IBM Spectrum Protect
Version 8.1.6

Einführung in Datenschutzlösungen

IBM Spectrum Protect
Version 8.1.6

Einführung in Datenschutzlösungen

Anmerkung:
Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen" auf Seite 59 gelesen werden.

Diese Ausgabe bezieht sich auf Version 8, Release 1, Modifikation 6 von IBM Spectrum Protect (Produktnummern 5725-W98, 5725-W99, 5725-X15) und auf alle nachfolgenden Releases und Modifikationen, bis dieser Hinweis in einer Neuausgabe geändert wird.

Inhaltsverzeichnis

Zu dieser Veröffentlichung

Diese Veröffentlichung bietet eine Übersicht über IBM Spectrum Protect-Konzepte und -Datenschutzlösungen, die Best Practices für IBM Spectrum Protect verwenden. Anhand einer Tabelle, die einen Vergleich der Funktionen bereitstellt, können Sie die beste Lösung gemäß den Anforderungen Ihres Unternehmens auswählen.

Zielgruppe

Dieses Handbuch richtet sich an alle Personen, die als Administrator für IBM Spectrum Protect registriert sind. Ein einzelner Administrator kann IBM Spectrum Protect verwalten oder die Zuständigkeit für Verwaltungsaufgaben kann auf mehrere Personen übertragen werden.

Sie sollten mit dem Betriebssystem, unter dem der Server ausgeführt wird, und den Kommunikationsprotokollen vertraut sein, die für die Client/Server-Umgebung erforderlich sind. Außerdem müssen Sie über Kenntnisse in den Speicherverwaltungspraktiken Ihres Unternehmens verfügen. Sie müssen beispielsweise wissen, wie gegenwärtig Workstationdateien gesichert und Speichereinheiten verwendet werden.

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.

Teil 1. IBM Spectrum Protect-Konzepte

IBM Spectrum Protect stellt eine umfassende Datenschutzumgebung bereit.

Kapitel 1. Übersicht über IBM Spectrum Protect

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

Datenschutzkomponenten

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

Server

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

Der Bestand umfasst die folgenden Komponenten:

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

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

Clientsysteme und -anwendungen

Clients sind Anwendungen, virtuelle Maschinen und Systeme, die geschützt werden müssen. Die Clients senden Daten an den Server (siehe Abb. 1 auf Seite 4).

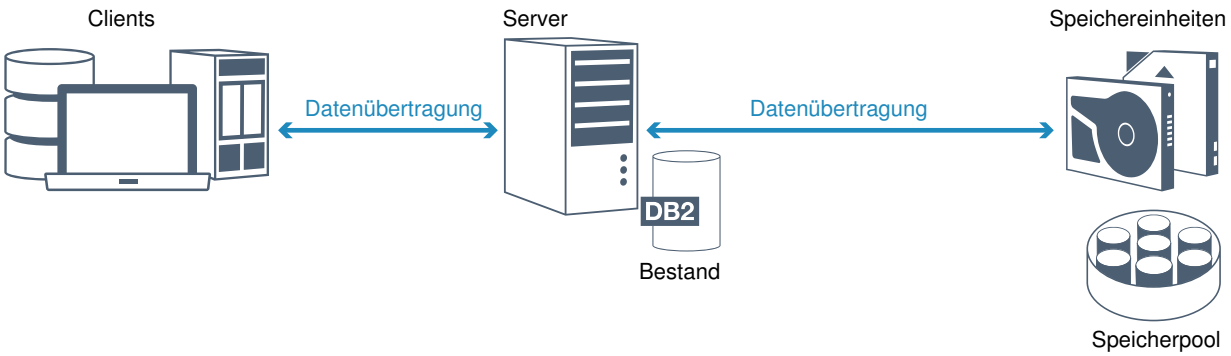


Abbildung 1. Komponenten in der Datenschutzlösung

Client-Software

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

Clientknoten

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

Speichermedien

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

Speichereinheiten

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

Speicherpools

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

Datenschutzservices

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

Typen von Datenschutzservices

IBM Spectrum Protect stellt Services zum Speichern und Wiederherstellen von Clientdaten bereit (siehe Abb. 2).

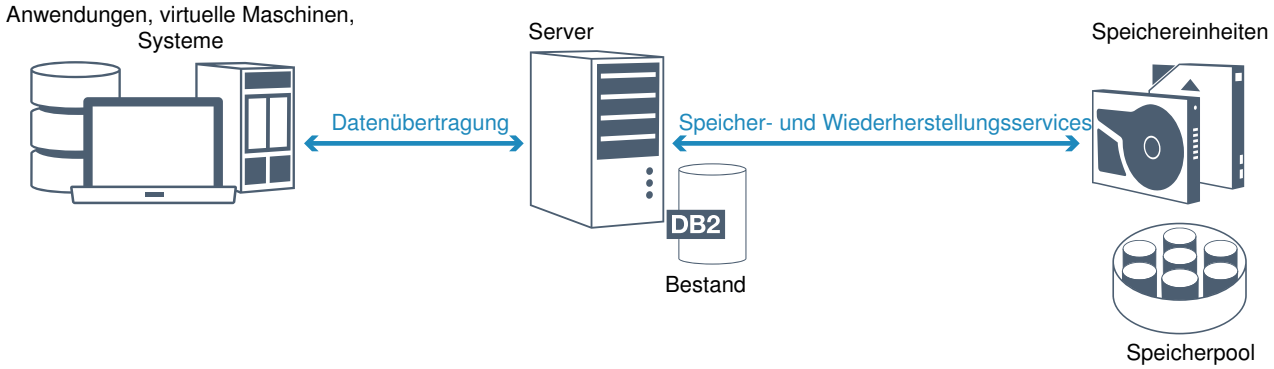


Abbildung 2. Datenschutzservices

IBM Spectrum Protect stellt die folgenden Typen von Datenschutzservices bereit:

Sicherungs- und Zurückschreibungsservices

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

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

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

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

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

Archivierungs- und Abrufservices

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

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

Vom Abrufservice werden die folgenden Funktionen bereitgestellt:

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

Umlagerungs- und Rückrufservices

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

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

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

Typen von Clientdaten, die geschützt werden können

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

Anwendungsclients

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

- IBM Spectrum Protect for Enterprise Resource Planning-Clients:
  - Data Protection for SAP HANA
  - Data Protection for SAP für Db2

  - Data Protection for SAP für Oracle
- IBM Spectrum Protect for Databases-Clients:
  - Data Protection for Microsoft SQL Server
  - Data Protection for Oracle
- IBM Spectrum Protect for Mail-Clients:
  - Data Protection for IBM Domino
  - Data Protection for Microsoft Exchange Server

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

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

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

Prozesse zur Verwaltung des Datenschutzes mit IBM Spectrum Protect

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

Datenverwaltungsprozess

Abb. 3 auf Seite 8 zeigt den IBM Spectrum Protect-Datenverwaltungsprozess.

