auf der Workstation des Clients für Sichern/Archivieren manuell den folgenden Befehl ein:

```
dsmc set password type=fastback FBServer Domäne:Benutzer-ID_für_Netzzugriff
Kennwort_für_Netzzugriff
```

Die Option fbserver gibt den kurzen Hostnamen der FastBack-Server-Workstation an. Für den FastBack DR Hub gibt die Option fbserver den Kurznamen der Workstation an, auf der der DR Hub installiert ist.

Benutzer-ID_für_Netzzugriff ist entweder die Windows-Administrator-ID oder das FastBack-Verwaltungskennwort.

Domäne ist der Domänenname der Benutzer-ID.

Kennwort_für_Netzzugriff ist entweder die Windows-Administrator-ID oder das FastBack-Verwaltungskennwort.

3. Diese Berechtigungsnachweise werden auf der Basis des kurzen Hostnamens abgerufen, den Sie mit der Option fbserver angeben.

Verwenden Sie TYPE=FILER auf Linux- und Windows-Systemen, um anzugeben, dass dieses Kennwort für Momentaufnahmedifferenzoperationen auf einem Dateiserver gilt.

Bei TYPE=FILER müssen Sie den Namen des Dateiservers sowie die Benutzer-ID und das Kennwort angeben, mit denen auf den Dateiserver zugegriffen wird.

Beispiel: `dsmc set password -type=filer myfiler filerid filerpasswd`.

Wenn Sie TYPE=FILER angeben, wird das Kennwort in der Kennwortdatei (TSM.sth) gespeichert, ohne zu überprüfen, ob das Kennwort gültig ist. Kennwörter, die mit TYPE=FILER gespeichert wurden, können von mehreren Clientknoten gemeinsam genutzt werden. Ein von Knoten NODE_A gespeichertes Kennwort kann beispielsweise von NODE_B verwendet werden. Für jeden Dateiserver wird nur ein Satz Berechtigungsnachweise gespeichert.

Verwenden Sie TYPE=VM, um ein Kennwort zu definieren, das für die Anmeldung bei einem ESX- oder vCenter-Server verwendet wird.

```
dsmc SET PASSWORD -type=VM Hostname Administrator Kennwort
```

Hierbei gilt Folgendes:

Hostname

Gibt den VMware VirtualCenter- oder ESX-Server an, der gesichert,

zurückgeschrieben oder abgefragt werden soll. Dieser Hostname muss der in der Option **vmchost** verwendeten Hostnamenssyntax entsprechen. Das heißt, wenn in **vmchost** kein Hostname, sondern eine IP-Adresse verwendet wird, muss in diesem Befehl die IP-Adresse und kein kurzer Hostname und kein vollständig qualifizierter Hostname angegeben werden.

Administrator

Gibt das für die Anmeldung beim ESXi-Host benötigte Konto an.

Kennwort

Gibt das Kennwort an, das dem Anmeldekonto zugeordnet ist, das Sie für den vCenter- oder ESXi-Administrator angegeben haben.

Verwenden Sie den Profileditor, um die Optionen **vmchost**, **vmcuser** und **vmcpw** zu definieren.

Sie können die Option **vmchost** auch in der Clientoptionsdatei definieren und anschließend mit dem Befehl **set password** diesen Hostnamen dem Administratorkonto und dem Kennwort des Administratorkontos zuordnen, mit denen die Anmeldung bei diesem Host ausgeführt wird. Beispiel: `set password TYPE=VM myvmchost.example.com Administratorname Administratorkennwort.`

Verwenden Sie **TYPE=VMGUEST** auf Linux- und Windows-Clients, wenn Sie die Option **INCLUDE.VMTSMVSS** zum Schutz einer virtuellen Maschine verwenden. Verwenden Sie für den Befehl **set password** das folgende Format:

```
set password -type=vmguest VM-Gastmaschine Administrator Kennwort
```

Hierbei gilt Folgendes:

VM-Gastmaschine

Gibt den Namen der virtuellen Gastmaschine an, die Sie schützen wollen.

Administrator

Gibt das für die Anmeldung bei der VM-Gastmaschine benötigte Konto an.

Kennwort

Gibt das Kennwort an, das dem Anmeldekonto zugeordnet ist.

Wenn Sie sich bei mehreren virtuellen Maschinen, die durch die Option **INCLUDE.VMTSMVSS** geschützt werden, mit denselben Berechtigungsnachweisen anmelden, können Sie das Kennwort für alle virtuellen Maschinen durch Angabe des Parameters **ALLVM** definieren. Der Parameter **ALLVM** bewirkt, dass bei der Anmeldung des Clients bei jeder Gastmaschine, die in einer Option **INCLUDE.VMTSMVSS** enthalten ist, dieselben Berechtigungsnachweise verwendet werden. Der folgende Befehl ist ein Beispiel für die Verwendung von **ALLVM**. In diesem Beispiel werden der Benutzername „Administrator“ und das Kennwort „Password“ für die Anmeldung bei jeder virtuellen Maschine verwendet, die Sie in einer Option **INCLUDE.VMTSMVSS** angegeben haben:

```
set password -type=vmguest ALLVM Administrator Password
```

Sie können auch eine Kombination aus gemeinsam genutzten und individuellen Berechtigungsnachweisen definieren. Wenn beispielsweise die meisten virtuellen Maschinen in Ihrer Umgebung dieselben Berechtigungsnachweise verwenden, aber einige virtuelle Maschinen andere Berechtigungsnachweise verwenden, können Sie mehrere Befehle **set password** verwenden, um die Berechtigungsnachweise anzugeben. Beispiel: Angenommen, die meisten virtu-

ellen Maschinen verwenden „Administrator1“ als Anmeldenamen und „Password1“ als Kennwort. Außerdem wird angenommen, dass eine virtuelle Maschine mit dem Namen VM2 „Administrator2“ als Anmelde-name und „Password2“ als Kennwort verwendet. Die folgenden Befehle werden verwendet, um die Berechtigungsnachweise für dieses Szenario zu definieren:

```
set password -type=vmguest ALLVM Administrator1 Password1 (definiert die Berechtigungsnachweise für die meisten virtuellen Maschinen).  
set password -type=vmguest VM2 Administrator2 Password2 (definiert eindeutige Berechtigungsnachweise für VM2).
```

Beispiele

Bei den folgenden Beispielen wird der Befehl **set password** verwendet.

Task Das Kennwort von osecret in nsecret ändern.

```
set password osecret nsecret
```

Task Eine Benutzer-ID und ein Kennwort für den Root auf dem Dateiserver myFiler.example.com definieren.

```
dsmc set password -type=filer myFiler.example.com root
```

Bitte Kennwort für Benutzer-ID "root@myFiler.example.com" eingeben:
***** Zur Bestätigung das Kennwort erneut eingeben: *****
ANS0302I Erfolgreich ausgeführt.

Task Eine Benutzer-ID und ein Kennwort für den Root auf dem Dateiserver myFiler.example.com definieren.

```
dsmc set password -type=filer myFiler.example.com root secret
```

Task Eine Benutzer-ID und ein Kennwort für den FastBack-Server myFastBackServer definieren. Verwenden Sie die Option **-fbserver** in den Befehlen **archive fastback** und **backup fastback** für den Servernamen.

```
dsmc set password -type=FASTBack myFastBackServer myUserId  
'pa$sword'
```

Wichtig:

1. Der Befehl `dsmc set password -type=fastback` muss auf einer dedizierten Client-Proxy-Workstation für jedes FastBack-Repository, zu dem der Client für Sichern/Archivieren eine Verbindung herstellen soll, einmal wiederholt werden.
2. Für gemeinsam genutzte Repositories im Netz geben Sie den Befehl `dsmc set password -type=fastback` im folgenden Format aus: `dsmc set password -type=fastback myFBServer domainName:userId password`. Der angegebene Servername, `myFBServer` in diesem Beispiel, muss mit dem Namen übereinstimmen, der in der Option **-fbserver** in einem Befehl **backup fastback** oder **archive fastback** angegeben wird.
3. Für den FastBack-Server oder den FastBack Disaster Recovery Hub muss die angegebene Benutzer-ID mit dem zugehörigen Kennwort über FastBack-Administratorberechtigungen verfügen.
Sie müssen den Befehl `dsmc set password -type=fastback` einmal für jedes Repository einer Filiale des FastBack-Servers auf dem FastBack DR Hub ausgeben, zu dem der Client für Sichern/Archivieren eine Verbindung herstellen soll.

Task Der Client für Sichern/Archivieren stellt eine Verbindung zu dem Fast-

Back-Server-Repository mit dem kurzen Hostnamen myFBServer her. USERID ist die FastBack-Netzbenutzer-ID, die über Schreib-/Lesezugriff auf die Repository-Freigabe verfügt. DOMAIN ist die Domäne, zu der die Benutzer-ID gehört. myNetworkPass ist das entsprechende Kennwort für die Benutzer-ID.

```
dsmc set password -type=fastback myFbServer DOMAIN:USERID  
myNetworkPass
```

Task Der Client für Sichern/Archivieren stellt eine Verbindung zu einem Repository auf einer DR Hub-Maschine mit dem kurzen Hostnamen myFbDrHub her. Die Benutzer-ID ist die Windows-Administrator-ID. DOMAIN ist die Domäne, zu der die DR Hub-Maschine gehört. myNetworkPass ist das entsprechende Kennwort für die Administrator-ID.

```
dsmc set password -type=fastback myFbDrHub DOMAIN:administrator  
adminPasswd
```

Zugehörige Verweise:

„Snapdiff“ auf Seite 581

Set Vmtags

Mit dem Befehl **set vmtags** werden Datenschutztags und Kategorien erstellt, die VMware-Bestandsobjekten hinzugefügt werden können. Sie können IBM Spectrum Protect-Sicherungen virtueller Maschinen in diesen VMware-Objekten verwalten, indem Sie die Tags mit Tools wie beispielsweise VMware vSphere PowerCLI Version 5.5 R2 oder höher angeben.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Wenn Sie die IBM Spectrum Protect vSphere-Client-Plug-in zum Verwalten von Sicherungen verwenden, müssen Sie nicht zuerst den Befehl **set vmtags** ausführen. Die Tags und Kategorien werden für Sie erstellt.

Wenn Sie Scripts schreiben, um diese Tags auf VMware-Bestandsobjekte anzuwenden, müssen Sie den Befehl **set vmtags** nur einmal ausgeben, damit Datenschutztags erstellt werden, bevor sie dem VMware-Bestand hinzugefügt werden.

Sie können Sicherungen virtueller Maschinen auf den folgenden VMware-Bestandsobjektebenen verwalten:

- Datencenter
- Ordner (Ordner 'Host' und 'Cluster' sowie Ordner 'VM' und 'Schablone')
- Host
- Host-Cluster
- Ressourcenpool
- Virtuelle Maschine

Die Liste der unterstützten Tags finden Sie in "Unterstützte Datenschutztags".

Bei Tags, die sich auf Zeitpläne beziehen, müssen sich die virtuellen Maschinen in einer Schutzgruppe befinden, die durch einen Zeitplan geschützt wird. Eine Schutzgruppe besteht aus den virtuellen Maschinen in einem Container, denen der Tag Schedule (IBM Spectrum Protect) zugeordnet ist.

Nach der Ausführung des Befehls **set vmtags** können Sie die Tags VMware-Objekten zuordnen, um den Schutz virtueller Maschinen zu steuern. Sie können beispielsweise virtuelle Maschinen in Services für geplante Sicherungen einschließen oder von ihnen ausschließen, die Aufbewahrungsmaßnahme für Sicherungen angeben, die Datenkonsistenz von Momentaufnahmen festlegen oder die zu schützenden Platten der virtuellen Maschinen auswählen.

Wenn die Datenschutztags bereits vorhanden sind, werden die Tags bei der Ausführung des Befehls **set vmtags** nicht erneut erstellt.

Wenn Sie einen Upgrade von einer Vorgängerversion der Einheit zum Versetzen von Daten durchführen, werden bei der erneuten Ausführung des Befehls **set vmtags** alle neuen Tags erstellt, die in der neuen Version der Einheit zum Versetzen von Daten verfügbar sind.

Voraussetzungen: Bevor Sie den Befehl **set vmtags** ausführen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Der VMware vCenter-Server muss über Version 6.0 Update 1 oder eine höhere Version verfügen.
- Die Option vmchost muss in der Datei dsm.opt auf Windows-Einheiten zum Versetzen von Daten oder in der Datei dsm.sys auf Linux-Einheiten zum Versetzen von Daten konfiguriert werden. Der Benutzername und das Kennwort, die dem Wert für vmchost zugeordnet sind, müssen ebenfalls definiert werden. Falls noch nicht definiert, können Sie den Befehl **dsmc set password** verwenden, um den Benutzernamen und das Kennwort zu definieren.

Unterstützte Clients

Dieser Befehl ist nur auf unterstützten Linux x86_64-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind, der VMware-Assets schützt.

Syntax

►►—SET VMTAGS—◄◄

Parameter

Für diesen Befehl sind keine Parameter erforderlich.

Beispiele

Task Erstellung von Datenschutztags und Kategorien, die VMware-Bestandsobjekten hinzugefügt werden können:

```
dsmc set vmtags
```

Zugehörige Konzepte:

„Verwaltungsklassen und Kopiengruppen“ auf Seite 310

Zugehörige Verweise:

„Unterstützte Datenschutztags“ auf Seite 829

„Vmchost“ auf Seite 637

„Vmtagdatamover“ auf Seite 668

„Set Password“ auf Seite 820

Übersicht über das Datenschutztagging

Um den Datenschutz für virtuelle Maschinen zu verwalten, können Sie VMware-Bestandsobjekten IBM Spectrum Protect-Tags zuordnen. Sie können VMware-Objekten Tags zuordnen, indem Sie Datenschutzeinstellungen in der IBM Spectrum Protect vSphere Client-Plug-in des vSphere-Web-Clients angeben. Wenn Sie die IBM Spectrum Protect vSphere Client-Plug-in nicht verwenden, können Sie Tags mithilfe von Scripting-Tools wie VMware Power CLI zuordnen.

Wenn Sie die Tagging-Unterstützung zur Verwaltung von Sicherungen aktivieren, können Sie den Schutz virtueller Maschinen steuern, um beispielsweise virtuelle Maschinen in Services für geplante Sicherungen einzuschließen oder von ihnen auszuschließen oder einen Zeitplan zum Schützen virtueller Maschinen in einem Container zuzuordnen. Bei Tags, die sich auf Zeitpläne beziehen, müssen sich die virtuellen Maschinen in einer Schutzgruppe befinden, die durch einen Zeitplan geschützt wird. Eine Schutzgruppe besteht aus den virtuellen Maschinen in einem Container, denen der Tag `Schedule` (IBM Spectrum Protect) zugeordnet ist.

Sie können auch die Aufbewahrungsmaßnahme für Sicherungen angeben, die Datenkonsistenz von Momentaufnahmen festlegen, die zu schützenden Platten der virtuellen Maschinen auswählen oder Anwendungsschutz mit der IBM Spectrum Protect vSphere Client-Plug-in aktivieren.

Die folgenden VMware-Bestandsobjekte sind die Container, mit denen Sie Sicherungen virtueller Maschinen verwalten können:

- Datencenter
- Ordner (Ordner 'Host' und 'Cluster' sowie Ordner 'VM' und 'Schablone')
- Host
- Host-Cluster
- Ressourcenpool
- Virtuelle Maschine

Wenn die Tagging-Unterstützung aktiviert ist, können Sie VMware-Containern Datenschutztags zuordnen. Wenn Sie die IBM Spectrum Protect vSphere-Client-Plug-in nicht verwenden, müssen Sie den Befehl **set vmtags** ausführen, um Datenschutzkategorien und -tags im VMware-Bestand zu erstellen.

Wenn die Option `vmtagdatamover` auf *yes* gesetzt wird, werden alle Tags, die einer virtuellen Maschine zugeordnet sind, während der Ausführung von Operationen **backup vm** gesichert. Die Tags werden zurückgeschrieben, wenn der Befehl **restore vm** ausgeführt wird. Tags, die anderen Bestandsobjekten zugeordnet sind, werden nicht gesichert und können nicht zurückgeschrieben werden.

Darstellung von Tags in der IBM Spectrum Protect vSphere Client-Plug-in

Wenn Sie Datenschutzeinstellungen im Fenster **IBM Spectrum Protect** in der IBM Spectrum Protect vSphere Client-Plug-in angeben, werden dem Bestandsobjekt Datenschutztags zugeordnet.

Wenn Sie beispielsweise **Ja** im Feld **Von Sicherung ausschließen** ausgewählt hatten, werden die Kategorie Backup Management (IBM Spectrum Protect) und der Tag Excluded dem Bestandsobjekt zugeordnet. Der zugeordnete Tag und die zugeordnete Kategorie werden im Portlet **Tags** auf der Registerkarte **Zusammenfassung** des Bestandsobjekts angezeigt.

Unterstützte Datenschutztags

IBM Spectrum Protect-Datenschutztags können VMware-Bestandsobjekten zugeordnet werden, um die Verwaltung von Sicherungen virtueller Maschinen zu steuern.



Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Wenn Sie die Sicherungsmaßnahme mithilfe der IBM Spectrum Protect vSphere Client-Plug-in konfigurieren, müssen Sie die Tags und Kategorien nicht manuell Bestandsobjekten zuordnen. Sie können das Fenster **IBM Spectrum Protect** verwenden, um Datenschutzeinstellungen für Bestandsobjekte im vSphere-Web-Client anzugeben. Diese Aktion ist äquivalent zur Zuordnung von Tags zu einem Bestandsobjekt.

Wenn Sie Scripting-Tools für das Tagging verwenden, können Sie den Befehl **set vmtags** in der Befehlszeile der Einheit zum Versetzen von Daten verwenden, um die Tags und Kategorien im vSphere-Bestand zu erstellen.

Sofern nicht anders angegeben, können Sie Datenschutztags den folgenden Typen von Bestandsobjekten zuordnen:

- Datencenter
- Ordner (Ordner 'Host' und 'Cluster' sowie Ordner 'VM' und 'Schablone')
- Host
- Host-Cluster
- Ressourcenpool
- Virtuelle Maschine

Die folgenden Datenschutztags werden unterstützt.

Kategorie	Tag	Tagbeschreibung
Application Protection (IBM Spectrum Protect)	Enabled	Anwendungsschutz wird von IBM Spectrum Protect bereitgestellt
Application Protection (IBM Spectrum Protect)	EnabledKeepSqlLog	Microsoft SQL Server schützen und Protokolldateien für die In-Guest-Protokolldateiverwaltung beibehalten
Backup Management (IBM Spectrum Protect)	Excluded	Das Objekt wird immer von Sicherungen mit IBM Spectrum Protect ausgeschlossen
Backup Management (IBM Spectrum Protect)	Included	Das Objekt wird immer in Sicherungen mit IBM Spectrum Protect eingeschlossen

Kategorie	Tag	Tagbeschreibung
Data Mover (IBM Spectrum Protect)	<i>Datamover_name</i>	Die Einheit zum Versetzen von Daten, die für Sicherungen in IBM Spectrum Protect verwendet wird
Data Mover (IBM Spectrum Protect)	Default Data Mover	Die Standardeinheit zum Versetzen von Daten, die einem Zeitplan (sofern vorhanden) zugeordnet ist, wird für Sicherungen in IBM Spectrum Protect verwendet
Disk Backup List (IBM Spectrum Protect)	Include Exclude: <i>disk number,disk number,...</i>	Die Liste der virtuellen Platten, die in Sicherungen mit IBM Spectrum Protect eingeschlossen oder von Sicherungen mit IBM Spectrum Protect ausgeschlossen werden
Local Backup Management (IBM Spectrum Protect) ¹	LocalIncluded	Das Objekt wird in lokale Sicherungen in den Hardwarespeicher eingeschlossen
Local Backup Management (IBM Spectrum Protect) ¹	LocalExcluded	Das Objekt wird von lokalen Sicherungen in den Hardwarespeicher ausgeschlossen
Local Management Class (IBM Spectrum Protect) ¹	<i>Management_class_name</i>	Die Maßnahme, die für Aufbewahrungseinstellungen für lokale Sicherungen in den Hardwarespeicher verwendet wird
Management Class (IBM Spectrum Protect)	<i>Management_class_name</i>	Die Maßnahme, die für Aufbewahrungseinstellungen in IBM Spectrum Protect verwendet wird
Schedule (IBM Spectrum Protect)	<i>Schedule_name</i>	Der Zeitplan, der für Sicherungen mit IBM Spectrum Protect verwendet werden soll
Schedule (IBM Spectrum Protect)	<i>Schedule_group</i>	Die Zeitplangruppe, die für Sicherungen mit IBM Spectrum Protect verwendet werden soll
Snapshot Attempts (IBM Spectrum Protect)	<i>quiesce,nonquiesce</i>	Die Anzahl stillgelegter und nicht stillgelegter Momentaufnahmen, die von IBM Spectrum Protect erstellt werden sollen, bevor die Sicherung fehlschlägt

¹ Diese Kategorie und dieser Tag gelten nur für virtuelle Maschinen, die in einem VVOL-Datenspeicher gespeichert werden.

Bei Namen von Kategorien und Tags in IBM Spectrum Protect muss die Groß-/Kleinschreibung beachtet werden. Die Kombinationen aus Kategorie und Tag sind wie folgt definiert:

Application Protection (IBM Spectrum Protect)

Enabled

Teilt Anwendungen virtueller Maschinen mit, dass in Kürze eine Sicherung ausgeführt werden soll. Diese Kombination aus Kategorie und Tag ermöglicht es einer Anwendung, Protokolle abzuschneiden und Transaktionen festzuschreiben, sodass die Anwendung nach dem Abschluss der Sicherung in einem konsistenten Zustand wiederaufgenommen werden kann.

Wenn einer virtuellen Maschine diese Kategorie und dieser Tag zugeordnet sind, wird Anwendungsschutz von IBM Spectrum Protect bereitgestellt. Die Einheit zum Versetzen von Daten blockiert (freeze) VSS Writer und hebt die Blockierung von VSS Writern auf (thaw) und schneidet Anwendungsprotokolle ab. Wenn einer virtuellen Maschine dieser Tag nicht zugeordnet ist, wird der Anwendungsschutz von VMware bereitgestellt, das die VSS Writer blockiert und die Blockierung der VSS Writer aufhebt, Anwendungsprotokolle aber nicht abschneidet.

Sie können diesen Tag und diese Kategorie nur virtuellen Maschinen zuordnen.

Wenn Sie diese Kategorie und diesen Tag einer virtuellen Maschine zuordnen, müssen Sie einen zusätzlichen Konfigurationsschritt ausführen. Speichern Sie auf jeder Einheit zum Versetzen von Daten, die Sie zum Sichern virtueller Maschinen verwenden, die Berechtigungsnachweise der virtuellen Gastmaschine in Data Protection for VMware, indem Sie in der Befehlszeile der Einheit zum Versetzen von Daten den folgenden Befehl ausführen:

```
dsmc set password -type=vmguest Anzeigename_der_VM-Gastmaschine Administrator-ID_für_Aministratorkennwort_für_Gastmaschine
```

Dabei gibt *Anzeigename_der_VM-Gastmaschine* den Namen der virtuellen Gastmaschine im VMware vSphere-Web-Client an.

Mit diesem Befehl werden die Berechtigungsnachweise der virtuellen Gastmaschine verschlüsselt auf dem System gespeichert, auf dem sich die Einheit zum Versetzen von Daten befindet. Für *Administrator-ID_für_Gastmaschine* und *Aministratorkennwort_für_Gastmaschine* sind mindestens die folgenden Berechtigungen erforderlich:

Sicherungsberechtigungen: Microsoft Exchange Server 2013 und 2016: Berechtigungen zur Organisationsverwaltung (Zugehörigkeit zur Verwaltungsrollengruppe, Organisationsverwaltung)

Sicherungsberechtigungen: Microsoft SQL Server 2014 und 2016: Berechtigungen zur Organisationsverwaltung (Zugehörigkeit zur Verwaltungsrollengruppe, Organisationsverwaltung)

Wenn Sie sich bei mehreren virtuellen Maschinen, die für den Anwendungsschutz aktiviert sind, mit denselben Berechtigungsnach-

weisen anmelden, können Sie das Kennwort für alle virtuellen Maschinen durch Angabe des Parameters **allvm** in dem folgenden Befehl festlegen:

```
dsmc set password -type=vmguest allvm Administrator-ID_für_Gastmaschine Administrator
```

Weitere Informationen finden Sie in Data Protection for VMware.

Wenn Sie den Anwendungsschutz nicht aktivieren, wird die Einstellung in der Option `include.vmtsmvss` verwendet. Diese Einstellung kann nicht geerbt werden.

Dieser Tag überschreibt die Option `include.vmtsmvss`.

EnabledKeepSqlLog

Stellt Anwendungsschutz bereit und verhindert, dass Microsoft SQL Server-Protokolle abgeschnitten werden, wenn eine Einheit zum Versetzen von Daten eine virtuelle Maschine sichert, auf der Microsoft SQL Server ausgeführt wird. Die Angabe dieses Tags ermöglicht es dem SQL Server-Administrator, die SQL Server-Protokolle manuell zu verwalten, sodass sie beibehalten und für die Zurschreibung von SQL-Transaktionen an einen bestimmten Prüfpunkt verwendet werden können, nachdem die virtuelle Maschine zurückgeschrieben wurde. Der SQL Server-Administrator muss die SQL Server-Protokolle auf der virtuellen Gastmaschine manuell sichern und gegebenenfalls abschneiden.

Sie können diesen Tag und diese Kategorie nur virtuellen Maschinen zuordnen. Zusätzlich zu diesem Tag müssen Sie den virtuellen Maschinen den Tag `Enabled` zuordnen.

Wenn dieser Tag angegeben wird, wird das SQL Server-Protokoll nicht abgeschnitten und die folgende Nachricht wird angezeigt und auf dem IBM Spectrum Protect-Server protokolliert:

```
ANS4179I Der IBM Spectrum Protect-Anwendungsschutz  
hat die Microsoft SQL Server-Protokolle auf der virtuellen Maschine 'VM' nicht abgeschnitten.
```

Wenn das Abschneiden der SQL Server-Protokolle nach dem Abschluss einer Sicherung ermöglicht werden muss, entfernen Sie den Tag `EnabledKeepSqlLog` und ordnen Sie der virtuellen Maschine die Kategorie Application Protection (IBM Spectrum Protect) und den Tag `Enabled` zu. In diesem Fall werden die SQL-Protokolldateien nicht von der Einheit zum Versetzen von Daten gesichert.

Wenn Sie diesen Tag nicht festlegen, werden Microsoft SQL Server-Protokolle während einer Sicherung mit aktiviertem Anwendungsschutz nicht beibehalten. Dieser Tag kann nicht geerbt werden.

Dieser Tag überschreibt den Parameter `keepsqllog` in der Option `include.vmtsmvss`.

Backup Management (IBM Spectrum Protect)

Excluded

Schließt die virtuellen Maschinen in einem Bestandsobjekt von Services für geplante Sicherungen aus.

Included

Schließt die virtuellen Maschinen in einem Bestandsobjekt in Services für geplante Sicherungen ein. Dieser Tag ist der Standardwert für die Kategorie Backup Management (IBM Spectrum Protect) und muss normalerweise nicht festgelegt werden.

Verwenden Sie diesen Tag, wenn einem übergeordnetes Objekt der Tag `Excluded` zugeordnet ist oder wenn sichergestellt werden soll, dass virtuelle Maschinen in einem Objekt, unabhängig von allen Vererbungseinstellungen, immer in geplante Sicherungen eingeschlossen werden sollen.

Wenn Sie diese Tags nicht zuordnen und keine geerbte Einstellung vorhanden ist, werden virtuelle Maschinen in geplante Sicherungen eingeschlossen.

Diese Tags überschreiben die Option `domain.vmfull` der Einheit zum Versetzen von Daten.

Data Mover (IBM Spectrum Protect)

Datamover_name

Ordnet eine Einheit zum Versetzen von Daten zur Ausführung von Sicherungen virtueller Maschinen zu.

Wenn Sie die IBM Spectrum Protect vSphere Client-Plug-in verwenden, werden Einheiten zum Versetzen von Daten automatisch virtuellen Maschinen zugeordnet, wenn Sie die Kategorie und den Tag `Schedule` auf einen Container anwenden. Sie können Einheiten zum Versetzen von Daten für einzelne virtuelle Maschinen jedoch auch manuell aktualisieren.

Wenn Sie nicht die IBM Spectrum Protect vSphere Client-Plug-in verwenden, um den Tag `Schedule` auf einen Container anzuwenden, müssen Sie die Tags für Einheiten zum Versetzen von Daten manuell den virtuellen Maschinen oder ihren übergeordneten Containern zuordnen, die sich in diesem Zeitplan befinden.

Wenn Sie einer virtuellen Maschine keine Einheit zum Versetzen von Daten zuordnen, wird die Einheit zum Versetzen von Daten des übergeordneten Objekts geerbt. Wenn keine geerbte Einstellung vorhanden ist oder der Tag `Default Data Mover` festgelegt ist oder geerbt wird, werden die virtuellen Maschinen von der Standardeinheit zum Versetzen von Daten gesichert, die einem Zeitplan (sofern vorhanden) zugeordnet ist. Andernfalls werden die virtuellen Maschinen nicht gesichert und in der IBM Spectrum Protect vSphere Client-Plug-in so lange mit dem Status **Gefährdet** gekennzeichnet, bis den virtuellen Maschinen eine Einheit zum Versetzen von Daten zugeordnet wird.

Dieser Tag überschreibt die Option `nodename` der Einheit zum Versetzen von Daten.

Default Data Mover

Ordnet die Standardeinheit zum Versetzen von Daten für einen Zeitplan (sofern vorhanden) für die Ausführung von Sicherungen virtueller Maschinen zu. Wenn für den Zeitplan keine Standardeinheit zum Versetzen von Daten festgelegt ist, werden die virtuellen Maschinen nicht gesichert und in der IBM Spectrum Protect vSphere Client-Plug-in so lange mit dem Status **Gefährdet** gekennzeichnet, bis den virtuellen Maschinen eine Einheit zum Versetzen von Daten zugeordnet wird oder bis dem Zeitplan eine Standardeinheit zum Versetzen von Daten zugeordnet wird.

Disk Backup List (IBM Spectrum Protect)

Include | Exclude:*disk number,disk number,...*

Schließt eine Gruppe von Festplatten virtueller Maschinen in Sicherungsoperationen ein oder von ihnen aus. Festplatten virtueller Maschinen werden in der virtuellen Maschine durch die Plattennummer identifiziert. Beispielsweise ist in den meisten Fällen Platte 1 die Systemplatte. Wenn Sie einer virtuellen Maschine diesen Tag nicht zuordnen, werden alle Festplatten in der virtuellen Maschine gesichert.

Aus Gründen der Benutzerfreundlichkeit wird die Kategorie Disk Backup List (IBM Spectrum Protect) vorab mit eine Reihe von häufig verwendeten Tags gefüllt:

Include:all

Schließt alle Platten in eine Sicherung ein.

Include:1

Schließt nur die Platte 1 in eine Sicherung ein und schließt explizit alle anderen Platten aus.

Exclude:1

Schließt alle Platten mit Ausnahme von Platte 1 in eine Sicherung ein.

Sie können die Plattennummern gemäß Ihren Anforderungen ändern. Sie können eine Plattennummer im Bereich von 1 bis 999 angeben. Die Plattennummern müssen als durch Kommas getrennte Werte ohne Leerzeichen zwischen den Kommas und den Zahlen angegeben werden.

Um beispielsweise nur die Platten 1, 3 und 5 in Sicherungen einzuschließen, ordnen Sie der virtuellen Maschine die Kategorie Disk Backup List (IBM Spectrum Protect) und den Tag `Include:1,3,5` zu.

Um alle Platten mit Ausnahme der Platten 1, 2 und 4 zu sichern, ordnen Sie der virtuellen Maschine die Kategorie Disk Backup List (IBM Spectrum Protect) und den Tag `Exclude:1,2,4` zu.

Wenn Sie die Platten, die eingeschlossen oder ausgeschlossen werden sollen, nicht angeben und keine geerbte Einstellung vorhanden ist, werden alle Platten virtueller Maschinen gesichert.

Diese Tags überschreiben die Optionen `include.vmdisk` und `exclude.vmdisk` der Einheit zum Versetzen von Daten.

Local Backup Management (IBM Spectrum Protect)**LocalExcluded**

Schließt Momentaufnahmen für virtuelle Maschinen in einem Bestandsobjekt von den Services für geplante Sicherungen aus.

LocalIncluded

Schließt Momentaufnahmen für virtuelle Maschinen in einem Bestandsobjekt in die Services für geplante Sicherungen ein. Dieser Tag ist der Standardwert für die Kategorie Local Backup Management (IBM Spectrum Protect) und muss normalerweise nicht festgelegt werden.

Verwenden Sie diesen Tag, wenn einem übergeordnetes Objekt der Tag `LocalExcluded` zugeordnet ist oder wenn sichergestellt werden soll, dass Momentaufnahmen für virtuelle Maschinen in einem Ob-

jekt, unabhängig von allen Vererbungseinstellungen, immer in geplante Sicherungen eingeschlossen werden sollen.

Wenn Sie diese Tags nicht zuordnen und keine geerbte Einstellung vorhanden ist, werden virtuelle Maschinen in geplante Sicherungen eingeschlossen.

Diese Tags überschreiben die Option `domain.vmfull` der Einheit zum Versetzen von Daten.

Local Management Class (IBM Spectrum Protect)

Management_class_name

Gibt den Namen der Aufbewahrungsmaßnahme an, die definiert, wie lange Momentaufnahmeversionen im Hardwarespeicher aufbewahrt werden oder wie viele Momentaufnahmeversionen im Speicher vorhanden sein können, bevor sie verfallen.

Wenn Sie die Verwaltungsklasse nicht angeben, wird die Aufbewahrungsmaßnahme eines übergeordneten Objekts geerbt. Wenn keine geerbte Einstellung vorhanden ist, wird die in der Option `vmmc` angegebene Verwaltungsklasse verwendet. Wenn die Option `vmmc` nicht definiert ist, wird die Standardaufbewahrungsmaßnahme für den Datacenterknoten verwendet.

Dieser Tag überschreibt die Option `include.vmlocalsnapshot`.

Management Class (IBM Spectrum Protect)

Management_class_name

Gibt den Namen der Aufbewahrungsmaßnahme an, die definiert, wie lange Sicherungsversionen auf dem IBM Spectrum Protect-Server aufbewahrt werden oder wie viele Sicherungsversionen auf dem Server vorhanden sein können, bevor sie verfallen.

Wenn Sie die Verwaltungsklasse nicht angeben, wird die Aufbewahrungsmaßnahme eines übergeordneten Objekts geerbt. Wenn keine geerbte Einstellung vorhanden ist, wird die in der Option `vmmc` angegebene Verwaltungsklasse verwendet. Wenn die Option `vmmc` nicht definiert ist, wird die Standardaufbewahrungsmaßnahme für den Datacenterknoten verwendet.

Dieser Tag überschreibt die Optionen `include.vm`, `vmmc` und `vmctlmc`.

Schedule (IBM Spectrum Protect)

Schedule_name

Gibt den Namen des Zeitplans an, der für Sicherungen virtueller Maschinen auf den IBM Spectrum Protect-Server verwendet wird. Der Zeitplanname muss eindeutig sein.

Zeitpläne werden vom IBM Spectrum Protect-Serveradministrator oder VMware-Administrator konfiguriert, um virtuelle Maschinen in Ihrem vSphere-Bestand automatisch zu sichern. Aus Gründen der Benutzerfreundlichkeit können Administratoren IBM Spectrum Protect Operations Center Version 8.1 verwenden, um Zeitpläne zu erstellen, die mit dem Tagging kompatibel sind.

Wenn Sie diese Kategorie und diesen Tag einer virtuellen Maschine zuordnen, werden alle virtuellen Maschinen auf der Bestandsobjektebene und allen untergeordneten Objektebenen gemäß dem Zeitplan gesichert.

Nur Zeitpläne mit der Option `-domain.vmfull="Schedule-Tag"` (ohne andere Parameter auf Domänenebene) in den Zeitplandefinitionen sind mit der Tagging-Unterstützung kompatibel. Andernfalls wird der Tag `Schedule` ignoriert und virtuelle Maschinen in Bestandsobjekten, denen Tags zugeordnet sind, die inkompatible Zeitpläne angeben, werden nicht gesichert.