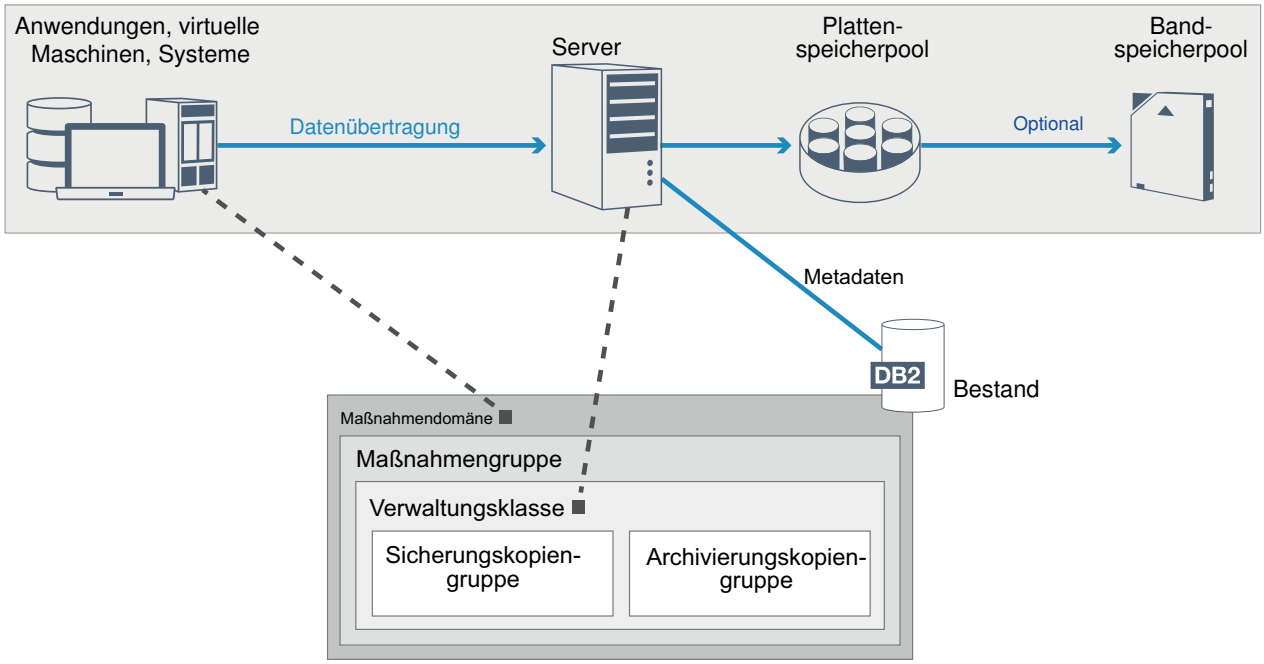


Abbildung 3. Datenverwaltungsprozess

IBM Spectrum Protect verwendet Maßnahmen, um zu steuern, wie der Server Datenobjekte auf verschiedenen Typen von Speichereinheiten und -medien speichert und verwaltet. Sie ordnen einen Client einer Maßnahmendomäne zu, die eine einzelne aktive Maßnahmengruppe enthält. Wenn ein Client eine Datei sichert, archiviert oder umlagert, wird die Datei an eine Verwaltungsklasse in der aktiven Maßnahmengruppe der Maßnahmendomäne gebunden. Die Verwaltungsklasse und die Sicherungs- und Archivierungskopiengruppen geben an, wo Dateien gespeichert werden und wie sie verwaltet werden. Wenn Sie Serverspeicher in einer Hierarchie konfigurieren, können Sie Dateien in andere Speicherpools umlagern.

Bestandskomponenten

Die folgenden Bestandskomponenten sind Schlüsselkomponenten für den Betrieb des Servers:

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

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

Wiederherstellungsprotokoll
Der Server zeichnet Datenbanktransaktionen im Wiederherstellungsproto-

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

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

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

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

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

Auf Maßnahmen basierende Datenverwaltung

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

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

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

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

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

Sie erstellen Maßnahmen, indem Sie die folgenden Maßnahmenkomponenten definieren:

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

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

Verwaltungsklasse

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

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

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

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

Sicherheitsmanagement

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

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

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

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

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

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

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

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

Benutzerschnittstellen für die IBM Spectrum Protect-Umgebung

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

Schnittstellen für die Datenspeicherverwaltung

Das Operations Center ist die primäre Schnittstelle für Administratoren zur Überwachung und Verwaltung von Servern. Ein Hauptvorteil des Operations Center ist die Möglichkeit, mehrere Server überwachen zu können (siehe Abb. 4). Sie können IBM Spectrum Protect auch über eine Befehlszeilenverwaltungsschnittstelle überwachen und verwalten.

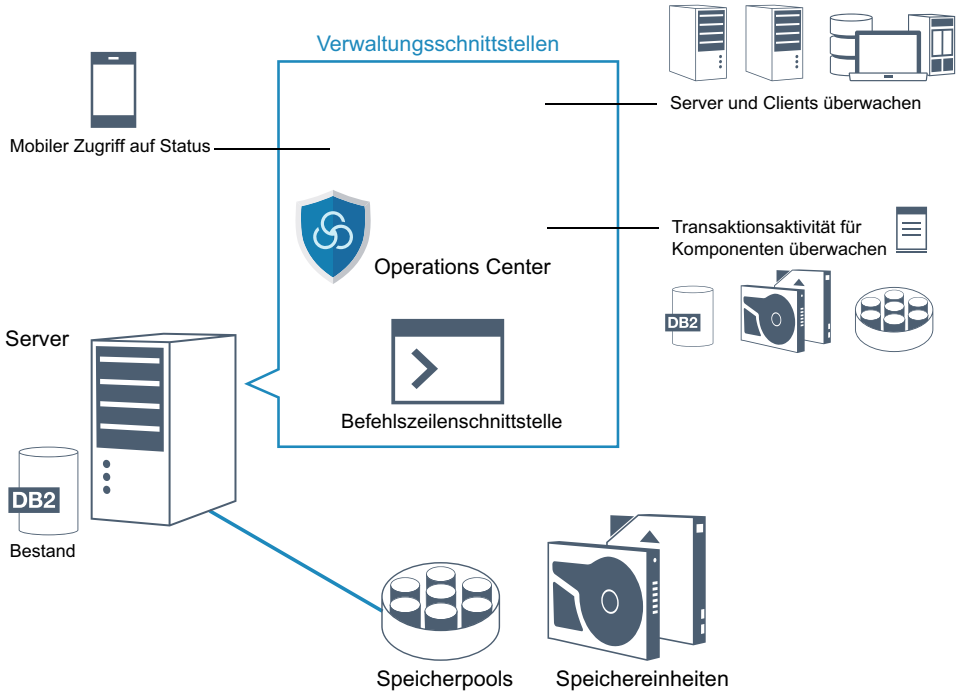


Abbildung 4. Benutzerschnittstellen für die Datenspeicherverwaltung

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

Operations Center

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

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

Befehlszeilenschnittstelle

Mithilfe einer Befehlszeilenschnittstelle können Sie Verwaltungstasks für

Server ausführen. Der Zugriff auf die Befehlszeilenschnittstelle kann entweder über den IBM Spectrum Protect-Verwaltungsclient oder das Operations Center erfolgen.

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

Schnittstellen für die Verwaltung der Clientaktivität

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

- Anwendungsprogrammierschnittstelle (API)
- Grafische Benutzerschnittstellen für Clients
- Browserschnittstelle für den Client für Sichern/Archivieren
- Befehlszeilenschnittstellen für Clients

Kapitel 2. Konzepte der Datenspeicherung in IBM Spectrum Protect

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

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

Typen von Speichereinheiten

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

Speichereinheiten und Speicherobjekte

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

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

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

Tabelle 1. Speicherobjekte und Darstellungen

Speicherobjekt	**Durch das Objekt dargestellte Ressource**
Datenträger	Eine diskrete Speichereinheit auf Platte, Band oder anderen Speichermedien. Jeder Datenträger ist einem einzelnen Speicherpool zugeordnet.
Speicherpool	Eine Gruppe von Speicherdatenträgern oder Containern, die als Ziel zum Speichern von Clientdaten dient. IBM Spectrum Protect verwendet die folgenden Typen von Speicherpools: • Verzeichniscontainerspeicherpools • Cloud-Containerspeicherpools • Speicherpools mit sequenziellem Zugriff, die einer Einheitenklasse zugeordnet sind • Speicherpools mit wahlfreiem Zugriff, die einer Einheitenklasse zugeordnet sind
Container	Eine Datenspeicherposition, beispielsweise eine Datei, ein Verzeichnis oder eine Einheit.

Tabelle 1. Speicherobjekte und Darstellungen (Forts.)

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

Der Administrator definiert die Speicherobjekte in der logischen Schicht des Servers (siehe Abb. 5 auf Seite 17).