Um mit dem Tagging kompatibel zu sein, müssen die folgenden Kriterien in die Zeitplandefinition eingeschlossen werden:

- Die Option `-domain.vmfull="Schedule-Tag"` (ohne andere Parameter auf Domänenebene) muss in der Optionszeichenfolge angegeben werden. Bei der Option muss die Groß-/Kleinschreibung nicht beachtet werden und die Option darf keine Leerzeichen enthalten. Die Anführungszeichen, die den Parameter `Schedule-Tag` einschließen, sind optional.
- Der Zeitplan muss die Parameter `ACTION=BACKUP` und `SUBACTION=VM` enthalten.
- Die Optionszeichenfolge muss die Option `-asnodename=Datencenter` enthalten; dabei muss der Wert für den Parameter `Datencenter` dem Datencenter entsprechen, das von der IBM Spectrum Protect vSphere Client-Plug-in verwaltet wird.
- Wenn die Option `-vmbackuptype=Sicherungstyp` in der Optionszeichenfolge angegeben wird, muss der Wert für den Parameter `Sicherungstyp` `FULLVM` lauten (die Groß-/Kleinschreibung muss dabei nicht beachtet werden).

In dem folgenden Beispiel eines Serverbefehls wird ein Zeitplan definiert, der mit dem Tagging kompatibel ist:

```
define schedule Domänenname Zeitplanname
description=Zeitplanbeschreibung action=backup subaction=VM
starttime=NOW+00:10 schedstyle=Classic period=1 perunits=Weeks
durunits=minutes duration=10 options='-vmbackuptype=fullvm
-asnodename=Name_des_Datencenterknotens -mode=IFIncremental
-domain.vmfull="Schedule-Tag"
```

Der Serveradministrator muss außerdem dem Zeitplan mit dem folgenden Serverbefehl eine Einheit zum Versetzen von Daten zuordnen:

```
define association Domänenname Zeitplanname Knotenname_der_Einheit_zum_Versetzen_von_
```

Diese Kategorie und dieser Tag können Datencentern, Ordnern, Hosts, Host-Clustern, Ressourcenpools und virtuellen Maschinen zugeordnet werden.

Tipp: Wenn Sie den Tag `Schedule` einem Container zuordnen, ohne die IBM Spectrum Protect vSphere Client-Plug-in zu verwenden, werden die Kategorie und der Tag `Data Mover` nicht automatisch den virtuellen Maschinen in dem Container zugeordnet. Sie müssen den Tag `Data Mover` jeder virtuellen Maschine manuell zuordnen. Wenn ein Zeitplan nur einer einzigen Einheit zum Versetzen von Daten zugeordnet ist, ist es auch möglich, die Einheit zum Versetzen von Daten direkt dem Container zuzuordnen, der durch den Zeitplan geschützt wird.

Wenn Sie diesen Tag für ein Objekt nicht festlegen, wird der Tag `Schedule` des übergeordneten Objekts geerbt. Wenn keine geerbte Einstellung vorhanden ist, werden virtuelle Maschinen nicht in geplante Sicherungen eingeschlossen.

Alle Parameter auf Domänenebene in der Option `domain.vmfull` der Einheit zum Versetzen von Daten werden für einen Zeitplan, der mit dem Tagging kompatibel ist, ignoriert.

Schedule_group

Gibt den Namen der Zeitplangruppe an, die für Sicherungen virtueller Maschinen verwendet wird. Eine Zeitplangruppe enthält mehrere Zeitpläne. Mithilfe des IBM Spectrum Protect vSphere Client-Plug-ins können Sie statt eines einzigen Zeitplans die Zeitplangruppe einem Objekt im VMware vSphere-Web-Client zuordnen. Ein Beispiel für die Verwendung dieser Option ist die Gruppierung mehrerer Zeitpläne zur täglichen lokalen Sicherung in einem einzigen Zeitplan zur Sicherung des IBM Spectrum Protect-Servers.

Snapshot Attempts (IBM Spectrum Protect)

quiesce,nonquiesce

Diese Kombination aus Kategorie und Tag gibt die Gesamtzahl Versuche an, eine Momentaufnahme für eine Sicherungsoperation für eine virtuelle Maschine zu erstellen, die aufgrund eines Momentaufnahmefehlers fehlschlägt. Der Tagwert besteht aus einem Paar positionsgebundener Parameter, die angeben, wie oft versucht wurde, eine Momentaufnahme zu erstellen, sowie die Datenkonsistenz, die während des Versuchs erzielt werden sollte.

quiesce

Ein positionsgebundener Parameter, der angibt, wie oft versucht werden soll, die Momentaufnahme mit Stilllegung zu erstellen, wobei eine anwendungskonsistente Momentaufnahme erstellt wird.

- Für virtuelle Windows-Maschinen, denen der Tag Application Protection zugeordnet ist, gibt der Parameter *quiesce* die Anzahl Versuche zur Erstellung der Momentaufnahme mit IBM Spectrum Protect-VSS-Stillegung und Microsoft Windows-System-Provider-VSS-Stillegung an.

Abhängig von der von Ihnen angegebenen Anzahl, erfolgt der erste Versuch zur Erstellung einer Momentaufnahme immer mit IBM Spectrum Protect-VSS-Stillegung. Nachfolgende Versuche zur Erstellung einer Momentaufnahme erfolgen mit Windows-System-Provider-VSS-Stillegung.

- Für virtuelle Windows-Maschinen ohne den Tag Application Protection oder für virtuelle Linux-Maschinen gibt der Parameter *quiesce* die Anzahl Versuche zur Erstellung einer Momentaufnahme mit VMware Tools-Dateisystemstillegung an.

Sie können einen Wert im Bereich von 0 bis 10 angeben. Der Standardwert ist 2.

nonquiesce

Ein positionsgebundener Parameter, der angibt, wie oft versucht werden soll, die Momentaufnahme ohne Stillegung zu erstellen, nachdem die Versuche, die Momentaufnahme mit Stillegung zu erstellen (wie durch den Parameter *quiesce* angegeben) abgeschlossen sind. Ohne die

Stilllegung von Momentaufnahmen werden absturzkonsistente Momentaufnahmen erstellt. Bei absturzkonsistenten Momentaufnahmen kann keine Betriebssystem-, Dateisystem- und Anwendungskonsistenz garantiert werden.

Sie können einen Wert im Bereich von 0 bis 10 angeben. Der Standardwert ist 0.

Einschränkung: Der Eintrag 0,0 ist nicht gültig. Für Sicherungsoperationen ist mindestens eine Momentaufnahme erforderlich.

Die folgenden Versuche, eine Momentaufnahme zu erstellen, sind für die Datenkonsistenz übliche Auswahlmöglichkeiten:

2,0 - Immer anwendungskonsistent

Es wird versucht, zwei stillgelegte Momentaufnahmen zu erstellen, bevor die Sicherung fehlschlägt. Diese Kombination ist der Standardwert.

2,1 - Versuch, Anwendungskonsistenz zu erzielen

Es wird versucht, zwei stillgelegte Momentaufnahmen und - als letzter Versuch - eine nicht stillgelegte, absturzkonsistente Momentaufnahme zu erstellen.

0,1 - Nur maschinenkonsistent

Es wird versucht, nur eine nicht stillgelegte Momentaufnahme für virtuelle Maschinen zu erstellen, für die nie eine stillgelegte Momentaufnahme ausgeführt werden kann.

Wenn Sie die Versuche zur Erstellung einer Momentaufnahme nicht angeben und keine geerbte Einstellung vorhanden ist, werden die in der Option `include.vmsnapshotattempts` angegebenen Versuche zur Erstellung einer Momentaufnahme verwendet.

Dieser Tag überschreibt die Option `include.vmsnapshotattempts`.

Tipp: Datenschutztags können von Bestandsobjekten höherer Ebene geerbt werden. Weitere Informationen finden Sie in „Vererbung von Datenschutzeinstellungen“.

Zugehörige Verweise:

„Schedgroup“ auf Seite 564

„Vmtagdatamover“ auf Seite 668

„Vmtagdefaultdatamover“ auf Seite 670

„Domain.vmfull“ auf Seite 414

„Include.vmdisk“ auf Seite 482

„INCLUDE.VMSNAPSHOTATTEMPTS“ auf Seite 485

„INCLUDE.VMTSMVSS“ auf Seite 488

Vererbung von Datenschutzeinstellungen

IBM Spectrum Protect-Datenschutzeinstellungen oder -tags können von einem übergeordneten Bestandsobjekt einer höheren Ebene im vSphere-Web-Client-Navigator geerbt, das heißt, an eine niedrigere Ebene übergeben werden.

Wenn Sie einem Bestandsobjekt im vSphere-Web-Client einen Datenschutztage zuordnen, erben die untergeordneten Objekte den Datenschutztage des übergeordneten Bestandsobjekts, dem der Tag zugeordnet wurde.

Die folgende Liste zeigt die Typen von vSphere-Bestandsobjekten, die mit Tags versehen werden können und Datenschutztags erben können:

- Datencenter
- Ordner (Ordner 'Host' und 'Cluster' sowie Ordner 'VM' und 'Schablone')
- Host
- Host-Cluster
- Ressourcenpool
- Virtuelle Maschine

Wenn Sie beispielsweise einem Host-Cluster den Tag `Excluded` zuordnen, übernehmen alle untergeordneten Objekte des Host-Clusters (Host, Hostordner und virtuelle Maschine) den Tag `Excluded`. In diesem Beispiel werden alle virtuellen Maschinen in dem Host-Cluster von geplanten Sicherungen ausgeschlossen.

Wenn einem untergeordneten Objekt ein Tag zugeordnet wird und das Objekt Tags in derselben Kategorie erbt, überschreibt der zugeordnete Tag des untergeordneten Objekts den geerbten Tag. Wenn ein untergeordnetes Objekt Tags in derselben Kategorie von mehreren Vorfahrenobjekten erbt, überschreibt der Tag, der vom nächststehenden Vorfahren geerbt wird, die Tags anderer Vorfahren.

Wenn in der vSphere-Bestandshierarchie keine Datenschutztags zugeordnet sind, werden die Standardtageinstellungen des Systems angewendet. Informationen zu den unterstützten Tags und alle Standardtageinstellungen finden Sie in "Unterstützte Datenschutztags".

Vorrangregelung bei der Vererbung

Abhängig von dem Objekt (Zielobjekt), dem ein Datenschutztag zugeordnet werden soll, ist eine Rangfolge vorhanden, um den Abstand des Zielobjekts zu seinen Vorfahren bei der Verarbeitung der Tagvererbung von mehreren Vorfahren zu bestimmen. Die folgende Tabelle enthält Zielobjekte und die potenziellen Vorfahren jedes Zielobjektyps auf der Basis der Objekthierarchie im vSphere-Web-Client-Navigators.

Tabelle 115. Vorrangregelung bei vSphere-Bestandsobjekten

Zielobjekt	Vorrangregelung bei verarbeiteten Tags
Virtuelle Maschine	Virtuelle Zielmaschine → Verschachtelte VM-Ordner → Verschachtelte Ressourcenpools → Host → Host-Cluster → Verschachtelte Hostordner → Datencenter
VM-Ordner	VM-Zielordner → Andere verschachtelte VM-Ordner → Datencenter
Hostordner	Zielhostordner → Andere verschachtelte Hostordner → Datencenter
Ressourcenpool	Zielressourcenpool → Anderer verschachtelter Ressourcenpool → Verschachtelte VM-Ordner → Host → Host-Cluster → Verschachtelte Hostordner → Datencenter
Host	Zielhost → Verschachtelte Hostordner → Cluster → Datencenter
Cluster	Zielcluster → Verschachtelte Hostordner → Datencenter
Datencenter	Zieldatencenter

Wenn das Zielobjekt eine virtuelle Maschine ist, können der virtuellen Maschine selbst und jeder beliebigen Kombination seiner Vorfahren (einschließlich VM-Ord-

ner, Ressourcenpools, Host, Host-Cluster, Hostordner, Datacenter) Tags aus derselben Kategorie zugeordnet werden. Während der Verarbeitung wird jeder Objekttyp gemäß der Vorrangregelung überprüft; die Verarbeitung wird gestoppt, wenn ein Tag in derselben Kategorie gefunden wird oder das Ende der Liste erreicht wird.

Um beispielsweise zu bestimmen, ob die Kombination aus dem Tag Excluded oder Included und der Kategorie Backup Management (IBM Spectrum Protect) auf virtuelle Maschinen angewendet wird, durchsucht IBM Spectrum Protect den Bestand eines Datacenters nach den Tags Excluded und Included. Gemäß der Vorrangregelung für das VM-Zielobjekt beginnt die Suche nach den Tags Excluded und Included mit dem Zielobjekt (der virtuellen Maschine) selbst, gefolgt von der Liste potenzieller Vorfahren. Wenn ein Tag gefunden wird, bevor das Ende der Liste erreicht wird, wird dieser Tag auf das Zielobjekt angewendet. Andernfalls wird kein Tag der Kategorie Backup Management (IBM Spectrum Protect) auf die virtuelle Zielmaschine angewendet.

Zugehörige Konzepte:

„Tipps für das Datenschutztagging“

Zugehörige Verweise:

„Unterstützte Datenschutztags“ auf Seite 829

Tipps für das Datenschutztagging

Sicherungsmaßnahmen werden durch die Zuordnungen von Datenschutztags zu vSphere-Bestandsobjekten festgelegt. Die Anzahl Tags, die auf den vSphere-Bestand angewendet und die Stelle, an der die Tags angewendet werden, kann ebenfalls Auswirkungen auf die Leistung bei der Verarbeitung von Datenschutztags haben.

Ziehen Sie die Ausführung der folgenden Aktionen in Betracht, wenn Sie die Sicherungsmaßnahme für Objekte im vSphere-Bestand definieren:

- Nutzen Sie die Vorteile der Vorrangregelung beim Tagging von Bestandsobjekten. Erstellen Sie eine allgemeine Maßnahmenkonfiguration für ein Unternehmen, indem Sie Sicherungsmaßnahmen (oder Tags) für den Container an der höchsten Position in der vSphere-Bestandshierarchie festlegen. Die Maßnahmen werden von untergeordneten Containern und ihren virtuellen Maschinen geerbt. Im Allgemeinen müssen Sie keine Maßnahmen für einzelne virtuelle Maschinen festlegen.

Erstellen Sie dann Ausnahmen, indem Sie die Maßnahme für einen untergeordneten Container oder für einzelne virtuelle Maschinen ändern, um die geerbte Maßnahmeneinstellung zu überschreiben.

Sie können auch wie folgt vorgehen: Wenn keine Gesamtsicherungsmaßnahme konfiguriert werden soll, ordnen Sie keinen Objekten höherer Ebene Datenschutztags zu. Ordnen Sie die Datenschutztags Objekten niedrigerer Ebene zu.

- Vermeiden Sie zur Vereinfachung der Verwaltung und zur Verbesserung der Leistung und Benutzerfreundlichkeit die Zuordnung von Tags zu zu vielen Bestandsobjekten.
- Vermeiden Sie zur Vereinfachung der Verwaltung und zur Verringerung der Komplexität die Zuordnung von Tags zu unterschiedlichen Objekttypen. Ordnen Sie beispielsweise Tags ausschließlich Clustern, Hosts, Hostordnern und VMs oder ausschließlich VM-Ordern und VMs, aber nicht beiden Objekttypen gleichzeitig zu.
- Bei der Tagging-Unterstützung können Sie mehrere Zeitpläne mehreren Einheiten zum Versetzen von Daten zuordnen. Die Zeitpläne für eine Einheit zum Versetzen von Daten dürfen sich jedoch nicht überschneiden. Andernfalls werden einige Zeitpläne übersprungen.

- Aus Gründen der Benutzerfreundlichkeit können Administratoren IBM Spectrum Protect Operations Center Version 8.1 verwenden, um Zeitpläne zu erstellen, die mit dem Tagging kompatibel sind.

Zugehörige Konzepte:

„Vererbung von Datenschutzeinstellungen“ auf Seite 838

Anhang. 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(www.w3.org/TR/wai-aria/), um die Einhaltung von US Section 508(www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) und der Web Content Accessibility Guidelines (WCAG) 2.0(www.w3.org/TR/WCAG20/) 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 (www.ibm.com/support/knowledgecenter/about/releasesnotes.html?view=kc#accessibility).

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 (www.ibm.com/able).

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden. IBM stellt dieses Material möglicherweise auch in anderen Sprachen zur Verfügung. Für den Zugriff auf das Material in einer anderen Sprache kann eine Kopie des Produkts oder der Produktversion in der jeweiligen Sprache erforderlich sein.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

*IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
France*

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

*IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US*

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesen Informationen beschriebenen Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete, der IBM Lizenzvereinbarung für Maschinencode oder einer äquivalenten Vereinbarung.

Die in diesem Dokument enthaltenen Leistungsdaten wurden von bestimmten Betriebsbedingungen abgeleitet. Die tatsächlichen Ergebnisse können davon abweichen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren; sie können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Beispielanwendungsprogramme, die in Quellsprache geschrieben sind und Programmier Techniken in verschiedenen Betriebsumgebungen veranschaulichen. Sie dürfen diese Beispielprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, zu verwenden, zu vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle für die Betriebsumgebung konform sind, für die diese Beispielprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten. Die Beispielprogramme werden ohne Wartung (auf "as-is"-Basis) und ohne jegliche Gewährleistung zur Verfügung gestellt. IBM übernimmt keine Haftung für Schäden, die durch die Verwendung der Beispielprogramme entstehen.

Kopien oder Teile der Beispielprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten: © (Name Ihrer Firma) (Jahr). Teile des vorliegenden Codes wurden aus Beispielprogrammen der IBM Corp. abgeleitet. © Copyright IBM Corp. _Jahr/Jahre angeben_.

Marken

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der IBM Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicennamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite "Copyright and trademark information" unter www.ibm.com/legal/copytrade.shtml.

Adobe ist eine eingetragene Marke von Adobe Systems Incorporated in den USA und/oder anderen Ländern.

Linear Tape-Open, LTO und Ultrium sind Marken von HP, der IBM Corporation und von Quantum in den USA und/oder anderen Ländern.

Intel und Itanium sind Marken oder eingetragene Marken der Intel Corporation oder ihrer Tochtergesellschaften in den USA oder anderen Ländern.

Linux ist eine eingetragene Marke von Linus Torvalds in den USA und/oder anderen Ländern.

Microsoft, Windows und Windows NT sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Java und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken der Oracle Corporation und/oder ihrer verbundenen Unternehmen.

UNIX ist eine eingetragene Marke von The Open Group in den USA und anderen Ländern.

VMware, VMware vCenter Server und VMware vSphere sind eingetragene Marken oder Marken der VMware, Inc. oder ihrer Tochtergesellschaften in den USA und/oder anderen Ländern.

Bedingungen für Produktdokumentation

Die Berechtigungen zur Nutzung dieser Veröffentlichungen werden Ihnen auf der Basis der folgenden Bedingungen gewährt.

Anwendbarkeit

Diese Bedingungen sind eine Ergänzung der Nutzungsbedingungen auf der IBM Website.

Persönliche Nutzung

Sie dürfen diese Veröffentlichungen für Ihre persönliche, nicht kommerzielle Nutzung unter der Voraussetzung vervielfältigen, dass alle Eigentumsvermerke erhalten bleiben. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM nicht weitergeben, anzeigen oder abgeleitete Werke davon erstellen.

Kommerzielle Nutzung

Sie dürfen diese Veröffentlichungen nur innerhalb Ihres Unternehmens und unter der Voraussetzung, dass alle Eigentumsvermerke erhalten bleiben, vervielfältigen, weitergeben und anzeigen. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM außerhalb Ihres Unternehmens weder vervielfältigen, weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Berechtigungen

Abgesehen von den hier gewährten Berechtigungen werden keine weiteren Berechtigungen, Lizenzen oder Rechte (veröffentlicht oder stillschweigend) in Bezug auf die Veröffentlichungen oder darin enthaltene Informationen, Daten, Software oder geistiges Eigentum gewährt.

IBM behält sich das Recht vor, die hierin gewährten Berechtigungen nach eigenem Ermessen zurückzuziehen, wenn sich die Nutzung der Veröffentlichungen für IBM als nachteilig erweist oder wenn die obigen Nutzungsbestimmungen nicht genau befolgt werden.

Sie dürfen diese Informationen nur in Übereinstimmung mit allen anwendbaren Gesetzen und Vorschriften, einschließlich aller US-amerikanischen Exportgesetze und Verordnungen, herunterladen und exportieren.

IBM übernimmt keine Gewährleistung für den Inhalt dieser Informationen. Diese Veröffentlichungen werden auf der Grundlage des gegenwärtigen Zustands (auf "as-is"-Basis) und ohne eine ausdrückliche oder stillschweigende Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit für einen bestimmten Zweck oder die Freiheit von Rechten Dritter zur Verfügung gestellt.

Hinweise zur Datenschutzrichtlinie

IBM Softwareprodukte, einschließlich Software as a Service-Lösungen ("Softwareangebote"), können Cookies oder andere Technologien verwenden, um Informationen zur Produktnutzung zu erfassen, die Endbenutzererfahrung zu verbessern und Interaktionen mit dem Endbenutzer anzupassen oder zu anderen Zwecken. In vielen Fällen werden von den Softwareangeboten keine personenbezogenen Daten erfasst. Einige der IBM Softwareangebote können Sie jedoch bei der Erfassung personenbezogener Daten unterstützen. Wenn dieses Softwareangebot Cookies zur Erfassung personenbezogener Daten verwendet, sind nachfolgend nähere Informationen über die Verwendung von Cookies durch dieses Angebot zu finden.

Dieses Softwareangebot verwendet keine Cookies oder andere Technologien zur Erfassung personenbezogener Daten.

Wenn die für dieses Softwareangebot bereitgestellten Konfigurationen Sie als Kunde in die Lage versetzen, personenbezogene Daten von Endbenutzern über Cookies und andere Technologien zu erfassen, müssen Sie sich zu allen gesetzlichen Bestimmungen in Bezug auf eine solche Datenerfassung rechtlich beraten lassen, insbesondere Meldepflichten sowie die Einforderung von Einwilligungen.

Weitere Informationen zur Nutzung verschiedener Technologien, einschließlich Cookies, für diese Zwecke finden Sie in den Schwerpunkten der IBM Online-Datenschutzerklärung unter <http://www.ibm.com/privacy>, in der IBM Online-Datenschutzerklärung unter <http://www.ibm.com/privacy/details> im Abschnitt "Cookies, Web-Beacons und sonstige Technologien" und auf der Seite "IBM Software Products and Software-as-a-Service Privacy Statement" unter <http://www.ibm.com/software/info/product-privacy>.

Glossar

Ein Glossar mit Begriffen und Definitionen für die IBM Spectrum Protect-Produktfamilie ist verfügbar.

Siehe das Glossar für IBM Spectrum Protect.

Index

Sonderzeichen

* ? 245

Numerische Stichwörter

128-Bit-AES-Verschlüsselung, Unterstützung für 173

256-Bit-AES-Verschlüsselung, Unterstützung für 173

A

Abfrage

aktive und inaktive Objekte anzeigen 471

basierend auf Datum und Zeit der Sicherung, Archivierung 461, 463

Beschreibung für 397

Dateien für einen anderen Knoten 461

Einschluss-/Ausschlussliste 760

Gruppe

Befehl 756

Member anzeigen 579

Informationsumfang, der auf dem Bildschirm angezeigt wird 572

Knoten, für die der Client über Proxy-Berechtigung verfügt 282

Knoten, für die der Client über Proxy-Knotenberechtigung verfügt 200

NAS- oder Clientobjekte 374

nur Verzeichnisse verarbeiten (keine Dateien) 403

Systeminformationen 767

Vorgaben für Blättern, wenn Informationen auf dem Bildschirm angezeigt werden 573

zeitpunktgesteuerte Sicherungen definieren 529, 530

Abfrage, Zurückschreiben ohne 271

Abruf

anderen Benutzern Berechtigung erteilen 274

archivierte Dateien mit Befehlen 287

Archivierungskopien 286

auf andere Workstation 632

ausführen 287

basierend auf Datum und Zeit der Archivierung 461, 463

Beschreibung für 397

btrfs 216

Dateien, die zu einem anderen Knoten gehören 275

Dateien auf eine andere Workstation 276

Dateien für einen anderen Knoten 461

Dateiliste 453

Dateiliste sortieren 162

Eingabeaufforderung vor dem Überschreiben vorhandener Dateien 547

feste Verbindungen 286

Geschwindigkeit mit Shared Memory verbessern 325

nur Verzeichnisse verarbeiten (keine Dateien) 403

primäre Tasks 279

symbolische Verbindungen 285

vorhandene Datei durch letzte Archivierung ersetzen, falls diese neuer als die vorhandene Datei ist 468

während der Übernahme 257

Web-Clientsitzung starten 158

Zusammenfassung der Optionen 337

Abruf, maximale Dateigröße 179

absolute (Option) 355

Absoluter Modus 314

Absoluter Mount, NFS 243

ACL

unterstützte Dateisysteme 174

afmskipuncachedfiles 356

AIX

für Momentaufnahmen konfigurieren 118

Workloadpartition (WPAR)

restore 263

Sicherung 226

AIX, Plattenspeicherplatz 4

AIX-Client

Clientkomponenten 4

Deinstallation 15

Installation 11

Übertragungsmethoden 4

AIX-Hardwarevoraussetzungen 4

AIX-Komponenten

installierbar 4

AIX-Softwarevoraussetzungen 4

AIX-Systemvoraussetzungen 4

Aktive Sicherungsversionen

anzeigen 162, 267

Anzeigen 748

Zurückschreibung 267

Anwendungsprogrammierschnittstelle (API)

Definition 67

Anzeigen

Archivierungsinformationen 745

geplante Ereignisse 765

Maßnahmeninformationen 311

Onlinehilfe 163

Sitzungsinformationen 765

wiederanlauffähige Zurückschreibungssitzungen 764

API unter Linux on Power Systems

Deinstallation 27

archive

Anzahl Versuche zum Archivieren offener Dateien 373

Befehl 692

Benutzerzugriff abfragen 745

Beschreibung zuordnen 397

Bestätigungsaufforderung vor dem Löschen unterdrücken 519

Dateien einschließen 473

Dateien komprimieren 380

Dateien löschen 397

Dateiliste 453

Datum der letzten Änderung und Datum des letzten Zugriffs/Erstellungsdatum anzeigen 745

einzelne Archive aus dem Dateibereich des Servers löschen 721

gemeinsam genutzte Daten auf mehreren Clients unter einem einzigen Knotennamen 359

Informationen, Abfrage 745

lokale Momentaufnahme Serverdateibereich zuordnen 593

nur Dateien 627

nur Verzeichnisse verarbeiten (keine Dateien) 403

removeoperandlimit 546

Verwaltungsklasse binden 357

- archive fastback
 - Befehl 695
- Archivierung
 - Aufbewahrungszeitraum 310
 - ausführen 279
 - Beschreibung über Befehlszeile zuordnen 282
 - btrfs 216
 - Dateibereiche löschen 199, 277
 - einzelne Archive aus dem Dateibereich des Servers löschen 284
 - feste Verbindungen 286
 - gemeinsam genutzte Daten auf mehreren Clients unter einem einzigen Knotennamen 282
 - Geschwindigkeit mit Shared Memory verbessern 325
 - Kopiengruppenattribut 311
 - Kopienmodus 314
 - Liste von Dateien 282
 - lokale Momentaufnahme Serverdateibereich zuordnen 282
 - mehrere Dateispezifikationen 282
 - mit Befehlen 280, 284
 - nur Dateien; keine Verzeichnisse 282
 - primäre Tasks 279
 - symbolische Verbindungen 285
 - über die Befehlszeile abrufen 287
 - Unterstützung für den Clientknoten-Proxy konfigurieren 282
 - Unterverzeichnisse 282
 - Verwaltung 288, 309
 - Verwaltungsklasse überschreiben während 317
 - Verwaltungsklassen an Dateien binden 282
 - Web-Clientsitzung starten 158
 - Zusammenfassung der Optionen 326
- Archivierung, maximale Dateigröße 179
- Archivierungskopiengruppe 310
- archmc (Option) 357
- archsmlinkasfile (Option) 358
- asnodename (Option) 359
- asnodename, Sitzungseinstellungen 360
- auditlogging (Option) 361
- auditlogname (Option) 363
- Aufbewahrungszeitraum
 - Archivierung 310, 319
 - Sicherung 310, 319
- Ausführbare Datei
 - Rückkehrcodes 307
- Ausschließen von Dateien
 - Platzhalterzeichen 136
 - Platzhalterzeichen verwenden 137
 - Systemdateien 134
- Austauschbare Datenträger
 - Sicherungssätze zurückschreiben 250
- Authentifizierung
 - IBM Spectrum Protect-Client 152
- autodeploy (Option) 365
- autofsrename (Option) 366
- Automatische Aktualisierung 365
- Automatische Clientaktualisierung 2
- Automatisierte Clientübernahme
 - andere Komponenten 101
 - Daten abrufen 257
 - Daten zurückschreiben 257
 - Einschränkungen 100
 - Konfiguration 102
 - Konfiguration und Verwendung 98
 - Replikationsstatus bestimmen 104
 - Übernahme erzwingen 106
 - Übersicht 98

Automatisierte Clientübernahme (Forts.)

- Verbindung testen 106
- verhindern 105
- Voraussetzungen 99
- automount (Option) 368

B

- backmc (Option) 369
- backup fastback (Befehl) 697
- backup group (Befehl) 699
- backup image
 - btrfs 216
- backup image (Befehl) 702
 - unterstützte Einheiten 209
- backup image (Befehl), Unterstützung nach Einheitentyp des Datenträgers 209
- backup nas (Befehl) 708
- backup vm (Befehl) 710
- backupsetname (Option) 370
- basesnapshotname (Option) 371
- Bedingter Mount, NFS 243
- Befehl
 - Abruf 805
 - allgemeine Regeln für die Eingabe von Optionen mit Befehlen 347
 - archive 692
 - archive fastback 695
 - backup fastback 697
 - backup group 699
 - backup image 702
 - backup nas 708
 - backup vm 710
 - cancel process 719
 - cancel restore 719
 - Dateispezifikation angeben 689
 - delete access 720
 - delete archive 721
 - delete backup 722
 - delete filespace 727
 - delete group 728
 - eingeben 688
 - expire 729
 - help 731
 - in die Befehlszeile eingeben 688
 - incremental 733
 - interaktiver Modus (loop) 687
 - loop 739
 - macro 741
 - maximale Anzahl Dateispezifikationen 689
 - monitor process 742
 - Optionen in Befehlen verwenden 346
 - Platzhalterzeichen verwenden 691
 - preview archive 743
 - preview backup 744
 - query access 745
 - query archive 745
 - query backup 748
 - query backupset 751, 753
 - query filespace 754
 - query group 756
 - query image 758
 - query inclexcl 760
 - query mgmtclass 761
 - query node 762
 - query options 763
 - query restore 764

- Befehl (*Forts.*)
 - query schedule 765
 - query session 765
 - query systeminfo 767
 - query VM 768
 - restart restore 771
 - restore 771
 - restore backupset 777, 781
 - restore backupset, Hinweise 253, 780
 - restore group 784
 - restore image 786
 - restore NAS 789
 - restore vm 791
 - schedule 808
 - Selektive Sicherung 810
 - set access 814
 - set event 817
 - set netappsvm 819
 - set password 820
 - set vmtags 826
 - Stapelbetrieb 686
 - Übersicht über die Parameter 689
 - verwenden 683
- Befehle
 - geplant, aktivieren oder inaktivieren 302
 - in ausführbaren Dateien verwenden 307
 - in Shell-Scripts verwenden 307
- Befehlsparameter
 - Übersicht 689
- Befehlssitzung
 - beenden 686
 - starten 686
- Befehlsverarbeitung, Zusammenfassung der Optionen 343
- Befehlszeile
 - aktuelle Einstellungen für Clientoptionen anzeigen 763
 - allgemeine Regeln für die Eingabe von Optionen mit Befehlen 347
 - anzeigen
 - Verarbeitungsstatus 235
 - archivierte Dateien abrufen 287
 - Beenden einer Sitzung 164
 - Befehle eingeben 688
 - Beschreibung einer Archivierung zuordnen 282
 - Dateien archivieren 284
 - Dateispezifikation angeben 689
 - Einschränkungen für NAS-Dateisysteme 219
 - Imagesicherung ausführen 215
 - NAS-Dateisysteme sichern 222
 - Optionsdatei während Sitzung angeben 523
 - Platzhalterzeichen verwenden 691
 - Rückkehrcodes für Operationen 307
 - Starten einer Sitzung 155
 - Übersicht über die Parameter 689
 - umfangreiche Zurückschreibungsoperationen ausführen 270
 - Verwaltungsklasse während der Archivierung überschreiben 317
 - Zurückschreibung nach Zeitpunkt durchführen 260
- Behinderung 843
- Benutzerberechtigungen
 - definieren 159
- Berechtigte Benutzer
 - Verschlüsselung aktivieren 56
- Berechtigter Benutzer
 - Definition 53
 - Tasks 53

- Berechtigung
 - Optionen 343
- Berechtigung erteilen
 - anderen Benutzern zum Zurückschreiben oder Abrufen eigener Dateien 274
- Berechtigungen
 - Standardzugriffs- und erweiterte Berechtigungen sichern 285
- Betriebssystemvoraussetzungen
 - Clients 3
- Bourne- und Korn-Shell
 - auf Clientbenutzeroptionsdatei zeigen 60
- Bourne- und Korn-Shell-Variablen definieren 66
- btrfs 248, 786
- btrfs (Dateisystem)
 - Abruf 216
 - Archivierung 216
 - backup image 216
 - restore image 216
 - Schutz 217
 - Sicherung 216
 - Unterdatenträger schützen 218
 - Zurückschreibung 216
- Btrfs-Dateisysteme schützen 217
- Btrfs-Unterdatenträger schützen 218

C

- C-Mode 121
- C-shell-Variablen
 - definieren 67
- cadlistenonport (Option) 372
- cancel process (Befehl) 719
- cancel restore (Befehl) 719
- changingretries (Option) 373
- CIFS
 - Dateisysteme sichern 224
- class (Option) 374
- Client
 - andere Client-TCP/IP-Adresse als die für den ersten Serverkontakt 611
 - andere Client-TCP/IP-Anschlussnummer als die für den ersten Serverkontakt 612
 - auf dem Server registrieren 128
 - automatische Aktualisierung 2
 - Größe des TCP/IP-Schiebefensters für Clientknoten 615
 - Kennwort definieren 128
- Client für Sichern/Archivieren
 - GUI 221
 - Installation 11
 - NAS
 - Dateisysteme sichern 221
 - Übersicht 1
- Client für Sichern/Archivieren, GUI
 - Datenfernverarbeitung durch Firewall aufbauen 74
- Client-Scheduler
 - Anzeigen geplanter Arbeit 299, 301
 - automatisch starten 160
 - beim Systemstart ausführen 297
 - Optionen für 302
 - starten 72, 808
- Client/Server-Kommunikation
 - andere Client-TCP/IP-Adresse als die für den ersten Serverkontakt 611
 - andere Client-TCP/IP-Anschlussnummer als die für den ersten Serverkontakt 612

Client/Server-Kommunikation (*Forts.*)

- Anzahl Kilobyte angeben, die der Client puffert, bevor er eine Transaktion an den Server sendet 623
- Einrichtung 58
- Größe des internen TCP/IP-Kommunikationspuffers 610
- Größe des TCP/IP-Schiebefensters für Clientknoten 615
- Ihre Workstation beim Server identifizieren 517
- kleine Transaktionen ohne vorherige Pufferung an den Server senden 613
- maximale Platten-E/A-Puffergröße, die der Client für Lesen oder Schreiben von Dateien verwendet 405
- Methode 376
- Name des Servers angeben, der für Services kontaktiert werden soll 574
- Standardserver angeben 396
- TCP/IP-Adresse des IBM Spectrum Protect-Servers 614
- TCP/IP-Adresse für dsmcad 610
- TCP/IP-Anschlussadresse des IBM Spectrum Protect-Servers 614
- TCP/IP-Anschlussadresse für Aufbau einer Verbindung über gemeinsam genutzten Speicher 579
- Verbindungswiederherstellungsintervall nach Fehler 378
- Verbindungswiederherstellungsversuche nach Fehler 378
- Clientakzeptordämon
 - Scheduler, Web-Client oder beides verwalten 502
 - zum Verwalten des Schedulers konfigurieren 70
- Clientbefehlsoptionen
 - Übersicht 688
- Clientbenutzeroptionen
 - anpassen 62
- Clientbenutzeroptionsdatei
 - mit Befehlen überschreiben 346
- Clientknoten-Proxy
 - Sicherung 202
 - Übersicht über die Archivierung 282
 - Unterstützung 282
 - Zeitplanung 202
- Clientknoten-Proxy, Unterstützung für 200
- Clientkomponenten
 - AIX-Client 4
 - Linux on Power Systems-Client 5
 - Linux on System z-Client 7
 - Linux x86_64-Client 6
 - Mac OS X-Client 8
 - Oracle Solaris-Client 9
- Clientoptionen
 - aktuelle Einstellungen anzeigen 763
 - exclude
 - exclude.archive 131
 - exclude.attribute.symlink 131
 - exclude.backup 131
 - exclude.compression 131
 - exclude.dir 131
 - exclude.file 131
 - exclude.file.backup 131
 - exclude.fs 131
 - exclude.image 131
 - in Befehlen verwenden 346
 - mit Hilfe der Befehlszeile überschreiben 346
 - Reihenfolge der Verarbeitung (Vorrangstellung) 346
 - Übersicht 688
- Clientoptionsdatei
 - erforderliche Optionen für 58
 - erstellen und ändern 58
 - Übersicht 56
- Clientoptionsreferenz 355