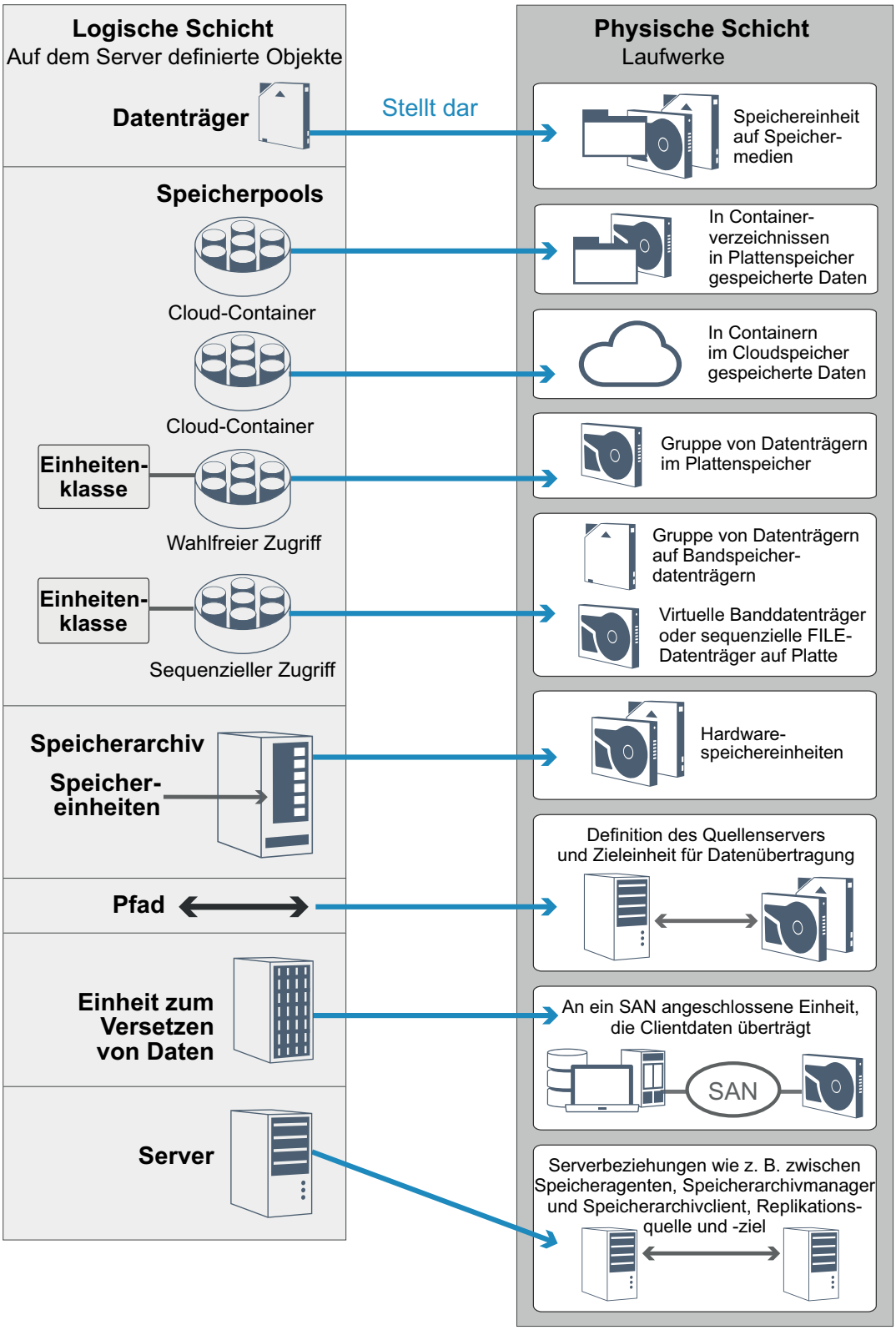


Abbildung 5. Speicherobjekte

Platteneinheiten

Sie können Clientdaten auf Platteneinheiten mit den folgenden Datenträgertypen speichern:

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

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

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

Physische Bandeinheiten

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

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

Das Versetzen von Daten auf Band bietet die folgenden Vorteile:

- Daten für Clients können auf einer Platteneinheit verbleiben, während die Daten gleichzeitig auf Band versetzt werden.
- Die Leistung von Bandlaufwerken kann verbessert werden, indem Daten mittels Streaming von Platte auf Band umgelagert werden.
- Die Nutzungszeiten für Bandlaufwerke können verlängert werden, um die Effizienz der Bandlaufwerke zu verbessern.
- Daten auf Band können in Vaults an anderen Standorten versetzt werden.
- Der Stromverbrauch kann eingeschränkt werden, da Bandeinheiten nach dem Schreiben von Daten auf Band keinen Strom mehr verbrauchen.
- Verschlüsselung, die von der Bandlaufwerkhardware bereitgestellt wird, kann angewendet werden, um die Daten auf Band zu schützen.

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

Virtuelle Bandarchive

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

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

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

Datenspeicherung in Speicherpools

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

Speicherpooltypen

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

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

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

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

Speicherpools für aktive Daten
: Eine benannte Gruppe von Speicherpooldatenträgern, die nur aktive Versionen von Clientsicherungsdaten enthalten.

Primäre Speicherpools

Wenn Sie Dateidaten zurückschreiben, abrufen, zurückrufen oder exportieren, wird die angeforderte Datei aus einem primären Speicherpool abgerufen. Abhängig vom Typ des primären Speicherpools können sich die Speicherpools vor Ort oder an einen anderen Standort befinden. Primäre Speicherpools können in einer Speicherhierarchie angeordnet werden, sodass Daten aus Plattenspeicher in kostengünstigeren Speicher, wie beispielsweise Bandeinheiten, übertragen werden können. Abb. 6 auf Seite 20 zeigt das Konzept primärer Speicherpools.

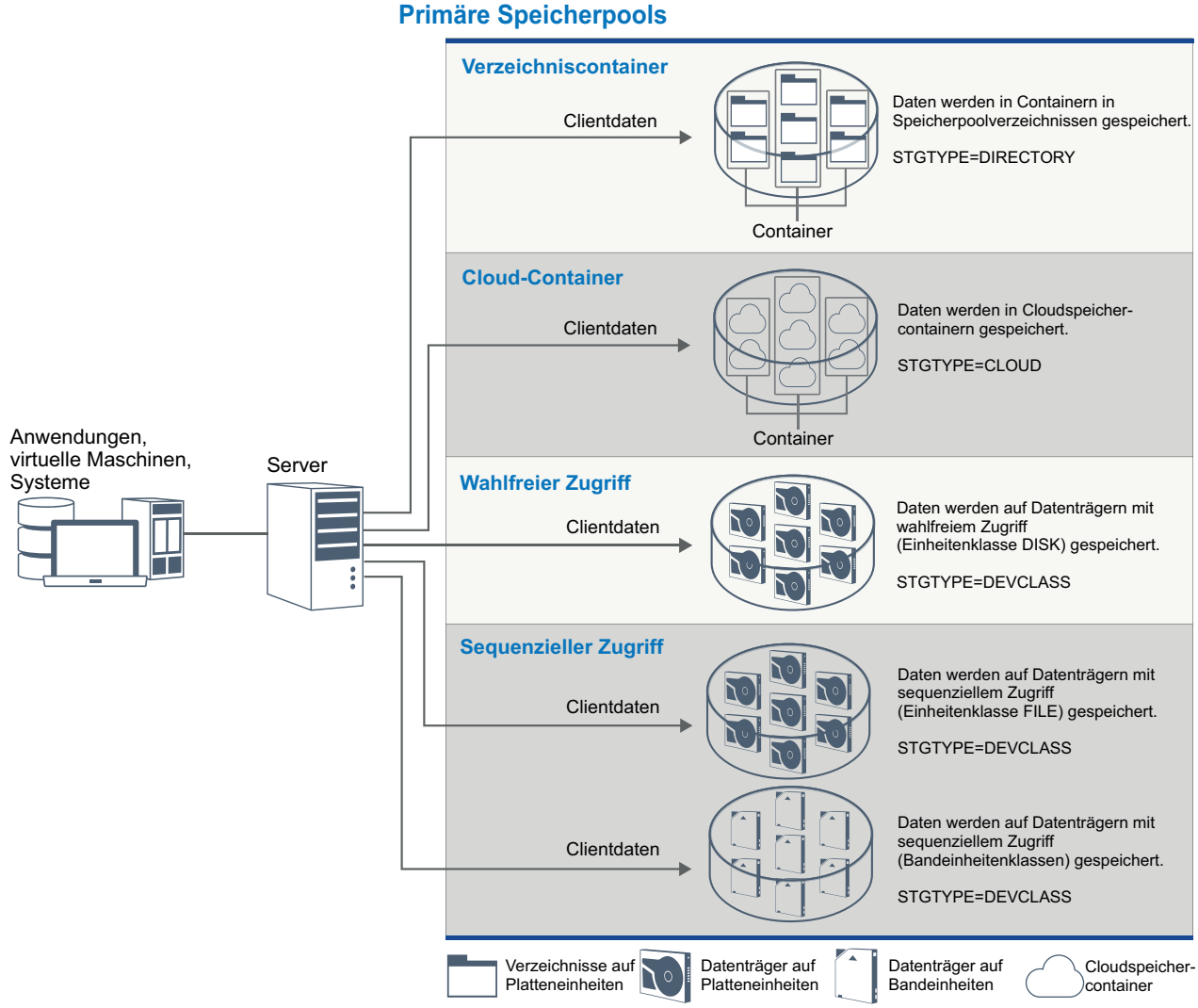


Abbildung 6. Primäre Speicherpools

Sie können die folgenden Typen primärer Speicherpools definieren:

Verzeichniscontainerspeicherpools

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

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

Durch die Verwendung von Verzeichniscontainerspeicherpools entfällt die Notwendigkeit zur Datenträgerkonsolidierung, wodurch die Serverleistung verbessert und die Kosten der Speicherhardware reduziert werden. Daten in Verzeichniscontainerspeicherpools können auf der Ebene des Speicher-

pools geschützt und repariert werden. Sie können Daten, die in einem Cloud-Containerspeicherpool gespeichert sind, mit Tiering in einen Cloud-Containerspeicherpool versetzen.

Einschränkung: Folgende Funktionen können bei Verzeichniscontainerspeicherpools nicht verwendet werden:

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

Cloud-Containerspeicherpools

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

Sie können die folgenden Typen von Cloud-Containerspeicherpools definieren:

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

Off premises
Sie können den Off-Premises-Typ für Cloud-Containerspeicherpools verwenden, um Daten in einer öffentlichen Cloud zu speichern. Die Verwendung einer öffentlichen Cloud hat den Vorteil, dass die Kosten geringer sind als bei einer privaten Cloud, da beispielsweise die Wartung entfällt. Sie müssen jedoch diesen Vorteil

und mögliche Leistungsprobleme aufgrund von Verbindungsgeschwindigkeiten und eingeschränkter Kontrolle über Ihre Daten gegeneinander abwägen.