Clientsystemoptionen

- exclude
 - exclude.archive 131
 - exclude.attribute.symlink 131
 - exclude.backup 131
 - exclude.compression 131
 - exclude.dir 131
 - exclude.file 131
 - exclude.file.backup 131
 - exclude.fs 131
- Clientsystemoptionsdatei
 - Include/Exclude-Optionen angeben 129
 - kopieren und ändern 58
- Clientverwaltungsservice 51
- Clustered Data ONTAP 121
- Clusterumgebung
 - IBM Spectrum Protect installieren 108
- collocatebyfilespec (Option) 375
- commmethod (Option) 376
- Common Internet File System (CIFS)
 - Dateisysteme sichern 224
- commrestartduration (Option) 378
- commrestartinterval (Option) 378
- compressalways (Option) 379
- compression
 - Include/Exclude-Anweisungen 479
 - Verarbeitung aktivieren 479
 - Verarbeitung inaktivieren 479
- compression (Option) 380
- console (Option) 382
- createnewbase 383
- createnewbase (Option) 383
- csv (Option) 385

D

- datacenter (Option) 388
- datastore (Option) 389
- dateformat (Option) 389
- Dateibereich
 - ausschließen 131
 - FSID bestimmen 398
 - Imagesicherung ausführen 702
 - löschen 199, 277
 - Löschen 727
 - NAS- oder Clientobjekte 374
- Dateibereiche 180
- Dateien
 - anderen Benutzern Berechtigung zum Zurückschreiben oder Abrufen erteilen 274
 - archivierte, Verwaltungsklasse überschreiben 317
 - archivierte abrufen 287
 - Archivierung 279, 692
 - Archivierung, Verwaltung 288
 - Archivierung mit Befehlen 284
 - Archivierungsinformationen abfragen 745
 - auf andere Workstation zurückschreiben oder abrufen 276
 - Benutzerzugriff abfragen 745
 - Dateien abrufen, die zu einem anderen Knoten gehören 275
 - Dateien zurückschreiben, die zu einem anderen Knoten gehören 275
 - Definition geänderter Dateien 183
 - Einschluss-/Ausschluss
 - im Unicode-Format erstellen 472
 - Einschluss-/Ausschlussverarbeitung 141

Dateien (*Forts.*)

- einzelne Archive aus dem Dateibereich des Servers löschen 284, 721
 - einzelne Sicherungen aus dem Dateibereich des Servers löschen 722
 - fest verbundene sichern 242
 - fest verbundene zurückschreiben 242
 - Gruppen ausschließen 136, 137
 - Gruppen einschließen 136, 137
 - Liste sortieren 162
 - Liste von Dateien archivieren 282, 453
 - maximale Dateigröße für Operationen 179
 - mehrere Dateispezifikationen archivieren 282
 - mit Befehlen abrufen 287
 - mit freien Bereichen zurückschreiben 243
 - nach Archivierung löschen 397
 - Nicht-Unicode-Dateibereiche in Unicode-fähige Dateibereiche umbenennen 366, 810
 - offene sichern 244
 - Sicherungsinformationen abfragen 748
 - umfangreiche Zurückschreibungsoperationen ausführen 270
 - Verschlüsselung 173
 - Verwaltungsklassen binden an 318
 - Verwaltungsklassen zuordnen 239
 - Wachstum während der Komprimierung verwalten 379
 - während der Archivierung oder Sicherung komprimieren 380
 - Zurückschreibung 268
 - Zurückschreibung, mit Befehlen 274
- Dateien mit freien Bereichen
- Sicherung 243
 - Verwendungshinweise zum Zurückschreiben oder Abrufen 501
 - Zurückschreibung 243
- Dateien mit freien Bereichen sichern 243
- Dateien mit freien Bereichen zurückschreiben 243
- Dateien von den Sicherungsservices ausschließen 172
- Dateispezifikation
- maximal zulässige Anzahl in Befehlen 689
- Dateisysteme
- ACL-Unterstützung 174
 - Btrfs 174
 - Dateien von der Sicherungsverarbeitung ausschließen 438
 - gelöscht 244
 - GPFS, Clusterumgebung mit mehreren Knoten 174, 407
 - Imagesicherung 206
 - QFS, Einschränkungen 174
 - unterstützte 174
 - virtuellen Mountpunkt definieren 630
- Daten
- Zurückschreibung 269
- Daten sichern 232
- Daten während der Archivierung verschlüsseln 173
- Daten während der Sicherung verschlüsseln 173
- Datendeduplizierung 90
- Datendeduplizierung, Clientkonfiguration 94
- Datendeduplizierungsdateien
- ausschließen 97
- Datendeduplizierungsdateien ausschließen 97
- Datenschutzeinstellungen
- als Tags dargestellt 828
 - Tipps zum Konfigurieren von Sicherungsmaßnahmen 840
 - Vererbung 838
- Datenschutztagging
- Liste unterstützter Tags 829
 - Übersicht 828

Datenschutztagging (*Forts.*)

- Vererbung von Tags 838
- Datenträger sichern 180
- Datenträgerkennsatz
- doppelte Namen 180
- Datenträgername 180
- Datenträgernamen, Hinweise
- Dual-Boot-Systeme 181
 - UNIX-Mountpunkt 180
- Datum des letzten Zugriffs
- angeben, ob Aktualisierung während Sicherung oder Archivierung erfolgen soll 183
 - beim Sichern oder Archivieren aktualisieren 536
- Datum des letzten Zugriffs aktualisieren 536
- Datumsformat
- angeben 389
- dedupcachepath (Option) 393
- dedupcachesize (Option) 394
- deduplication (Option) 394
- defaultserver (Option) 396
- Definieren
- Benutzerberechtigungen 159
- Definieren von Umgebungsvariablen
- API, UNIX und Linux
 - DSMI_CONFIG 67
 - DSMI_DIR 67
 - DSMI_LOG 67
- Deinstallation
- AIX-Client 15
 - API unter Linux on Power Systems 27
 - API unter Ubuntu Linux on Power Systems (Little Endian) 25
 - Client unter Linux on Power Systems (Little Endian) 21
 - Client unter Ubuntu Linux on Power Systems (Little Endian) 25
 - HP-UX Itanium 2-API 17
 - IBM Spectrum Protect auf Mac OS X-Client 44
 - IBM Spectrum Protect auf Oracle Solaris x86_64-Client 48
 - IBM Spectrum Protect in Oracle Solaris SPARC-API 50
 - Linux on System z-Client 41
 - Linux x86_64-Client 32, 37
- delete access (Befehl) 720
- delete archive (Befehl) 721
- delete backup (Befehl) 722
- delete group (Befehl) 728
- deletefiles (Option) 397
- description (Option) 397
- detail (Option) 311, 398
- Diagnose
- Optionen 346
- Diagnoseinformationen erfassen 51
- diffsnapshot (Option) 400
- diffsnapshotname (Option) 401
- dirmc (Option) 402
- dirsonly (Option) 403
- disablenqr (Option) 404
- diskbuffsize (Option) 405
- diskcachelocation (Option) 406
- domain
- für Imagesicherung einschließen 412
 - für NAS-Imagesicherung einschließen 413
 - für Teilsicherung einschließen 407
 - für vollständige VM-Sicherungen einschließen 414
- domain (Option) 407
- domain.image (Option) 412
- domain.nas (Option) 413
- domain.vmfull (Option) 414

- Domäne
 - Laufwerke in der Standarddomäne angeben 193
 - mit der grafischen Benutzerschnittstelle sichern 193
 - Teilsicherung 242
- dontload (Option) 421
- DSM_CONFIG 64
 - auf Clientbenutzeroptionsdatei zeigen 60, 64
 - Datei .cshrc hinzufügen 67
 - Verwendung auf Solaris 64
- DSM_DIR
 - Datei .cshrc hinzufügen 67
 - für Image-/NAS-Sicherung oder -Zurückschreibung definieren 64
 - zeigen auf ausführbare Dateien 64
 - zeigen auf Datei dsm.sys 64
 - zeigen auf Ressourcendateien 64
- DSM_LOG
 - Datei .cshrc hinzufügen 67
 - zeigen auf dsmerror.log, dsmwebcl.log, dsm sched.log 64
- dsm.opt (Datei)
 - anpassen 62
 - Beispiel 60
 - erforderliche Optionen für 58
 - erstellen 60
 - erstellen und ändern 58
 - Laufwerkspezifikation mit Platzhalterzeichen angeben 136
- dsm.opt.smp (Datei) 60
- dsm.smp (Datei)
 - nach dsm.opt kopieren 58
 - Position 58
- dsm.sys (Datei)
 - Beispiel 58
 - erstellen 58
- dsm.sys.smp (Datei) 58
- dsmerlog.pru, Datei 434
- dsmererror.log
 - mit DSM_LOG zeigen auf 64
- dsmererror.log, Datei 434
- DSMI_CONFIG, Umgebungsvariable
 - API, UNIX und Linux 67
- DSMI_DIR, Umgebungsvariable
 - API, UNIX und Linux 67
- DSMI_LOG, Umgebungsvariable
 - API, UNIX und Linux 67
- dsm sched.log 565, 568
- dsm tca, ausführbare Datei
 - mit DSM_DIR zeigen auf 64
- dsm webcl.log 565, 568
- Dual-Boot-Systeme
 - doppelte Namen 181
- Durchnummerierung
 - Kopiennummerierung
 - dynamisch 313
 - gemeinsam statisch 313
 - statisch 313
- dynamicimage (Option) 423
- Dynamisch, gemeinsam (Durchnummerierung) 313

E

- EFS (Encrypted File Systems - Verschlüsselte Dateisysteme)
 - Dateisysteme sichern 228
 - Dateisysteme zurückschreiben 262
- efsdecrypt (Option) 424
- Eigenständiger Anwendungsschutz 488
- Eingabezeichenfolgen
 - mit Leerzeichen 157

- Einrichtung
 - erforderliche Root-Tasks 58
- Einschließen
 - INCLUDE.VMDISK 482
 - INCLUDE.VMLOCALSNAPSHOT 484
- Einschluss-/Ausschlussliste 172
 - erstellen 129
 - Größeneinschränkung 141
 - Reihenfolge der Verarbeitung abfragen 760
 - Voranzeige 140
- Einschluss-/Ausschlussoptionsdatei
 - für die Archivierungsverwaltung 288
 - Pfad und Dateinamen angeben 471
 - Übersicht 172
 - Unicode-fähige Dateibereiche 471
 - Verarbeitung von unten nach oben 141
- Einschluss-/Ausschlussverarbeitung
 - Optionen für 131
 - Übersicht 131
- Einschränkungen
 - asnodename (Option) 359
 - asnodename, Sitzungseinstellungen 360
 - innerhalb einer Sitzung mit Proxy-Berechtigung 201, 282
 - vollständigen Pfad mit Clientakzeptordämon angeben 523
- Einschränkungen bei Sitzungen mit Proxy-Berechtigung 201, 282
- Einzelne Sicherungen aus dem Dateibereich des Servers löschen 197
- Einzige Version aufbewahren, Attribut 313
- enablearchiveretentionprotection (Option) 425
- enablededupcache (Option) 426
- enableinstrumentation (Option) 427
- enablelanfree (Option) 429
- encryptiontype (Option) 173, 431
- encryptkey (Option)
 - encryptkey=generate 432
 - encryptkey=prompt
 - encryptkey=save 432
- Ereignisgesteuerte Maßnahme für Aufbewahrungsschutz
 - Archivierung 320
 - Sicherung 320
- Ereignisprotokollierung
 - Scheduler 301
- Erneutes Binden von Dateien an andere Verwaltungsklasse 319
- errorlogmax (Option) 434
- errorlogname (Option) 435
- errorlogretention (Option) 434, 436
- Erste Schritte
 - Beenden einer Sitzung 145
 - Befehlszeilensitzung 145
 - Client-Scheduler 145
 - Dateilisten sortieren 145
 - GUI-Sitzung 145
 - Kennwort ändern 145
 - Online-Hilfetext anzeigen 145
 - Web-Clientsitzung 145
- Erweiterte Berechtigungen
 - Archivierung 285
- Erweiterter Befehl query schedule 765
- Erweitertes query schedule 299
- exclude
 - EXCLUDE.VMDISK 443
 - EXCLUDE.VMLOCALSNAPSHOT 445
- exclude.image (Option) 131
- Exclude-Optionen 438
 - exclude.archive 131

- Exclude-Optionen (*Forts.*)
 - exclude.attribute.symlink 131
 - exclude.backup 131
 - exclude.compression 131
 - exclude.dir 131
 - exclude.file 131
 - exclude.file.backup 131
 - exclude.fs 131
 - exclude.image 131
 - Platzhalterzeichen 136, 137
 - preview 140
 - Verarbeitung 141
- EXCLUDE.VMDISK 443
- EXCLUDE.VMLOCALSNAPSHOT 445
- expire (Befehl) 729
- Extraversionen aufbewahren, Attribut 313

F

- fbbranch (Option) 446
- fbclient (Option) 447
- fbpolicyname (Option) 448
- fbreposlocation (Option) 450
- fbserver (Option) 451
- fbvolumename (Option) 452
- Fehlerbehebung 277
- Fehlerprotokoll 64
 - bereinigen 436
 - Pfad und Dateinamen angeben 435
- Fehlerverarbeitung, Zusammenfassung der Optionen 344
- Feste Verbindungen
 - Archivierung und Abruf 286
 - Sicherung 242
 - Zurückschreibung 242
- Feste Verbindungen sichern 242
- Feste Verbindungen zurückschreiben 242
- filelist (Option) 453
- filename (Option) 456
- filesonly (Option) 457
- Firewall
 - Datenfernverarbeitung aufbauen 74, 465, 614
 - Einleitung von Sitzungen über die Firewall durch Server oder Client 576
 - TCP/IP-Anschlüsse für den Web-Client angeben 680
 - Web-Client verwenden 680
- followsymbolic (Option) 458
- forcefailover (Option) 460
- Format
 - Zusammenfassung der Optionen 342
- Format und Sprache
 - Zusammenfassung der Optionen 342
- fromdate (Option) 461
- fromnode (Option) 461
- fromowner (Option) 462
- fromtime (Option) 463
- Funktionen zur behindertengerechten Bedienung 843

G

- Geändert (Modus) 312
- Gelöschte Dateisysteme 244
- Gemeinsam dynamisch (Durchnummerierung) 313, 373
- Gemeinsam statisch (Durchnummerierung) 313, 373
- Geplante (automatisierte) Sicherungen
 - Anwendungen nach Sicherung erneut starten 244
 - Anzeigen geplanter Arbeit 299, 301

- Geplante (automatisierte) Sicherungen (*Forts.*)
 - Befehle nach Sicherung verarbeiten 531
 - Befehle vor Sicherung verarbeiten 534
 - Dateien vor Sicherung schließen 244
 - Optionen für 302
 - starten 72
- Geplante Befehle
 - aktivieren und inaktivieren 302
- Geplante Ereignisse anzeigen 765
- Geplante Services
 - Einschränkungen für NAS-Dateisysteme 219
 - geplante Befehle inaktivieren 562, 563
 - Zeitpläne für andere Benutzer-IDs als Null definieren 302
- Gesamtsicherung erstellen 233
- Geschlossene Registrierung
 - Berechtigungen 128
 - verwenden 128
- Gleichzeitig ausgeführte Sicherungen 234
- GPFS (Dateisystem)
 - Clusterumgebung mit mehreren Knoten 174, 407
 - Speicherpools 259
 - Zeitplanung 205
- Grafische Benutzerschnittstelle
 - aktive und inaktive Sicherungsversionen anzeigen 162, 267
 - Ändern des Kennworts 160
 - Beenden einer Sitzung 164
 - einzelne Dateien oder Images aus dem Dateibereich des Servers löschen 722
 - für das Zurückschreiben lokaler Sicherungssätze aktivieren 500
 - Imagesicherung ausführen 213
 - lokalen Sicherungssatz aktivieren 250
 - Online-Hilfetext anzeigen 163
 - Starten einer Sitzung 153
 - Verarbeitungsstatus anzeigen 235
 - zum Sichern von Objekten verwenden 193
- Grobe Übereinstimmung, Sicherungsversion mit 313
- groupname (Option) 464
- Gruppensicherung
 - aktive und inaktive Objekte anzeigen 471
 - alle Member anzeigen 579
 - Name der Gruppe angeben 464
 - Namen des virtuellen Dateibereichs angeben 630
 - Übersicht 199
 - vollständige oder differenzielle Sicherung angeben 509
- GUI
 - Beenden einer Sitzung 164
 - Starten einer Sitzung 153
 - Verwaltungsklasse während der Archivierung überschreiben 317
 - Zurückschreibung nach Zeitpunkt durchführen 260

H

- Hardwarevoraussetzungen, AIX 4
- Hardwarevoraussetzungen, HP-UX Itanium 2 5
- Hardwarevoraussetzungen, Linux on Power Systems 6
- Hardwarevoraussetzungen, Linux System z 7
- Hardwarevoraussetzungen, Linux x86_64 7
- Hardwarevoraussetzungen, Mac OS X 8
- Hardwarevoraussetzungen, Solaris 9
- help (Befehl) 731
- Hilfe
 - Internetressourcen 163
 - Kundendienst und technische Unterstützung 163
 - Onlineforum 163

- Hilfe (*Forts.*)
 - Onlinehilfe anzeigen 163
- Hinweise für Sicherung 238
- Hochkommas oder Anführungszeichen 157
- host (Option) 464
- HP-UX Itanium 2, Plattenspeicherplatz 5
- HP-UX Itanium 2-API
 - Deinstallation 17
 - Installation 15
 - Übertragungsmethoden 5
- HP-UX Itanium 2-Client
 - Standardbegrenzung für Datensegmentgröße erhöhen 17
- HP-UX Itanium 2-Hardwarevoraussetzungen 5
- HP-UX Itanium 2-Softwarevoraussetzungen 5
- HP-UX Itanium 2-Systemvoraussetzungen 5
- HP-UX-Komponenten
 - installierbar 5
- httpport (Option) 465

I

- IBM Knowledge Center xiv
- IBM PowerHA SystemMirror-Cluster
 - Zeitplanung 203
- IBM Spectrum Protect
 - Clientkomponenten
 - AIX-Client 4
 - Linux on Power Systems-Client 5
 - Linux on System z-Client 7
 - Linux x86_64-Client 6
 - Mac OS X-Client 8
 - Oracle Solaris-Client 9
 - Installationsvoraussetzungen 8
 - Kennwort 155
 - Onlineforum 164
 - Übertragungsmethoden
 - AIX-Client 4
 - HP-UX Itanium 2-API 5
 - Linux on Power Systems-Client 6
 - Linux on System z-Client 7
 - Linux x86_64-Client 7
 - Mac OS X-Client 8
 - Oracle Solaris-Client 9
 - Upgrade von älteren Versionen des Produkts durchführen 1
- IBM Spectrum Protect auf Mac OS X-Client
 - Deinstallation 44
- IBM Spectrum Protect auf Oracle Solaris x86_64-Client
 - Deinstallation 48
 - Installationsschritte 45
- IBM Spectrum Protect-Client
 - Authentifizierung 152
- IBM Spectrum Protect in Oracle Solaris SPARC-API
 - Deinstallation 50
 - Installationsschritte 49
- IBM Spectrum Protect installieren
 - Clusterumgebung 108
- IBM Spectrum Protect-Kennwort
 - verwenden 154
- ieobjtype (Option) 467
- ifnewer (Option) 468
- Image
 - mit chkdsk reparieren 248
 - mit fsck reparieren 248, 786
 - mit Tool chkdsk reparieren 786
 - Zurückschreibung 248

- Image in Datei
 - Zurückschreibung 258
- imagegapsize (Option) 469
- Imagesicherung
 - ausführen 206
 - Dateien ausschließen 438
 - Dateien einschließen für; Verwaltungsklasse zuordnen zu 473
 - Hinweise 208
 - Imageteilsicherung nach Datum 212
 - include.dedup 473
 - Löschen 722
 - mit DSM_DIR auf Plug-In-Bibliothek zeigen 64
 - mit Teilsicherung 211, 706
 - mit Teilsicherung des Dateisystems verwenden 212
 - mit Teilsicherung nach Datum verwenden 212
 - mithilfe der grafischen Benutzerschnittstelle 213
 - selektive Sicherung oder Teilsicherung angeben 509
 - statisch, dynamisch, Momentaufnahme 206
 - über die Befehlszeile 215
 - Unterstützung nach Einheitentyp des Datenträgers 209
 - Zugriff widerrufen 720
 - Zurückschreibung nach Zeitpunkt 706
- Imagesicherung, Hinweise 208
- imagetofile (Option) 470
- inactive (Option) 471
- Inaktive Sicherungsversionen
 - anzeigen 162, 267
 - Anzeigen 748
 - Zurückschreibung 267
- indexcl (Option) 471
- include (Option)
 - Platzhalterzeichen 136, 137
 - Verarbeitung 141
 - Verwaltungsklasse 316
- include.vm (Option) 481
- INCLUDE.VMDISK 482
- INCLUDE.VMLOCALSNAPSHOT 484
- include.vmsnapshotattempts, Option 485
- include.vmtsmvss (Option) 488
- incrbydate (Option) 490
- incremental (Befehl) 733
 - Journalgestützte Sicherung 737
- incremental (Option) 492
- Installation
 - AIX-Client 11
 - API unter Linux on Power Systems (Big Endian) 25
 - API unter Ubuntu Linux on Power Systems (Little Endian) 22
 - Client für Sichern/Archivieren 11
 - Client unter Linux on Power Systems (Little Endian) 18
 - Client unter Ubuntu Linux on Power Systems (Little Endian) 22
 - HP-UX Itanium 2-API 15
 - Linux on System z-Client 38
 - Linux x86_64-Client 29
 - Mac OS X-Client 43
 - Solaris SPARC-API 49
 - Solaris x86_64-Client 45
 - Übersicht 1
 - Ubuntu x86_64-Client 34
- Installationsschritte
 - IBM Spectrum Protect auf Oracle Solaris x86_64-Client 45
 - IBM Spectrum Protect in Oracle Solaris SPARC-API 49
 - Mac OS X-Client 43
- Installationsvoraussetzungen
 - AIX-Client 4

Installationsvoraussetzungen (*Forts.*)

- Client 3
- HP-UX Itanium 2-API 5
- Linux for zSeries-Client 7
- Linux on Power Systems 5
- Linux x86_64-Client 6
- Solaris-Client 9

Installieren des Clientverwaltungsservice 51

instrlogmax (Option) 492

instrlogname (Option) 493

Instrumentierungsprotokoll

- Erfassung von Leistungsdaten 427
- Größe steuern 492
- Pfad und Dateinamen zum Speichern von Leistungsdaten angeben 493

Integritätsprüfungen für Sicherungsketten 673, 675

Interaktive Sitzung

- beenden 739
- starten 156, 739
- verwenden 739

Interaktiver Modus 687

J

Java-GUI

- Konfigurationseinschränkungen 155

journalbasierte Sicherung

- Ausschließen von Dateien 132
- Ausschließen von Verzeichnissen 132
- Einschluss-/Ausschlussoptionen
 - journalbasierte Sicherung 132
- Konfigurationseinstellungen angeben 83
- Start des Journaldämons 83
- Stopp des Journaldämons 83
- Vergleich mit vollständiger Teilsicherung und Teilsicherung nach Datum 188
- Verwendung 188
- Zurückschreibung 187

Journalbasierte Sicherung 185

Journalbasierte Sicherungen

- Zurückschreibung 187

Journaldämon

- Einstellungen für Journalkonfigurationsdatei 83
- Start des Journaldämons 83
- Stopp des Journaldämons 83

Journaldatenbankdateien

- ErrorLog 85
- JournalDir 85

journalgestützte Sicherung 737

- stattdessen traditionelle vollständige Teilsicherung ausführen 519

Journalgestützte Sicherung

- stattdessen traditionelle vollständige Teilsicherung ausführen 737

Journalkonfigurationsdatei

- Hinweise zur Konfiguration 83

K

Kennwort

- ändern 160
- Anzahl Zeichen 160
- für Client definieren 128
- gültige Zeichen 160
- verwenden 155

Kennwortposition 151

Kennwortspeicher 151

Klassische Zurückschreibung (Standardzurückschreibung) 271

Knoten

- Typ für Abfrage angeben 624

Knotenname 58

Knotenname (Feld) 275

Knowledge Center xiv

Komprimierungs- und Verschlüsselungsverarbeitung

- Exclude-Optionen 479
- Sicherung 479
- von der Sicherung ausschließen 479

Komprimierungsverarbeitung

- Dateien einschließen 473
- Exclude-Optionen 479
- von der Sicherung ausschließen 479

Konfiguration

- Client-Scheduler 69
- erforderliche Tasks 53
- optionale Tasks 53
- vom Clientakzeptor verwalteter Scheduler 70

Konfiguration des Clients für die Datendeduplizierung 94

Konfigurieren des Web-Clients 68

Kopienart, Attribut 312

Kopiengruppen 310

- Archivierung 310
- Sicherung 310

Kopiengruppenname, Attribut 312

Kopienhäufigkeit, Attribut 312

Kopienmodus, Parameter für

- absolut 314
- geändert 314

Kopiennummerierung, Attribut 313

Kopienziel, Attribut 315

Kundendienst und technische Unterstützung 163

L

LAN-freie Datenversetzung 429

- Datenfernverarbeitung aktivieren 495, 497
- Shared Memory-Anschluss für 496

LAN-gestützte Imagesicherung

- Momentaufnahmeimagesicherung 702

LAN-unabhängige Datenversetzung

- Datenfernverarbeitung aktivieren 169
- Optionen 170

Voraussetzungen 170

lanfreecommmethod (Option) 495

lanfreeshmport (Option) 496

lanfreessl (Option) 498

lanfreetcpport (Option) 497

lanfreetcpserveraddress (Option) 499

LANG, Umgebungsvariable

- Spracheinstellung definieren 63

latest (Option) 500

Leistung

- Geschwindigkeit von Sicherungen, Zurückschreibungen, Archivierungen und Abrufen verbessern 325
- Transaktionsoptionen 344
- Transaktionsverarbeitung 623

Linux Logical Volume Manager

- Momentaufnahmeimagesicherung von Datenträgern 206

Linux on Power Systems (Big Endian), API

- Installation 25

Linux on Power Systems (Little Endian), Client

- Deinstallation 21
- Installation 18

- Linux on Power Systems-Client
 - Clientkomponenten 5
 - Übertragungsmethoden 6
- Linux on Power Systems-Hardwarevoraussetzungen 6
- Linux on Power Systems-Komponenten
 - installierbar 5
- Linux on Power Systems-Plattenspeicherplatz 6
- Linux on Power Systems-Softwarevoraussetzungen 6
- Linux on Power Systems-Systemvoraussetzungen 6
- Linux on System z-Client
 - Clientkomponenten 7
 - Deinstallation 41
 - Installation 38
 - Übertragungsmethoden 7
- Linux on System z-Komponenten
 - installierbar 7
- Linux System z, Hardwarevoraussetzungen 7
- Linux System z, Plattenspeicherplatz 7
- Linux System z, Softwarevoraussetzungen 7
- Linux System z, Systemvoraussetzungen 7
- Linux x86_64-Client
 - Clientkomponenten 6
 - Deinstallation 32, 37
 - Installation 29
 - Übertragungsmethoden 7
- Linux x86_64-Hardwarevoraussetzungen 7
- Linux x86_64-Komponenten
 - installierbar 6
- Linux x86_64-Plattenspeicherplatz 7
- Linux x86_64-Softwarevoraussetzungen 7
- Linux x86_64-Systemvoraussetzungen 7
- localbackupset (Option) 500
- Logischer Datenträger
 - Imagesicherung 206
 - Zurückschreibung 248, 258
- Lokale Momentaufnahme
 - lokale Momentaufnahme einem Serverdateibereich zuordnen 206
- Lokaler Sicherungssatz
 - GUI für lokales Zurückschreiben aktivieren 250
- loop (Befehl) 739
- Löschen
 - Dateibereich 199, 277
 - einzelne Archive aus dem Dateibereich des Servers 284, 721
 - einzelne Sicherungen aus dem Dateibereich des Servers 722
 - NAS- oder Clientobjekte 374
- LVM
 - Anwendung nach dem Starten von LVM aktivieren 533
 - Anwendung vor dem Starten von LVM in den Wartemodus versetzen 540

M

- Mac OS X, Plattenspeicherplatz 8
- Mac OS X-Client
 - Clientkomponenten 8
 - Installation 43
 - Installationsschritte 43
 - Übertragungsmethoden 8
- Mac OS X-Hardwarevoraussetzungen 8
- Mac OS X-Komponenten
 - installierbar 8
- Mac OS X-Softwarevoraussetzungen 8
- Mac OS X-Systemvoraussetzungen 8

- Macintosh-Client
 - Installationsvoraussetzungen 8
 - Umgebungsbedingungen 8
- macro (Befehl) 741
- makesparsefile (Option) 501
- managedservices (Option) 502
- Maßnahmen der Speicherverwaltung 309
- Maßnahmendomänen
 - Standardmaßnahmendomäne 309
- Maßnahmengruppen
 - aktive Maßnahmengruppe 309
- maxcmdretries (Option) 504
- mbobjrefreshtresh 505
- mbpctrefreshtresh 506
- memoryefficientbackup (Option) 507
- Migration
 - Web-Client 1
 - Web-Client-Sprachdateien 1
- Migration der Dateibereiche auf Unicode 181
- Migration von Clients für Sichern/Archivieren durchführen 1
- Mit Mehrfachsitzungen 235
- mode (Option) 509
- Modus
 - interaktiv (loop) 687
 - Stapelbetrieb 686
- Modus (Parameter) 312
- Momentaufnahmedifferenz 119, 581
 - mit HTTPS 190
- Momentaufnahmedifferenzsicherung
 - mit HTTPS 190
- Momentaufnahmedifferenzsicherung ausführen
 - mit HTTPS 191
- Momentaufnahmedifferenzsicherung mit HTTPS-Verbindung 588
- Momentaufnahmedifferenzteilsicherung 581
- Momentaufnahmen
 - Konfiguration 118
- monitor (Option) 512
- monitor process (Befehl) 742
- myreplicationserver (Option) 513

N

- Nachrichten
 - anzeigen 628
 - keine Nachrichtenanzeige 544
- NAS
 - Dateibereiche löschen 199, 277, 727
 - Dateisysteme sichern 219
 - Dateisysteme zurückschreiben 264, 789
 - query node (Befehl) 762
 - restore NAS (Befehl) 789
 - Verwaltungsklasse für Dateisysteme zuordnen 473
 - vollständige oder differenzielle Sicherung angeben 509
- NAS-Dateiserver
 - Dateibereiche löschen 199, 277
- NAS-Dateisysteme sichern
 - Befehlszeile 222
 - Client für Sichern/Archivieren
 - GUI 221
- NAS sichern
 - mit DSM_DIR auf Plug-In-Bibliothek zeigen 64
- nasnodename (Option) 515
- NetApp-Dateiserver 121
- Network-Attached Storage (NAS)
 - angeben, ob für jede Dateisystemsicherung Inhaltsverzeichnisangaben gesichert werden sollen 619

- Network-Attached Storage (NAS) *(Forts.)*
 - Dateibereiche auf Server anzeigen 754
 - Dateibereiche löschen 727
 - Dateien von der Sicherung ausschließen 438
 - Dateisysteme sichern 708
 - Dateisysteme zurückschreiben 264, 789
 - für Abfrage angeben 624
 - Knoten anzeigen, für die Admin-ID Berechtigung hat 762
 - Knotennamen für Operationen angeben 515
 - Sicherungs- oder Zurückschreibungsoperationen überwachen 512
 - Sicherungs- und Zurückschreibungsprozesse abbrechen 719, 742
 - zugehörige Dateisystemimages abfragen 748
- Network Data Management Protocol (NDMP) 10
- Network File System (NFS)
 - Dateisysteme sichern 224
- Neuerungen für den Client für Sichern/Archivieren Version 8.1.6 xvii
- NFS
 - absoluter Mount 243
 - bedingter Mount 243
 - Dateisysteme sichern 224
 - virtuelle Mountpunkte 239
- nfstimeout (Option) 243, 516
- NLSPATH, Umgebungsvariable
 - Hilfemenüs im Browser in der gewünschten Sprache anzeigen 63
- nodename (Option) 517
- nojournal (Option) 519
- noprompt (Option) 519
- nrtablepath (Option) 520
- numberformat
 - angeben 521
- numberformat (Option) 521

O

- Offene Dateien sichern 244
- Offene Registrierung
 - Berechtigungen 129
 - verwenden 129
- Onlinehilfe
 - anzeigen 163
 - Kundendienst und technische Unterstützung 163
 - Onlineforum 163
- optfile (Option) 523
- Optionen 600
 - absolute 355
 - afmskipuncachedfiles 356
 - allgemeine Regeln für die Eingabe mit Befehlen 347
 - Archivierung, Zusammenfassung 326
 - archmc 357
 - archsmlinkasfile 358
 - asnodename 359
 - auditlogging 361
 - auditlogname 363
 - ausschließen
 - Platzhalterzeichen 136
 - autodeploy 365
 - autofsrename 366
 - automount 368
 - backmc 369
 - backupsetname 370
 - basesnapshotname 371
 - Befehlsverarbeitung, Zusammenfassung 343
 - Berechtigungsoptionen 343

- Optionen *(Forts.)*
 - cadlistenonport 372
 - changingretries 373
 - class 374
 - collocatebyfilespec 375
 - commmethod 376
 - commrestartduration 378
 - commrestartinterval 378
 - compressalways 379
 - compression 380
 - console 382
 - createnewbase 383
 - CSV-Datei 385
 - datacenter 388
 - datastore 389
 - dateformat 389
 - dedupcachepath 393
 - dedupcachesize 394
 - deduplication 394
 - defaultserver 396
 - deletefiles 397
 - description 397
 - detail 398
 - Diagnose 346
 - diffsnapshot 400
 - diffsnapshotname 401
 - dirmc 402
 - dironly 403
 - disablenqr 404
 - diskbuffsize 405
 - diskcachelocation 406
 - domain 407
 - domain.image 412
 - domain.nas 413
 - domain.vmfull 414
 - dontload 421
 - dynamicimage 423
 - efsdecrypt 424
 - enablearchiveretentionprotection 425
 - enablededupcache 426
 - enableinstrumentation 427
 - enablelanfree 429
 - encryptiontype 173, 431
 - encryptkey
 - encryptkey=generate 432
 - encryptkey=prompt 432
 - encryptkey=save 432
 - errorlogmax 434
 - errorlogname 435
 - errorlogretention 436
 - exclude
 - exclude.archive 131, 438
 - exclude.attribute.symmlink 131, 438
 - exclude.backup 131, 438
 - exclude.compression 131, 438
 - exclude.dir 131, 438
 - exclude.encrypt 438
 - exclude.file 131, 438
 - exclude.file.backup 131, 438
 - exclude.fs 131, 438
 - exclude.fs.nas 438
 - exclude.image 131, 438
 - exclude.image 131, 438
 - Platzhalterzeichen 137
 - exclude.dedup 438
 - Exclude-Optionen für virtuelle Maschinen 443
 - EXCLUDE.VMDISK 443
 - EXCLUDE.VMLOCALSNAPSHOT 445

Optionen (*Forts.*)

- fbbranch 446
- fbclient 447
- fbpolicyname 448
- fbreposlocation 450
- fbserver 451
- fbvolumename 452
- filelist 453
- filename 456
- filesonly 457
- followsymbolic 458
- forcefailover 460
- Format, Zusammenfassung 342
- Format und Sprache, Zusammenfassung 342
- fromdate 461
- fromnode 461
- fromowner 462
- fromtime 463
- für Zurückschreiben und Abrufen, Zusammenfassung 337
- groupname 464
- host 464
- httpport 465
- ieobjtype 467
- ifnewer 468
- imagegapsize 469
- imagetofile 470
- in Befehlen angeben 346
- inactive 471
- includ 471
- include
 - Platzhalterzeichen 136, 137
- include.archive 473
- include.attribute.sym link 473
- include.backup 473
- include.compression 473
- include.encrypt 473
- include.file 473
- include.fs.nas 473
- include.image 473
- Include-Optionen für virtuelle Maschinen 480
- include.vm 481
- INCLUDE.VMDISK 482
- INCLUDE.VMLOCALSNAPSHOT 484
- include.vmsnapshotattempts 485
- include.vmtsmvss 488
- incrbydate 490
- incremental 492
- instrlogmax 492
- instrlogname 493
- lanfreecomm method 495
- lanfreeshmport 325, 496
- lanfreessl 498
- lanfreetcpport 497
- lanfreetcpserveraddress 499
- latest 500
- localbackupset 500
- makesparsefile 501
- manageservices 502
- maxcmdretries 504
- mbobjrefreshthresh 505
- mbpctrefreshthresh 506
- memoryefficientbackup 507
- mode 509
- monitor 512
- myreplicationserver 513
- nasnodename 515
- nfstimeout 516

Optionen (*Forts.*)

- nodename 517
- nojourn al 519
- noprompt 519
- nrtablepath 520
- numberformat 521
- optfile 523
- password 524
- passwordaccess 526
- passworddir 528
- pick 528
- pitdate 529
- pittime 530
- postnschedulecmd 531
- postschedulecmd 531
- postsnapshotcmd 533
- prenschedulecmd 534
- preschedulecmd 534
- preservelastaccessdate 536
- preservepath 537
- presnapshotcmd 540
- querschedperiod 541
- quersummary 542
- quiet 544
- quotesareliteral 544
- Reihenfolge der Verarbeitung (Vorrangstellung) 346
- removeoperandlimit 546
- replace 547
- replserverguid 548
- replservername 550
- replsslport 552
- repltcpport 554
- repltcpserveraddress 556
- resourceutilization 557
- retryperiod 560
- revokeremoteaccess 561
- schedcmddisabled 562, 563
- schedcmduser (nur serverdefiniert) 302
- schedgroup 564
- schedlogmax 565
- schedlogname 567
- schedlogretention 568
- schedmode 570
- schedrestretrdisabled 572
- scrolllines 572
- scrollprompt 573
- servername 574
- sessioninitiation 576
- setwindowtitle 578
- shmport 579
- showmembers 579
- Sicherung
 - Systemstatus ausschließen 438
- Sicherung, Zusammenfassung 326
- skipacl 580
- skipaclupdatecheck 581
- snapdiff 119, 581
- snapdiffchangelogdir 587
- snapdiffhttps 588
- snapshotcachesize 590
- snapshotproviderfs 591
- snapshotproviderimage 592
- snapshotroot 593
- srvoptsetencryptiondisabled 595
- srvprepostscheddisabled 596
- srvprepostsnapdisabled 597
- ssl 598

Optionen (Forts.)