Speicherpools, die Einheitenklassen zugeordnet sind

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

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

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

Der Server verwendet die folgenden primären Standardspeicherpools mit wahlfreiem Zugriff:

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

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

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

Kopienspeicherpools

Kopienspeicherpools enthalten aktive und inaktive Versionen von Daten, die aus primären Speicherpools gesichert werden. Ein Verzeichniscontainerspeicherpool kann nicht als Kopienspeicherpool verwendet werden. Außerdem können Daten aus einem Verzeichniscontainerspeicherpool nicht in einen Kopienspeicherpool kopiert werden. Um Verzeichniscontainerspeicherpools zu schützen, kopieren Sie die Daten in einen Containerkopienspeicherpool. Abb. 7 auf Seite 23 zeigt das Konzept von Kopienspeicherpools.

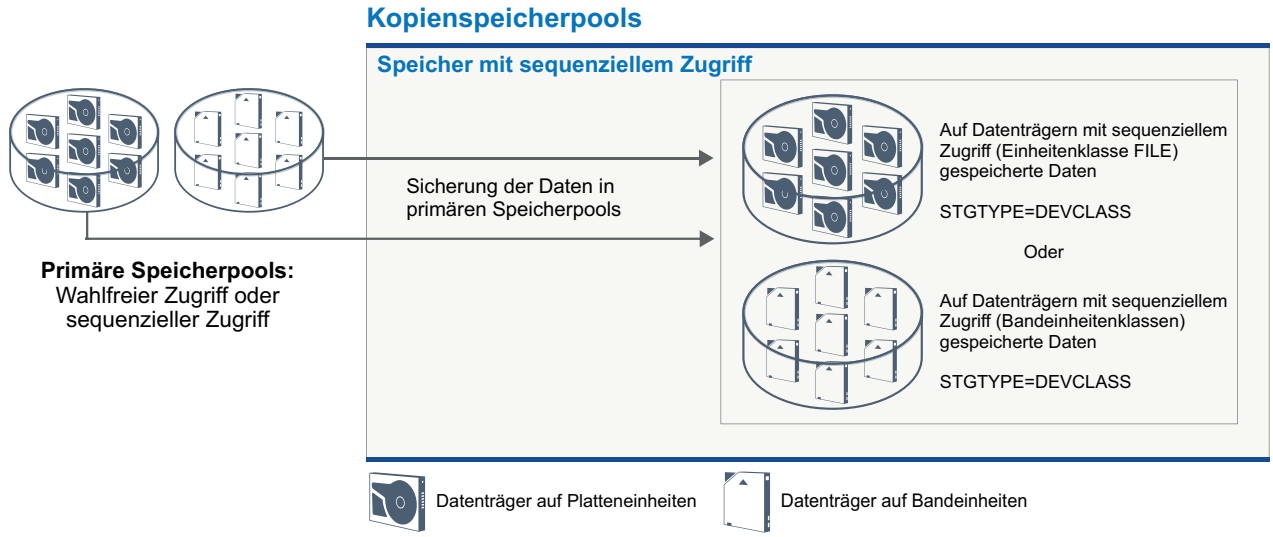


Abbildung 7. Kopienspeicherpools

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

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

Containerkopienspeicherpools

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

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

- Bei der Replikation können Sie Clientdaten direkt vom Zielserver zurückschreiben, wenn der Quellenserver nicht verfügbar ist.

- Bei Containerkopienspeicherpools müssen Sie zunächst den Server aus einer Datenbanksicherung zurückschreiben und dann die Verzeichniscontainerspeicherpools mithilfe von Banddatenträgern reparieren.

Abb. 8 zeigt das Konzept von Containerkopienspeicherpools.

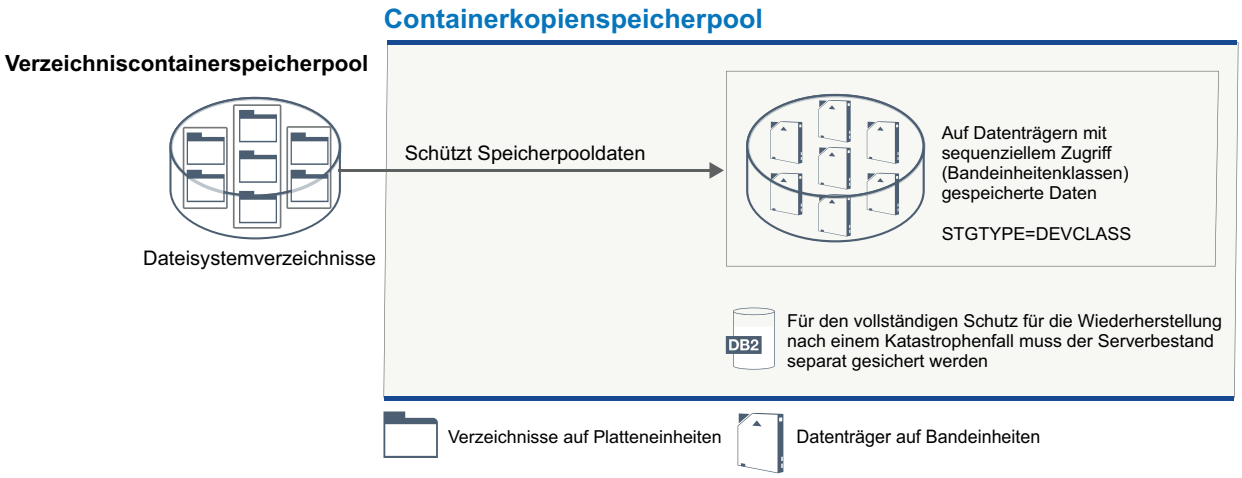


Abbildung 8. Containerkopienspeicherpools

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

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

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

- Die Notwendigkeit, einen weiteren Server und weiteren Plattenspeicherplatz verwalten zu müssen, entfällt.
- Daten werden in Speicherpools kopiert, die auf dem Server definiert sind. Die Leistung ist nicht von der Netzverbindung zwischen Servern abhängig oder von ihr betroffen.

- Sie können gesetzliche Bestimmungen und Geschäftsanforderungen für Bandkopien an einem anderen Standort erfüllen.

Speicherpools für aktive Daten

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

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

Daten, die von Clients für die hierarchische Speicherverwaltung (HSM-Clients) umgelagert werden, und Archivierungsdaten sind in Pools für aktive Daten nicht zulässig. Während aktualisierte Versionen von Sicherungsdaten in Pools für aktive Daten gespeichert werden, werden ältere Versionen entfernt, da die verbleibenden Daten von einer großen Anzahl Datenträger mit sequenziellem Zugriff auf einer geringeren Anzahl neuer Datenträger mit sequenziellem Zugriff konsolidiert werden. Abb. 9 zeigt das Konzepts von Speicherpools für aktive Daten.

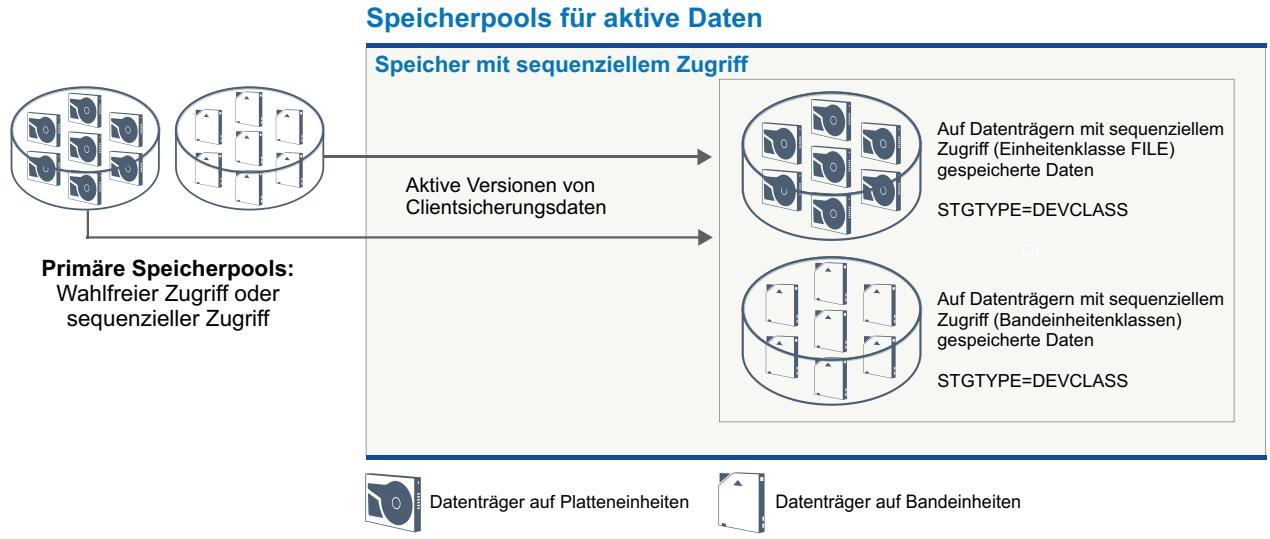


Abbildung 9. Speicherpools für aktive Daten

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

- FILE-Datenträger müssen nicht physisch bereitgestellt werden.