- sslacceptcertfromserv 600
- sslrequired 602
- stagingdirectory 604
- subdir 605
- Systemstatus
 - von der Sicherungsverarbeitung ausschließen 438
- tapeprompt 607
- tcpadminport 609
- tcpbuffsize 610
- tcpcadaddress 610
- tcpclientaddress 611
- tcpclientport 612
- tcpnodelay 613
- tcpport 614
- tcpserveraddress 614
- tcpwindowsize 615
- timeformat 616
- toc 619
- todate 621
- totime 622
- Transaktionsverarbeitung, Zusammenfassung 344
- txnbytelimit 623
- type 624
- Übertragung, Zusammenfassung 324
- updatectime 624
- useexistingbase 625
- usereplicationfailover 626
- v2archive 627
- verbose 628
- verifyimage 629
- virtualfsname 630
- virtualmountpoint 630
- virtualnodename 632
- vmbackupdir 633
- vmbackuplocation 634
- vmbackupmailboxhistory 636
- vmbackuptype 637
- vmchost 637
- vmcpw 638
- vmcuser 640
- vmdatastorethreshold 641
- vmdefaultdvportgroup 643
- vmdefaultdvswitch 644
- vmdefaultnetwork 645
- vmenabletemplatebackups 646
- vmlimitperdatastore 648
- vmlimitperhost 649
- vmmaxbackupsessions 650
- vmmaxparallel 652
- vmmaxparallelrestoresessions 655
- vmmaxparallelrestorevms 656
- vmmaxrestoresessions 654
- vmmc 659
- vmnoprdmdisks 660
- vmnovrdmdisks 661
- vmpreferdagpassive 662
- vmprocessvmwithprdm 664
- vmprocesswithindependent 663
- vmskipctlcompression 665
- vmskipmaxvirtualdisks 666
- vmskipmaxvmdks 667
- vmtagdatamover 668
- vmtagdefaultdatamover 671
- vmtimeout 679
- vmverifyifaction 673
- vmverifyiflatest 675

Optionen (Forts.)

- vmvstorcom 676
- vmvstortransport 678
- Web-Client, Zusammenfassung 345
- webports 680
- wildcardsareliteral 681
- zentrale Zeitplanung, Zusammenfassung 340
- Oracle Solaris-Client
 - Clientkomponenten 9
 - Übertragungsmethoden 9
- Oracle Solaris-Komponenten
 - installierbar 9
- Ordner
 - Übersicht über die Verarbeitung bei der Teilsicherung 183

P

- Parallele Sicherungen 234, 648, 649, 650, 652
- Parameter
 - yes und no, Alternativen 355
- Partielle Teilsicherung
 - Definition 182
 - Teilsicherung nach Datum
 - ausführen 194
- password
 - ändern 820
 - angeben, ob automatisch generiert oder als Benutzereingabeaufforderung definiert werden soll 526
 - definieren 524
 - Verzeichnisposition zum Speichern der verschlüsselten Kennwortdatei angeben 528
- password (Option) 524
- passwordaccess (Option) 526
- passworddir (Option) 528
- pick (Option) 528
- PIHDW, Plug-in 421
- pitdate 529
- pittime (Option) 530
- Planungsprotokoll
 - Aufbewahrungsdauer in Tagen für Einträge angeben und ob bereinigte Einträge gespeichert werden sollen 568
 - Größe steuern 565
 - Pfad und Dateinamen zum Speichern von Planungsprotokollaten angeben 567
- Platte wiederherstellen 277
- Plattenspeicherplatz, AIX 4
- Plattenspeicherplatz, HP-UX Itanium 2 5
- Plattenspeicherplatz, Linux on Power Systems 6
- Plattenspeicherplatz, Linux System z 7
- Plattenspeicherplatz, Linux x86_64 7
- Plattenspeicherplatz, Mac OS X 8
- Plattenspeicherplatz, Solaris 9
- Plattenspeicherplatzvoraussetzungen
 - Client 3
- Platzhalterzeichen
 - Dateien einschließen oder ausschließen 135
 - Dateigruppen einschließen oder ausschließen 136
 - in Befehlen verwenden 245
 - in Dateispezifikationen verwenden 245
 - Laufwerkspezifikation in dsm.opt angeben 136
 - Richtlinien 691
 - zum Ein- oder Ausschließen von Dateigruppen 137
- Plug-In-Bibliothek
 - für Image-/NAS-Sicherung oder -Zurückschreibung 64
- postnschedulecmd (Option) 531
- postsnapshotcmd (Option) 533
- prenschedulecmd (Option) 534

- preschedulecmd (Option) 534
- preservelastaccessdate (Option) 536
- preservepath (Option) 537
- Presnapshotcmd (Option) 540
- preview archive (Befehl) 743
- preview backup (Befehl) 744
- Profileditor
 - Domänen von der Sicherung ausschließen 193
- Protokoll
 - siehe auch* Planungsprotokoll
 - DSM_LOG (Umgebungsvariable) 435, 493, 567
 - errorlogname (Option) 435
 - errorlogretention (Option) 435
 - Fehlerprotokoll bereinigen 434
 - Größe steuern 492
 - instrlogmax (Option) 492
 - intrlogname (Option) 493
 - Pfad und Dateinamen angeben 435, 493, 567, 808
 - schedlogname (Option) 567, 808
 - schedlogretention (Option) 567, 808
 - Web-Client 565
- Protokolle
 - Abschneiden von Anwendungsprotokollen 488
 - dsmsched.log 568
 - dsmsched.pru 568
 - dsmwebcl.log 568
 - dsmwebcl.pru 568

Q

- QFS (Dateisystem)
 - Einschränkungen 174
- query access (Befehl) 745
- query archive (Befehl) 745
- query backup (Befehl) 748
- query backupset (Befehl) 751, 753
- query filespace (Befehl) 754
- query group (Befehl) 756
- query image (Befehl) 758
- query inexpl (Befehl) 760
- query mgmtclass (Befehl) 311, 761
- query node (Befehl) 762
- query options (Befehl) 763
- query restore (Befehl) 764
- query schedule
 - erweitert 299
- query schedule (Befehl) 765
- query schedule (Befehl), erweitert 765
- query session (Befehl) 765
- query systeminfo (Befehl) 767
 - Verschlüsselungsverarbeitung 767
- query VM (Befehl) 768
- querschedperiod (Option) 541
- querysummary (Option) 542
- quiet (Option) 544
- quotesareliteral (Option) 544

R

- Registrieren
 - Client auf Server 128
 - geschlossene Registrierung 128
 - offene Registrierung 128, 129
- removeoperandlimit (Option) 546
- replace (Option) 547
- replserverguid (Option) 548

- replservername (Option) 550
- replsslport (Option) 552
- repltcpport (Option) 554
- repltcpserveraddress (Option) 556
- resourceutilization (Option) 557
- restart restore (Befehl) 771
 - unterbrochene Zurückschreibung erneut starten 274
- restore 786
 - aktive und inaktive Objekte anzeigen 471
 - aktive Version 267
 - anderen Benutzern Berechtigung erteilen 274
 - auf andere Workstation 632
 - aus nicht Unicode-fähigen Dateibereichen 776
 - basierend auf Datum und Zeit der Sicherung 461, 463
 - Benutzer ohne Rootberechtigung unter RHEL 5 278
 - Dateien, die zu einem anderen Knoten gehören 275
 - Dateien auf eine andere Workstation 276
 - Dateien für einen anderen Benutzer 462
 - Dateien für einen anderen Knoten 461
 - Dateien und Verzeichnisse 268
 - Dateiliste 453
 - Dateiliste sortieren 162
 - Daten über die Befehlszeile 269
 - EFS (Encrypted File Systems - Verschlüsselte Dateisysteme) 262
 - Eingabeaufforderung vor dem Überschreiben vorhandener Dateien 547
 - Geschwindigkeit mit Shared Memory verbessern 325
 - Gruppe
 - Befehl 784
 - GUI, aktive und inaktive Versionen anzeigen 162
 - Image 248
 - Feststellung von defekten Sektoren auf Zieldatenträger
 - aktivieren 629
 - Hinweise 786
 - in eine Datei 470
 - mit DSM_DIR auf Plug-In-Bibliothek zeigen 64
 - mit Tool chkdsk reparieren 248
 - mit Tool fsck reparieren 248
 - Image, Bestätigungsaufforderung unterdrücken 519
 - inaktive Version 267
 - klassisch (auch als Standardzurückschreibung bekannt) 271
 - Liste der Sicherungsversionen erstellen 528
 - logischer Datenträger 248
 - lokalen Sicherungssatz mit GUI 250
 - mit Befehlen 274
 - mit Tool fsck reparieren 786
- NAS
 - mit DSM_DIR auf Plug-In-Bibliothek zeigen 64
- NAS-Dateisysteme 264
- neueste Sicherungsversion 500
- nur Verzeichnisse verarbeiten (keine Dateien) 403
- ohne Abfrage 271
- Platte 277
- primäre Tasks 247
- SELinux aktivieren 278
- Sicherungssatz
 - unterstützte Bandeneinheiten 777, 781
- Sicherungssätze
 - Übersicht 250
- Standard (auch als klassische Zurückschreibung bekannt) 271
- Symbolische Verbindungen
 - UNIX- und Linux-Einschränkungen 771
- Übersicht 247
- unformatierter logischer Datenträger 248

- restore (*Forts.*)
 - Verarbeitungsstatusfenster 268
 - von austauschbaren Datenträgern
 - Übersicht 250
 - vorhandene Datei durch letzte Sicherung ersetzen 468
 - während der Übernahme 257
 - Web-Clientsitzung starten 158
 - wiederanlauffähig 271
 - zeitpunktgesteuerte Sicherungen definieren 529, 530
 - Zusammenfassung der Optionen 337
- restore (Befehl) 771
 - umfangreiche Operationen ausführen 270
- restore backupset (Befehl) 777, 781
- restore backupset (Befehl), Hinweise 253, 780
- restore group (Befehl) 784
- restore image
 - btrfs 216
- restore image (Befehl) 786
- restore NAS (Befehl) 789
- restore vm (Befehl) 791
 - Voranzeige 791, 803
- retrieve (Befehl) 805
- retryperiod (Option) 560
- revokeremoteaccess (Option) 561
- Root
 - Rootzugriff anfordern 53
- Root-Tasks
 - Einrichtung 58
 - Standardclientbenutzeroptionsdatei erstellen 60
- Rückkehrcodes für Operationen 307

S

- SAN
 - Sicherungssätze zurückschreiben 781
- Schätzfunktion 193
- schedcmddisabled (Option) 562, 563
- schedcmduser, Option (nur serverdefiniert) 302
- schedgroup (Option) 564
- schedlogmax (Option) 565
- schedlogname (Option) 567
- schedlogretention (Option) 568
- schedmode (Option) 570
- schedrestretrdisabled (Option) 572
- schedule (Befehl) 808
- Scheduler
 - Anzahl Minuten zwischen Versuchen, geplante Befehle zu verarbeiten 560
 - Anzahl Stunden zwischen Kontakten zum Server für geplante Arbeit 541
 - Anzeigen geplanter Arbeit 299, 301
 - Ausführung von Zurückschreibungs- oder Abrufoperationen inaktivieren 572
 - Einleitung von Sitzungen über die Firewall durch Server oder Client 576
 - Ereignisprotokollierung 301
 - Konfiguration 69
 - Modus 'polling' (Clientsendeaufruf) oder 'prompted' (Servergesteuerte Ausführung) 570
 - Optionen für 302
 - Speicheraufbewahrungszeitraum nach geplanten Sicherungen beseitigen 502
 - starten 72
 - vom Clientakzeptordämon verwaltet 502
- Schedulervergleich
 - Clientakzeptor im Vergleich zum traditionellen Scheduler 69

- scrolllines (Option) 572
- scrollprompt (Option) 573
- Secure Sockets Layer (SSL)
 - Kommunikation einrichten mit 77
- selective (Befehl) 810
- selektive Sicherung 593
- Selektive Sicherung 810
 - Befehlszeile 194
 - Clientbefehlszeile 194
 - lokale Momentaufnahme Serverdateibereich zuordnen 206
 - mithilfe der Client-Java-GUI 193
 - symbolische Verbindungen 240
 - Übersicht 182, 192, 194
- Server
 - Datenfernverarbeitung durch Firewall aufbauen 74
 - identifizieren, um eine Zeilengruppe mit Optionen zu beginnen 574
 - Kommunikation einrichten mit 58
 - Kommunikation mit 58
 - Kommunikation mit Secure Sockets Layer (SSL) einrichten 77
 - Name des Servers angeben, der für Services kontaktiert werden soll 574
 - TCP/IP-Adresse des IBM Spectrum Protect-Servers 614
 - TCP/IP-Anschlussadresse 614
- servername (Option) 574
- Serveroptionen
 - Sslfipsmode 601
- sessioninitiation (Option) 576
- set access (Befehl) 814
 - Berechtigung zum Zurückschreiben/Abrufen 274
- set event (Befehl) 817
- set netappsvm 121
- set password (Befehl) 820
- set vmtags (Befehl) 826
- setwindowtitle 578
- Shared Memory, Übertragungsmethode
 - Optionen 325
- Shell-Scripts
 - Befehle verwenden 307
 - Rückkehrcodes 307
- shimport (Option) 579
- showmembers (Option) 579
- Sicherung 192
 - ACL-Verarbeitung überspringen 580
 - Anzahl Versuche zum Sichern offener Dateien 373
 - Aufbewahrungszeitraum 310
 - Benutzerzugriff abfragen 745
 - btrfs 216
 - EFS (Encrypted File Systems - Verschlüsselte Dateisysteme) 228
 - eine Serversitzung pro Dateispezifikation 375
 - gemeinsam genutzte Daten auf mehreren Clients unter einem einzigen Knotennamen 359
 - Geschwindigkeit mit Shared Memory verbessern 325
- Image 206
 - Clientdomäne 412
 - mit Teilsicherung 706
- Image: statisch, dynamisch, Momentaufnahme 206
- in Parallelsitzungen 234
- incremental
 - lokale Momentaufnahme Serverdateibereich zuordnen 739
- Kopienmodus 314
- Mehrfachsitzung, Dateien zusammenhängend an den Server senden 375
- Network-Attached Storage (NAS) 708

- Sicherung (*Forts.*)
 - neue oder geänderte Dateien 183
 - nur Verzeichnisse verarbeiten (keine Dateien) 403
 - parallel 648, 649, 650, 652
 - primäre Tasks 167
 - selektiv
 - lokale Momentaufnahme Serverdateibereich zuordnen 814
 - selektive Sicherung über Clientbefehlszeile 194
 - symbolische Verbindungen 240
 - Teilsicherung nach Datum
 - Clientbefehlszeile 194
 - Übersicht 167
 - Verarbeitungsstatus anzeigen 235
 - VM-Schablonen 646
 - Web-Clientsitzung starten 158
 - Zusammenfassung der Optionen 326
- Sicherung, maximale Dateigröße 179
- Sicherung mit Clientknotenproxy
 - Agentenknoten 200
 - Zielknoten 200
- Sicherung mit dem Clientknoten-Proxy
 - Übersicht 200
- Sicherungsdateien
 - Verwaltungsklasse zuordnen 316
- Sicherungskopiengruppe 168, 310
 - Attribute 311
- Sicherungsplanung 167
- Sicherungssatz
 - GUI für lokales Zurückschreiben aktivieren 250, 500
 - in einer SAN-Umgebung zurückschreiben 781
 - Zurückschreibung 247, 250
- Sicherungssätze
 - Hinweise zum Zurückschreiben 253, 780
- Sicherungsservices automatisieren
 - Anzeigen geplanter Arbeit 299, 301
 - Befehle nach Sicherung verarbeiten 531
 - Befehle vor Sicherung verarbeiten 534
 - Optionen für 302
 - Starten des Client-Schedulers 72
- Sitzungsinformationen anzeigen 765
- skipacl (Option) 580
- skipaclupdatecheck (Option) 581
- snapdiff (Option) 119, 581
- snapdiffchangelogdir (Option) 587
- snapdiffhttps (Option) 588
- snapshotcachesize (Option) 590
- snapshotproviderfs (Option) 591
- snapshotproviderimage (Option) 592
- snapshotroot (Option) 593
- Softwareaktualisierungen 51
- Softwarevoraussetzungen, AIX 4
- Softwarevoraussetzungen, HP-UX Itanium 2 5
- Softwarevoraussetzungen, Linux on Power Systems 6
- Softwarevoraussetzungen, Linux System z 7
- Softwarevoraussetzungen, Linux x86/x86_64 7
- Softwarevoraussetzungen, Mac OS X 8
- Softwarevoraussetzungen, Solaris 9
- Solaris, Plattenspeicherplatz 9
- Solaris, Systemvoraussetzungen 9
- Solaris-Hardwarevoraussetzungen 9
- Solaris-Softwarevoraussetzungen 9
- Solaris SPARC-API
 - in Solaris Zones installieren 49
 - Installation 49
- Solaris x86_64-Client
 - in Solaris Zones installieren 45
- Solaris x86_64-Client (*Forts.*)
 - Installation 45
- Solaris Zones 192
- Speicher
 - Anzeigen wiederanlauffähiger Zurückschreibungssitzungen 764
 - bei begrenztem Speicher optimieren 172
- Speicheragent
 - für LAN-freie Datenversetzung verwenden 429
 - für LAN-unabhängige Datenversetzung 169
- Speicherbereichsnetz
 - für LAN-freie Datenversetzung verwenden 429
 - für LAN-unabhängige Datenversetzung 169
 - Sicherungssätze zurückschreiben 429, 781
- Speicherpools
 - GPFS 259
- Speicherverwaltungsmaßnahmen 309
 - Einschluss-/Ausschlussliste 310
 - in der GUI des Clients für Sichern/Archivieren anzeigen 239
 - Kopiengruppen 310
 - Maßnahmendomänen
 - Standard 309
 - Maßnahmengruppen
 - Aktive Maßnahmengruppe 309
 - Standardverwaltungsklasse 309
 - Verwaltungsklassen 310
 - Verwaltungsklassen Dateien zuordnen 239
- Spezielle Dateisysteme 174, 239
- Spracheinstellung
 - unterstützte 63
- Spracheinstellung definieren 63
- srvoptsetencryptiondisabled (Option) 595
- srvprepostscheddisabled (Option) 596
- srvprepostsnapdisabled (Option) 597
- ssl (Option) 598
- SSL (Secure Socket Layer)
 - Kommunikation einrichten mit 77, 80
- sslacceptcertfromserv (Option) 600
- Sslfipsmode (Option) 601
- sslrequired (Option) 602
- stagingdirectory (Option) 604
- Standardclientbenutzeroptionsdatei
 - Beispiel 60
 - erstellen und ändern 60
- Standarddomäne
 - Domänen von der Sicherung ausschließen 194, 407
- Standardeinheit zum Versetzen von Daten 671
- Standardmaßnahmendomäne 309
- Standardverwaltungsklasse 309
 - Daten deduplizieren (Attribut) 315
 - einzigste Version aufbewahren 313
 - Extraversionen aufbewahren 313
 - Kopienart 312
 - Kopiengruppenname 312
 - Kopienhäufigkeit 312
 - Kopienmodus
 - absolut 314
 - geändert 314
 - Kopiennummerierung 313
 - Kopienziel 315
 - Standardwerte 311
 - Version aufbewahren 315
 - Versionen bestehender Daten 312
 - Versionen gelöschter Daten
 - aktive Versionen 313
 - inaktive Versionen 313

- Standardzurückschreibung (klassische Zurückschreibung) 271
- Stapelbetrieb 686
- Stapelmodus
 - Starten einer Sitzung 155
- Starten
 - automatisch 160
 - Übersicht 1
- Starten des Client-Schedulers beim Systemstart 297
- Starten einer Sitzung
 - interaktiver Modus 156
 - Stapelmodus 155
- Statisch (Durchnummerierung) 313
- Steuerdateien 633
- subdir (Option) 605
- Swing-Browser
 - zum Ausführen des Web-Clients erforderlich 158
- Symbolische Verbindungen
 - archivieren und abrufen 285
 - Exclude-Optionen 478
 - Sicherung 240, 478
 - Verarbeitung 478
 - von der Sicherung ausschließen 478
 - Zurückschreibung 458
 - UNIX- und Linux-Einschränkungen 771
- Symbolische Verbindungen und Aliasnamen
 - Exclude-Optionen 442, 478
 - Sicherung 442, 478
 - Verarbeitung 442, 478
 - von der Sicherung ausschließen 442, 478
- Syntaxdiagramm
 - erforderliche Auswahlmöglichkeiten xiv
 - lesen xiv
 - Wiederholungswerte xiv
- Systemdateien
 - ausschließen 134
- Systeminformationen
 - zusammenstellen 382, 456
- Systemstatus
 - aktive und inaktive Objekte anzeigen 471
- Systemvoraussetzungen, AIX 4
- Systemvoraussetzungen, HP-UX Itanium 2 5
- Systemvoraussetzungen, Linux on Power Systems 6
- Systemvoraussetzungen, Linux System z 7
- Systemvoraussetzungen, Linux x86_64 7
- Systemvoraussetzungen, Mac OS X 8
- Systemvoraussetzungen, Solaris 9

T

- tapeprompt (Option) 607
- Tasks
 - geschlossene Registrierung 128
 - grafische Benutzerschnittstelle, Verwaltungsklasse überschreiben 317
 - Kennwort ändern 160
 - offene Registrierung 128
 - Root 53
 - Sitzungen beenden 160
 - Verwaltungsklassen anzeigen 311
 - Verwaltungsklassen zu Verzeichnissen zuordnen 317
- Tastatur 843
- TCP/IP-Übertragungsmethode
 - Optionen 324
- tcpadminport (Option) 609
- tcpbuffsize (Option) 610
- tcpaddress (Option) 610
- tcpclientaddress (Option) 611

- tcpclientport (Option) 612
- tcpnodelay (Option) 613
- tcpserveraddress (Option) 614
- tcpwindowsize (Option) 615
- Teilsicherung
 - ACL-Aktualisierungsüberprüfung überspringen 581
 - Befehlszeile 194
 - Beschreibung 183
 - Clientbefehlszeile 194
 - Clientdomäne 407
 - Dateiliste verarbeiten 453
 - GPFS, Clusterumgebung mit mehreren Knoten 174, 407
 - lokale Momentaufnahme Serverdateibereich zuordnen 593
 - mit Imagesicherung 211, 706
 - mithilfe der Client-Java-GUI 193
 - nach Datum 194
 - neue und geänderte Dateien 183
 - neue und geänderte Dateien mit Änderungsdatum später als letzte Sicherung 490
 - neue und geänderte Dateien mit Änderungsdatum später als letzte Sicherung sichern 490
 - Ordner
 - Verarbeitungsübersicht 183
 - Ordner, Übersicht 183
 - Speicher optimieren 172
 - Speichersparalgorithmus 507
 - symbolische Verbindungen 240
 - Übersicht 182
 - Verzeichnisse
 - Verarbeitungsübersicht 183
 - Verzeichnisse, Verarbeitungsübersicht 183
- Teilsicherung, lokale Momentaufnahme Serverdateibereich zuordnen 206
- Teilsicherung erzwingen 355
- Teilsicherung nach Datum 187
 - Befehlszeile 194
 - Beschreibung 187
 - Clientbefehlszeile 194
 - mithilfe der Client-Java-GUI 193
 - Übersicht 182
 - Vergleich mit vollständiger Teilsicherung 188
 - Vergleich mit vollständiger Teilsicherung und journalbasierter Sicherung 188
 - Verwendung 188
 - Verwendung mit Imagesicherung 212
 - Verzeichnisse
 - Verarbeitungsübersicht 187
- timeformat (Option) 616
- Tivoli Storage Manager FastBack, Installationsvoraussetzungen 10
- Tivoli Storage Manager FastBack-Datensicherung 235
- Tivoli Storage Manager FastBack-Datenzurückschreibung 235
- Tivoli Storage Manager FastBack-Konfiguration 106
- toc (Option) 619
- todate (Option) 621
- totime (Option) 622
- Traditionelle vollständige Teilsicherung 185
- Traditionelle vollständige Teilsicherung ausführen 737
- Transaktionsverarbeitung
 - txnbytelimit (Option) 623
 - Zusammenfassung der Optionen 344
- TSM.sth (Datei) 432
- tsmjbbd.ini
 - Konfiguration 83
- txnbytelimit (Option) 623
- type (Option) 624

U

Übernahme

- Abruf 257
- andere Komponenten 101
- Client 98
- Clientkonfiguration 102
- Einschränkungen 100
- inaktivieren 105
- Konfiguration und Verwendung 98
- Replikationsstatus bestimmen 104
- Voraussetzungen 99
- Zurückschreibung 257

Übersicht, Konfiguration des Web-Clients 67

Übertragung

- mit Secure Sockets Layer (SSL) einrichten 77
- über Firewall 74

Übertragungsmethoden

- installierbare Software 5, 6, 7, 8, 9

Shared Memory

- AIX-Client 4
- HP-UX Itanium 2-API 5
- Linux on System z-Client 7
- Linux x86_64-Client 7
- Oracle Solaris-Client 9

TCP/IP

- AIX-Client 4
- HP-UX Itanium 2-API 5
- Linux on Power Systems-Client 6
- Linux on System z-Client 7
- Linux x86_64-Client 7
- Mac OS X-Client 8
- Oracle Solaris-Client 9

Zusammenfassung 324

Ubuntu Linux on Power Systems (Little Endian), API

- Deinstallation 25
- Installation 22

Ubuntu Linux on Power Systems (Little Endian), Client

- Deinstallation 25
- Installation 22

Ubuntu x86_64-Client

- Installation 34

Umgebungsvariablen

- API definieren 67
- Bourne- und Korn-Shell-Variablen definieren 66
- C-Shell-Umgebungsvariablen definieren 67
- DSM_CONFIG 64
- DSM_DIR 64
- DSM_LOG 64
- LANG 64

Umgebungs Voraussetzungen

- AIX-Client 4
- HP-UX Itanium 2-API 5
- Linux for zSeries-Client 7
- Linux on Power Systems 5
- Linux x86_64-Client 6
- Solaris-Client 9

Unformatierter logischer Datenträger

- Imagesicherung 206
- Zurückschreibung 248

Unicode

- aus nicht Unicode-fähigen Dateibereichen zurückschreiben 776
- Dateibereiche migrieren auf 181
- Nicht-Unicode-Dateibereiche in Unicode-fähige Dateibereiche umbenennen 366, 810

UNIX

- Dateisysteme, ACL-Unterstützung 174

UNIX (Forts.)

- Standardzugriffsberechtigungen sichern 285

UNIX und Linux

- Clusterumgebung 108
 - IBM Spectrum Protect installieren 108
- Einschränkungen
 - symbolische Verbindungen zurückschreiben 771

Unterstützte Spracheinstellungen 63

Unterstützung

- Systeminformationen zusammenstellen für 382, 456, 767

Unterstützung für Sicherungen mit dem Clientknoten-Proxy konfigurieren 200

Unterverzeichnisse

- Archivierung 282
- für Sicherung einschließen 194

updatectime (Option) 624

Upgrade des Clients für Sichern/Archivieren von älteren Versionen des Produkts durchführen 1

Upgrade von Clients für Sichern/Archivieren durchführen 1

useexistingbase (Option) 625

usereplicationfailover (Option) 626

V

v2archive (Option) 627

Verarbeitung symbolischer Verbindungen 478

Verarbeitung von Aliasnamen 478

Verarbeitung von symbolischen Verbindungen und Aliasnamen 442

Verarbeitung von unten nach oben

- Einschluss-/Ausschlussliste 141
- Einschluss-/Ausschlussoptionsdatei 141

Verarbeitungsoptionen

- Berechtigung 343
- Diagnose 346
- Fehlerverarbeitung 344
- Format 342
- Format und Sprache 342
- für Zurückschreiben und Abrufen 337
- in Befehlen angeben 346
- Sicherung und Archivierung 326
- Transaktionsverarbeitung 344
- Übersicht 323
- Übertragung 324
- verwenden 145, 148, 323
- Web-Client 345
- zentrale Zeitplanung 340

Verarbeitungszeit

- schätzen 193

verbose (Option) 628

Vergleich: vollständige Teilsicherung und Teilsicherung nach Datum 188

verifyimage (Option) 629

Veröffentlichungen xiv

Verschlüsselung

- Chiffrierschlüsselkennwort sichern 432
- mehrere Clients unter einem einzigen Knotennamen 359
- von Dateidaten 173

Verschlüsselung, Hinweise 56

Verschlüsselung für berechtigte Benutzer aktivieren 56

Verschlüsselungsverarbeitung

- Dateien ausschließen 438
- Dateien einschließen 473
- query systeminfo (Befehl) 767
- verfügbare Verschlüsselungsverfahren 173
- Version aufbewahren, Attribut 315

- Versionsdaten
 - Attribut 312, 313
 - Parameter 313
- Verwaltungsclient
 - gesicherte Sitzungen innerhalb eines privaten Netzes zulassen 609
- Verwaltungsklasse
 - zuordnen 239
- Verwaltungsklassen
 - an Dateien binden 318
 - anzeigen 311
 - Archivierungsdateien binden an 282
 - Dateien zuordnen 316
 - für Dateien auswählen 315
 - Hinweise 315
 - Informationen anzeigen 761
 - mit Option "include" angeben 316
 - Standard 310
 - Standardwert überschreiben 316
 - Verarbeitung 316
 - Verwendung durch IBM Spectrum Protect 172
 - Verwendungsbeispiel 316
 - Verzeichnissen zuordnen 317, 402
 - während der Archivierung überschreiben 317
- Verzeichnisse
 - ausschließen 131
 - Dateien von der Sicherungsverarbeitung ausschließen 438
 - in der Befehlszeile angeben 689
 - Übersicht über die Verarbeitung bei der Teilsicherung 183
 - Verarbeitung bei der Teilsicherung nach Datum 187
 - Verwaltungsklassen zuordnen 402
- virtualfsname (Option) 630
- virtualmountpoint (Option) 630
- virtualnodename (Option) 632
 - auf andere Workstation zurückschreiben oder abrufen 276
- Virtuelle Maschine
 - Exclude-Optionen 443
 - Include-Optionen 480
- Virtuelle VMware-Maschine, Sicherung 233
 - Typen 230
- Virtuellen Mountpunkt definieren 193
- VM 230
- VM-Schablonen in Sicherungen einschließen 646
- vmbakdir (Option) 633
- vmbakuplocation (Option) 634
- vmbakupmailboxhistory 636
- vmbakuptype (Option) 637, 659
- vmchost (Option) 637
- vmcpw (Option) 638
- vmctlmc (Option)
 - Optionen
 - vmctlmc 639
- vmcuser (Option) 640
- vmdatastorethreshold
 - Option 641
- vmdefaultdvportgroup (Option) 643
- vmdefaultdvswitch Option 644
- vmdefaultnetwork (Option) 645
- vmenabletemplatebackups (Option) 646
- vmlimitperdatastore (Option) 648
- vmlimitperhost (Option) 649
- vmmaxbackupsessions (Option) 650
- vmmaxparallel (Option) 652
- vmmaxparallelrestoresessions (Option) 655
- vmmaxparallelrestorevms (Option) 656
- vmmaxrestoresessions (Option) 654
- vmnoprdmdisks 660

- vmnovrdmdisks 661
- vmpreferdagpassive (Option) 662
- vmprocessvmwithprdm 664
- vmprocesswithindependent 663
- vmskipctlcompression (Option) 665
- vmskipmaxvirtualdisks 666
- vmskipmaxvmdks 667
- vmtagdatamover
 - Option 668
- vmtagdefaultdatamover
 - Option 671
- vmtimeout (Option) 679
- vmverifyifaction 673
- vmverifyiflatest 675
- vmvstorcom (Option) 676
- vmvstortransport (Option) 678
- VMware-Tagging
 - als Datenschutzeinstellungen dargestellt 828
 - Tipps zum Konfigurieren von Sicherungsmaßnahmen 840
 - Übersicht 828
 - unterstützte Datenschutztags 829
 - Vererbung 838
- VMware-Tagging-Unterstützung
 - aktivieren 668
- Vollständige Teilsicherung
 - Beschreibung 183
 - Definition 182
 - Vergleich mit journalbasierter Sicherung und Teilsicherung nach Datum 188
 - Vergleich mit Teilsicherung nach Datum 188
 - Verwendung 188
- Voranzeige
 - Einschluss-/Ausschlussliste 140
 - restore vm 791, 803
- vStorage-Sicherungsserver
 - Off-Host-Sicherung 232

W

- Wartemodus, Anwendungen versetzen in 488
- Wartung 365
 - automatische Aktualisierung 2
- Wartungsaktualisierungen herunterladen 51
- Web-Client
 - Administratorzugriff auf den Client, auf dem der Web-Client ausgeführt wird, einschränken 561
 - Datenfernverarbeitung durch Firewall aufbauen 465
 - Einschränkungen für NAS-Dateisysteme 219
 - für Swing-Browser aktivieren 158
 - Konfiguration 68
 - nicht unterstützte Funktionen 167
 - starten 158
 - TCP/IP-Anschlussadresse angeben 465
 - über Firewall verwenden 680
 - Übersicht über die Konfiguration 67
 - unterstützte Browser 158
 - Zusammenfassung der Optionen 345
- webports (Option) 680
- Wiederanlauffähige Zurückschreibung 271
- Wiederanlauffähige Zurückschreibungssitzungen anzeigen 764
- wildcardsareliteral (Option) 681

Z

- Zeilengruppe JournalSettings 85

- Zeitformat
 - angeben 616
- Zeitplanung
 - Clientknoten-Proxy 202
 - GPFS (Dateisystem) 205
 - IBM PowerHA SystemMirror-Cluster 203
 - Sicherung mit Proxy für Clientknoten 200
- Zentrale Zeitplanung
 - Zusammenfassung der Optionen 340
- Zertifizierungsstellen
 - Stammzertifikate 82
 - Zertifizierungsstellen 82
- Zettabyte-Dateisysteme (ZFS) 227
 - Dateisysteme sichern 227
- Zugriff
 - Berechtigungen archivieren 285
- Zugriffssteuerungslisten
 - Berechtigungen, Sicherung 192
 - erweiterte Berechtigungen, Sicherung 192
- Zurückschreibung
 - btrfs 216
 - Image in Datei 258
 - logischer Datenträger 258
 - NAS-Dateisysteme
 - Befehlszeile 266
 - Web-Client 265
 - umfangreiche Operationen ausführen 270
- Zurückschreibung, maximale Dateigröße 179
- Zurückschreibung nach Zeitpunkt 260
 - Imagesicherung 706
 - über die Befehlszeile 260
 - über die GUI 260



Programmnummer: 5725-W98
5725-W99
5725-X15

Gedruckt in Deutschland