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

Datenübertragung über Netze in Speicher

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

Netzkonfigurationen für Speichereinheiten

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

Datensicherungsoperationen über ein LAN

Abb. 10 zeigt den Datenpfad für IBM Spectrum Protect-Sicherungsoperationen über ein LAN.

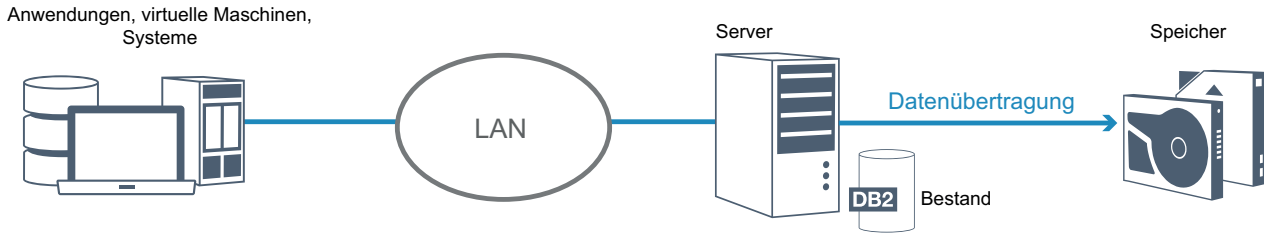


Abbildung 10. IBM Spectrum Protect-Sicherungsoperationen über ein LAN

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

Datensicherungsoperationen über ein SAN

Abb. 11 auf Seite 27 zeigt den Datenpfad für IBM Spectrum Protect-Sicherungsoperationen über ein SAN.

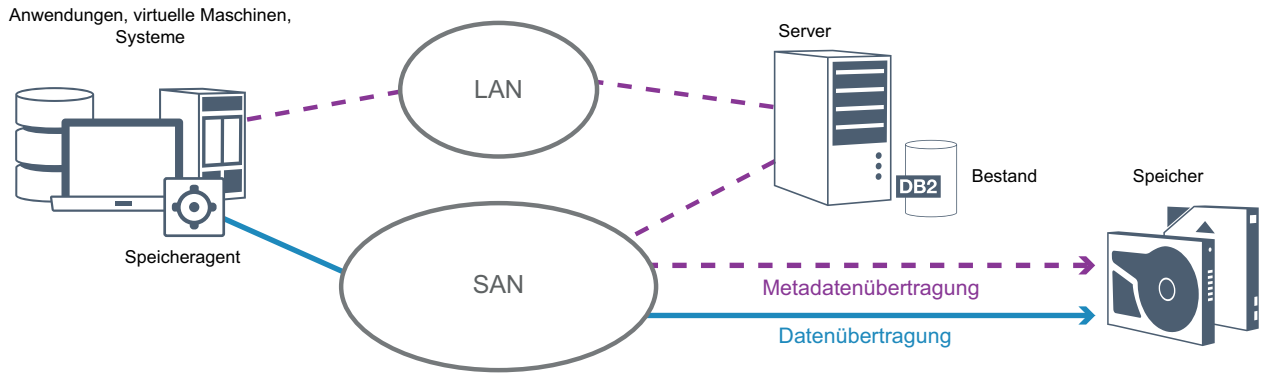


Abbildung 11. IBM Spectrum Protect-Sicherungsoperationen über ein SAN

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

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

  Über den Speicheragenten kann der Client Daten direkt in einem Bandarchiv oder einem gemeinsam genutzten Dateisystem, wie beispielsweise GPFS, sichern und aus ihm zurückzuschreiben. Der IBM Spectrum Protect-Server verwaltet die Serverdatenbank und das Wiederherstellungsprotokoll und fungiert als Speicherarchivmanager, um Einheitenoperationen zu steuern. Der Speicheragent auf dem Client handhabt die Datenübertragung zu der Einheit auf dem SAN. Diese Implementierung gibt Bandbreite im LAN frei, die andernfalls für das Versetzen von Clientdaten verwendet würde.
- Gemeinsame Nutzung von Bandlaufwerken und Speicherarchiven, die vom IBM Spectrum Protect-Server unterstützt werden.
- Konsolidierung mehrerer Clients unter einem einzelnen Clientknotennamen in einem GPFS-Cluster (GPFS = General Parallel File System).

Network-attached Storage (NAS)

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

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

Speicherverwaltung

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

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

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

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

Datenträgerwiederverwendung durch Konsolidierung
Da Daten aufgrund von Servermaßnahmen automatisch verfallen, nimmt der freie Speicherbereich auf den Datenträgern, auf denen die Daten gespeichert sind, ständig zu. Bei allen Speichermedien mit Ausnahme von Verzeichniscontainerspeicherpools und Plattenspeicherpools mit wahlfrei-

em Zugriff implementiert der IBM Spectrum Protect-Server die *Konsolidierung*, ein Prozess, bei dem Datenträger für die Wiederverwendung freigegeben werden, ohne dass die traditionelle Bandrotation angewendet wird. Bei der Konsolidierung wird ein Datenträger automatisch defragmentiert, indem nicht verfallene Daten auf anderen Datenträgern konsolidiert werden, wenn der freie Speicherbereich auf einem Datenträger einen definierten Stand erreicht. Der konsolidierte Datenträger kann dann vom Server erneut verwendet werden. Die Konsolidierung ermöglicht den automatischen Umlauf von Datenträgern im Speicherverwaltungsprozess und die Minimierung der Anzahl erforderlicher Datenträger.

Gesicherte Clientdaten konsolidieren

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

Clientdaten kollokieren

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

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

Pools für aktive Daten verschiedenen Einheiten zuordnen

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

Sicherungsgruppe erstellen

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

Daten für einen Clientknoten versetzen

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

Kapitel 3. Datenschutzstrategien bei IBM Spectrum Protect

IBM Spectrum Protect stellt Möglichkeiten zur Implementierung verschiedener Datenschutzstrategien bereit.

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

Strategien zum Minimieren der Verwendung von Speicherbereich für Sicherungen

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

Datendeduplizierung

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

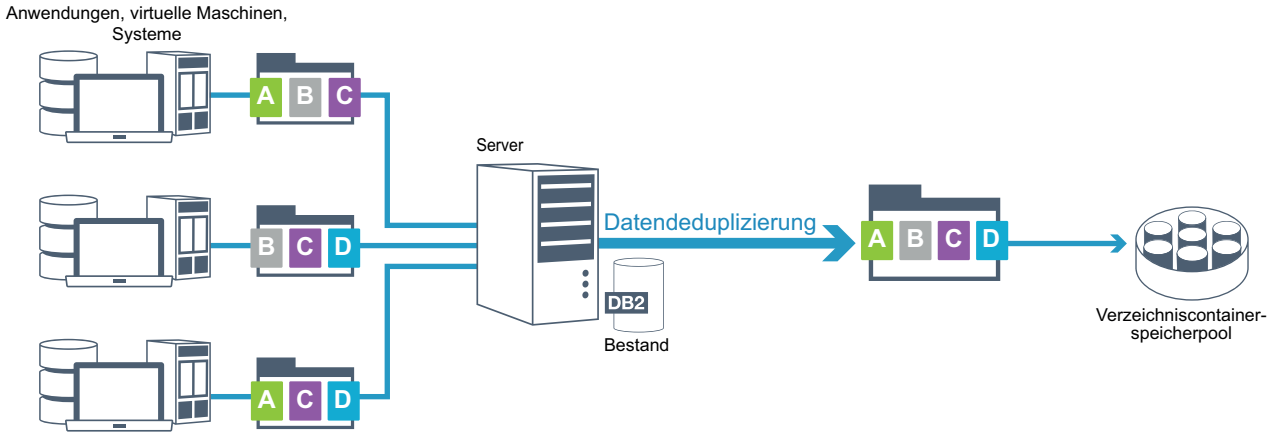


Abbildung 12. Datendeduplizierungsprozess

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

IBM Spectrum Protect stellt die folgenden Datendeduplizierungstypen bereit:

Serverseitige Datendeduplizierung

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

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

Clientseitige Datendeduplizierung

Mit dieser Methode wird die Verarbeitung während eines Sicherungsprozesses auf den Server und den Client verteilt. Der Client und der Server identifizieren und entfernen doppelte Daten, um Speicherbereich auf dem Server einzusparen. Bei der clientseitigen Datendeduplizierung werden nur komprimierte, deduplizierte Daten an den Server gesendet. Der Server speichert die Daten in dem vom Client zur Verfügung gestellten komprimierten Format. Die clientseitige Datendeduplizierung bietet die folgenden Vorteile:

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

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

Komprimierung

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

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

Progressive Teilsicherung

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

Strategien zum Schutz vor Katastrophen

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

Replikation an einen fernen Standort

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

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

Vorteile

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

Nachteile

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

Abb. 13 auf Seite 34 zeigt den Replikationsprozess an einen fernen Standort.

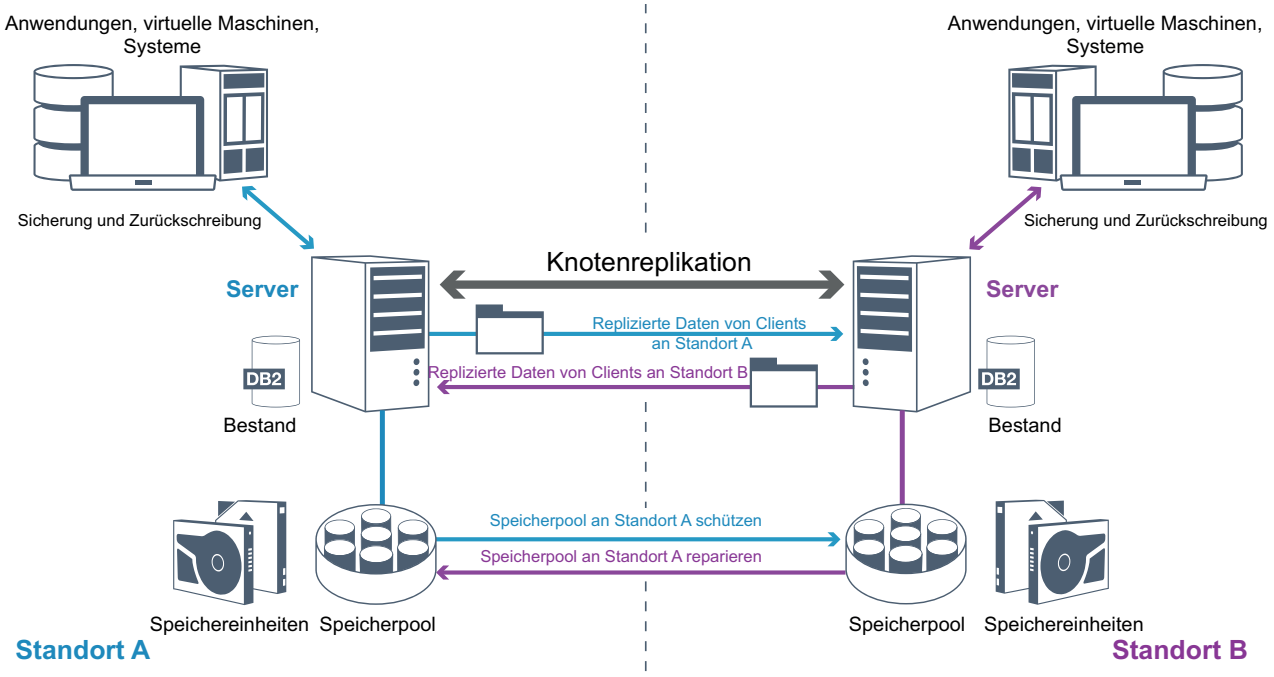


Abbildung 13. Knotenreplikationsprozess

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

IBM Spectrum Protect stellt die folgenden Replikationsfunktionen bereit:

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

  Wenn ein Katastrophenfall eintritt und der Quellenserver nicht verfügbar ist, können Clients Daten vom Zielserver wiederherstellen. Wenn eine Wiederherstellung des Quellenservers nicht möglich ist, können Sie Clients anweisen, Daten auf dem Zielserver zu speichern. Bei einem Ausfall kann für die Clients, die auf dem Quellenserver gesichert werden, automatisch eine Übernahme erfolgen, damit ihre Daten vom Zielserver zurückgeschrieben werden können.
- Mithilfe der Replikationsverarbeitung können Sie beschädigte Dateien aus Speicherpools wiederherstellen. Sie müssen die Clientdaten auf den Zielserver replizieren, bevor die Datei beschädigt wird. Nachfolgende Replikationsprozesse erkennen beschädigte Dateien auf dem Quellenserver und ersetzen sie durch unbeschädigte Dateien vom Zielserver.

Rolle der Replikation beim Schutz vor Katastrophen

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

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

Speicherpoolschutz

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

Vorteile

- Schnelle Wiederherstellung und Neuerstellung des Quellensystems

Nachteile

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

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

Verzeichniscontainerspeicherpools

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

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

Containerkopienspeicherpools

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

Speicherpools, die Einheitenklassen FILE und DISK zugeordnet sind

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

Datenbanksicherungen

Sie verwenden Datenbanksicherungen, um Ihr System nach einer Beschädigung der Datenbank wiederherzustellen. Datenbanksicherungsoperationen müssen außerdem verwendet werden, um zu verhindern, dass bei Db2 der Speicherbereich für das Archivprotokoll knapp wird. Datenbanksicherungsoperationen sind nicht Teil der Knotenreplikation. Bei einer Datenbanksicherung kann es sich um eine Gesamt-, Teil- oder Momentaufnahmesicherung handeln. Um eine schnelle Wiederherstellung nach einem Katastrophenfall zu ermöglichen, muss eine Kopie der Datenbanksicherungen an einen anderen Standort gespeichert werden. Um die Datenbank zurückschreiben zu können, müssen Sie über die Sicherungsdatenträger für die Datenbank verfügen. Sie können die Datenbank mithilfe einer Operation für die Zurückschreibung nach Zeitpunkt oder einer Operation für die Zurückschreibung mit dem neuesten Stand aus Sicherungsdatenträgern zurückschreiben.

Zurückschreibung nach Zeitpunkt

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

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

Zurückschreibung mit dem neuesten Stand

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

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

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

Alternativmethoden zum Schutz vor Katastrophen

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

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

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

Vergleich der Konfigurationsstrategien für den Schutz

Beachten Sie die folgenden potenziellen Datenverlustszenarios:

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

Die folgenden potenziellen Konfigurationen betreffen die gängigsten Datenschutzszenarios:

Konfigurationen ausschließlich für den Schutz vor einer Beschädigung

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

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

- Implementieren Sie Datenbanksicherungsoperationen an einen anderen Standort mit Containerkopienspeicherpools an einen anderen Standort, um Daten in Verzeichniscontainerspeicherpools zu schützen.

- Implementieren Sie Datenbanksicherungsoperationen vor Ort und die Knotenreplikation an einem anderen Standort mit einem optionalen Containerkopienspeicherpool vor Ort für die schnellere Wiederherstellung beschädigter Daten.

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

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

Automatische Übernahme für die Wiederherstellung nach einem Katastrophenfall

Die *automatische Übernahme* ist eine Operation, mit zu einem Standby-System gewechselt wird, wenn eine Software-, Hardware- oder Netzunterbrechung auftritt. Die automatische Übernahme wird zusammen mit der Knotenreplikation zur Wiederherstellung von Daten nach einem Systemfehler verwendet. Abb. 14 zeigt den automatischen Übernahmeprozess in IBM Spectrum Protect.

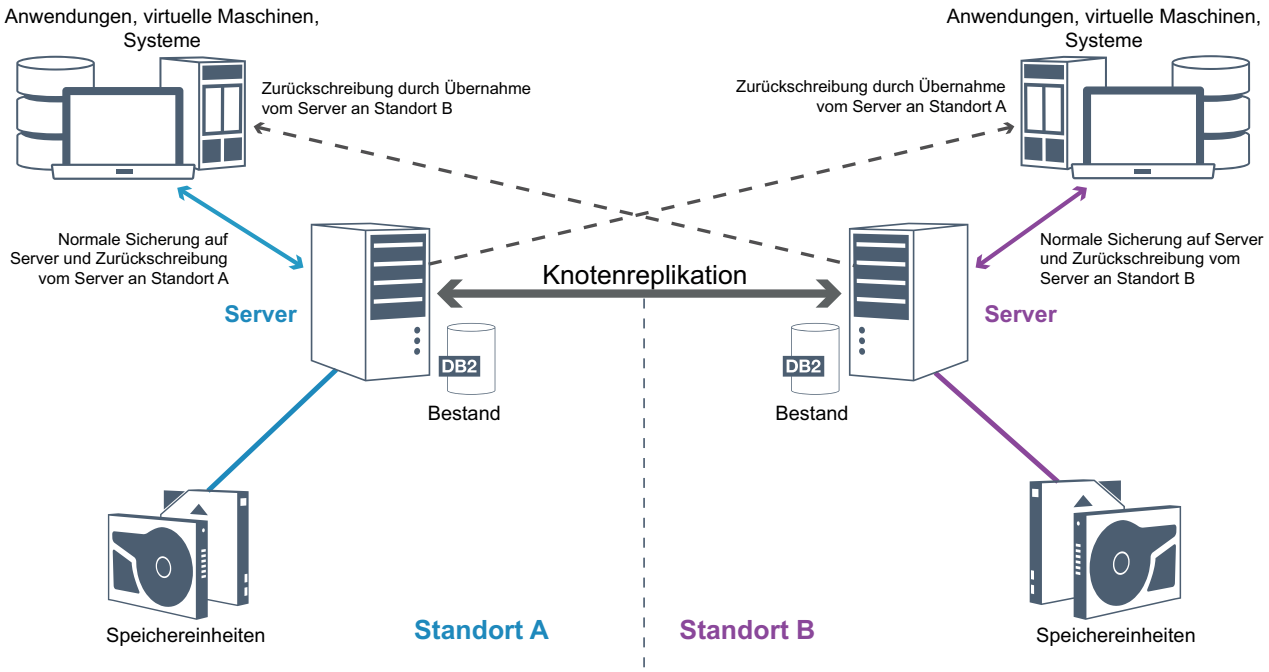


Abbildung 14. Automatischer Übernahmeprozess

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

Während Clientzurückschreibungsoperationen wechseln Clients automatisch vom Quellenreplikationsserver zum Zielreplikationsserver und wieder zurück; dieser Wechsel wird durch den Server ausgeführt. Für den Schutz durch Übernahme

kann jeweils nur ein einziger Server pro Knoten verwendet werden. Wenn eine neue Clientoperation gestartet wird, versucht der Client, die Verbindung zum Quellenreplikationsserver herzustellen. Der Client nimmt die Operationen auf dem Quellenserver wieder auf, wenn der Quellenreplikationsserver verfügbar ist.

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

Wiederherstellung von IBM Spectrum Protect-Komponenten

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

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

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

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

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

Vorbeugende Maßnahmen für die Wiederherstellung

Die Wiederherstellung basiert auf folgenden vorbeugenden Maßnahmen:

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

Wenn Sie Bänder zum Speichern verwenden, können Sie auch einen Plan zur Wiederherstellung nach einem Katastrophenfall (der auch als Wiederherstellungsplan

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

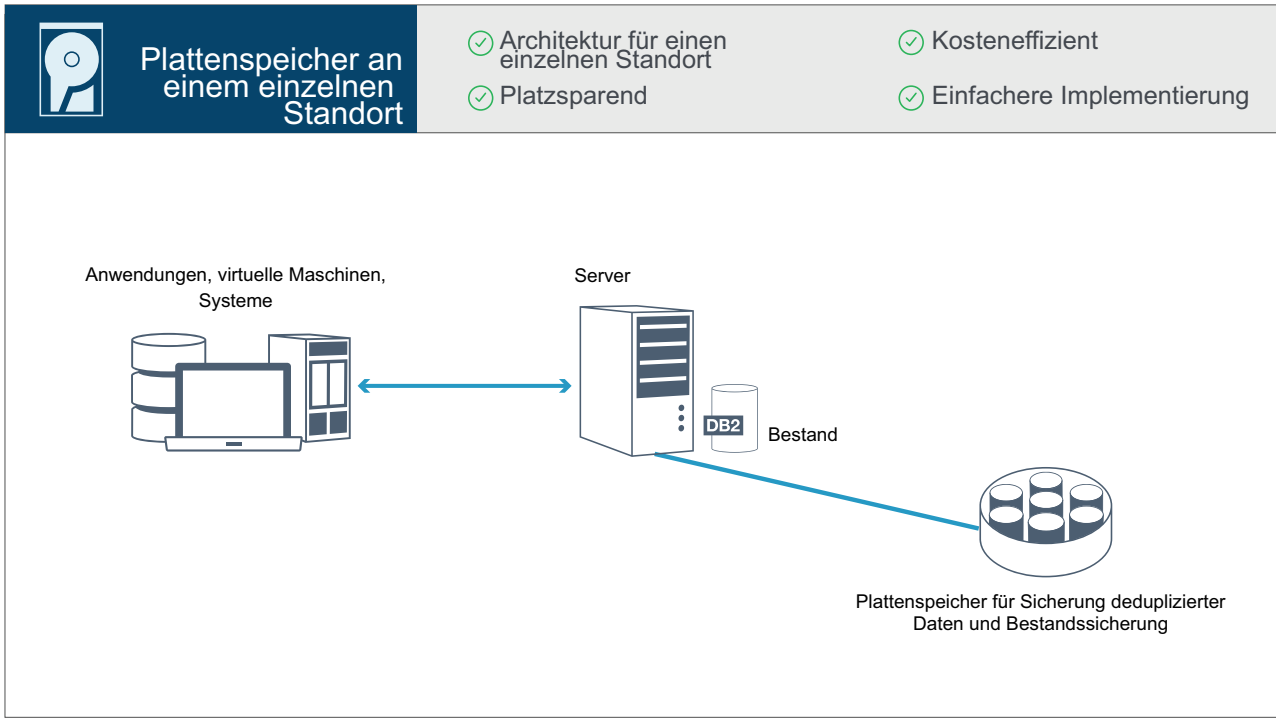
- Erstellen einer Wiederherstellungsplandatei für den Server
- Sichern von Serverdaten auf Band
- Senden der Serversicherungsdaten an einen fernen Standort oder einen anderen Server
- Speichern von Clientsysteminformationen
- Definieren und Verfolgen der Speichermedien, die zum Speichern und Wiederherstellen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

Teil 2. IBM Spectrum Protect-Lösungen für den Datenschutz

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

Kapitel 4. Plattenbasierte Implementierung einer Datenschutzlösung für einen einzelnen Standort

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



Diese Datenschutzlösung bietet die folgenden Vorteile:

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

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

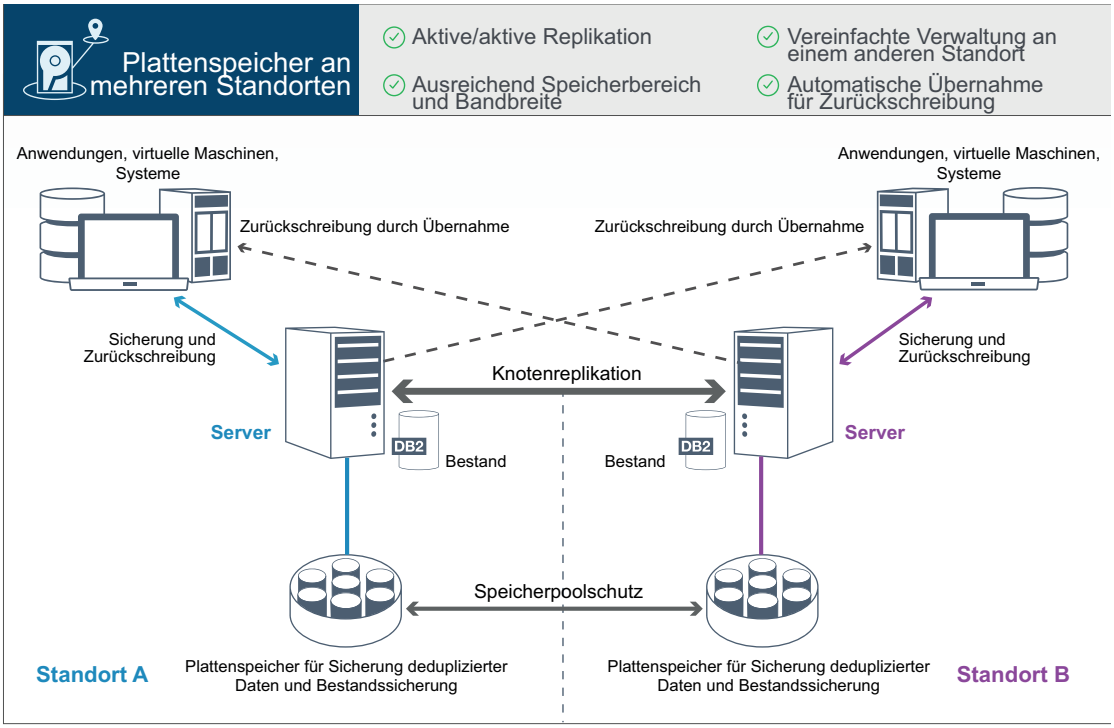
Zugehörige Verweise:

Kapitel 8, „Vergleich der Datenschutzlösungen", auf Seite 51

Kapitel 9, „Roadmap für die Implementierung einer Datenschutzlösung", auf Seite 53

Kapitel 5. Plattenbasierte Implementierung einer Datenschutzlösung für mehrere Standorte

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



Diese Datenschutzlösung bietet die folgenden Vorteile:

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

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

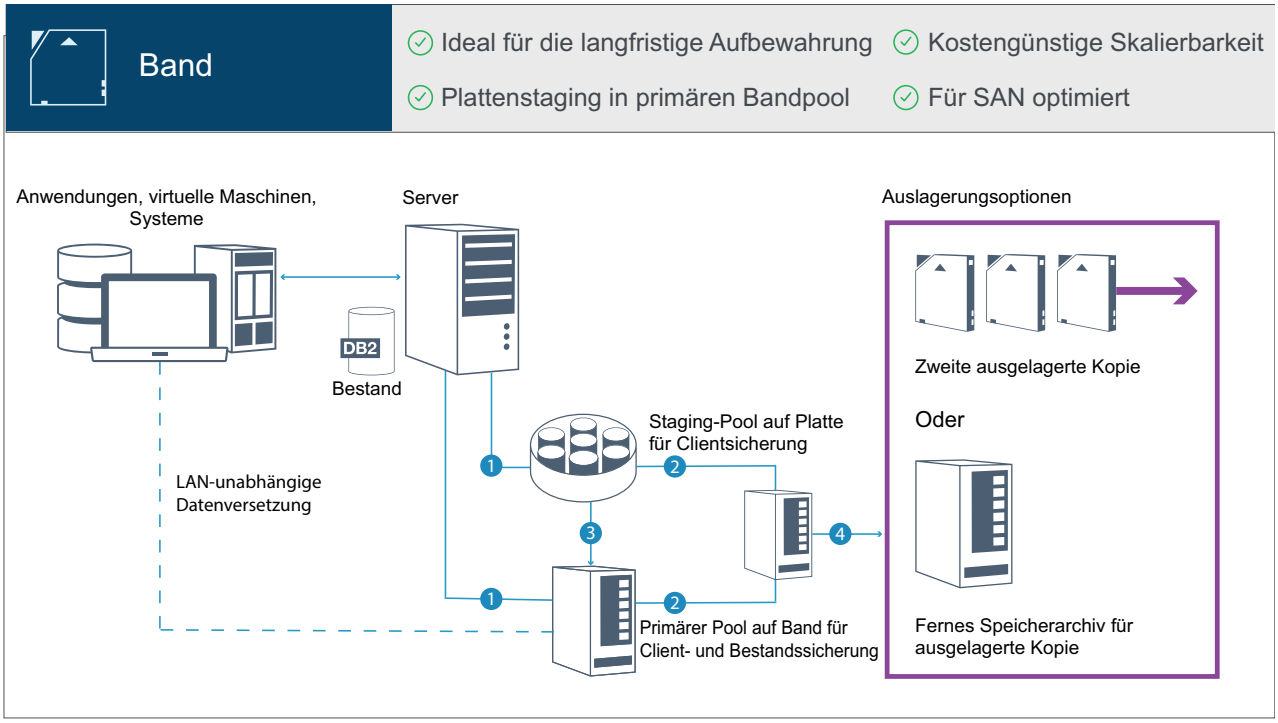
Zugehörige Verweise:

Kapitel 8, „Vergleich der Datenschutzlösungen”, auf Seite 51

Kapitel 9, „Roadmap für die Implementierung einer Datenschutzlösung”, auf Seite 53

Kapitel 6. Bandbasierte Implementierung einer Datenschutzlösung

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



Diese Datenschutzlösung bietet die folgenden Vorteile:

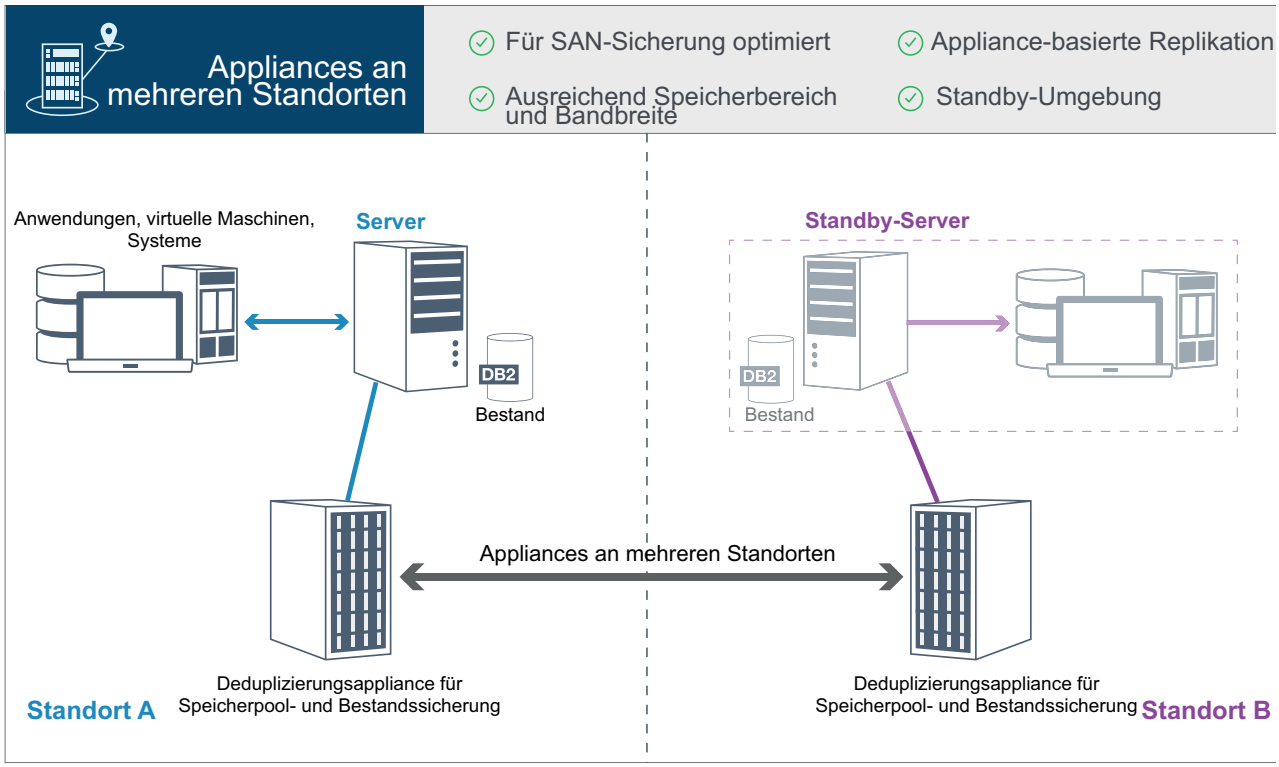
- Die Leistung wird für Sicherungsoperationen in Hochgeschwindigkeits-SANs, die direkt auf Band erfolgen, für große Datentypen und für die langfristige Aufbewahrung von Daten optimiert.
- Die Datenverfügbarkeit wird optimiert, indem Kopien von Daten für die Wiederherstellung nach einem Katastrophenfall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

Zugehörige Verweise:

Kapitel 8, „Vergleich der Datenschutzlösungen”, auf Seite 51

Kapitel 7. Appliance-basierte Implementierung einer Datenschutzlösung für mehrere Standorte

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



Diese Datenschutzlösung bietet die folgenden Vorteile:

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

Bei dieser Datenschutzkonfiguration verwendet der Server Hardware-Appliances zum Deduplizieren und Replizieren von Daten. Die Appliance an Standort A dedupliziert Daten und repliziert die Daten anschließend zum Schutz vor Katastrophen

auf die Appliance an Standort B. Bei einem Ausfall an Standort A können Sie den Standby-Server aktivieren, indem Sie die neueste Datenbanksicherung zurückschreiben und die replizierte Kopie der Daten aktivieren.

Weitere Informationen zum Konfigurieren virtueller Bandarchive finden Sie in Virtuelle Bandarchive konfigurieren.

Zugehörige Verweise:

Kapitel 8, „Vergleich der Datenschutzlösungen", auf Seite 51

Kapitel 9, „Roadmap für die Implementierung einer Datenschutzlösung", auf Seite 53

Kapitel 8. Vergleich der Datenschutzlösungen

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

	Plattenspeicher an einem einzelnen Standort	**Plattenspeicher an mehreren Standorten**	**Appliances an mehreren Standorten**	**Band**
				
Schwerpunkte				
Kosten	$	$$$	$$$$	$$
Schutzstufe	1 Datenkopie	2 oder mehr Datenkopien	2 oder mehr Datenkopien	2 oder mehr Datenkopien
Wiederherstellung nach einem Katastrophenfall	Keine	Aktiver Server	Standby-Server	Kopien an einem anderen Standort
Hauptvorteile				
Erstklassige Datenreduktion	✓	✓	✓	✓
Schnelle und effiziente plattenbasierte Sicherungs- und Zurückschreibungsoperationen	✓	✓	✓	
Vereinfachte Verwaltung an einem anderen Standort		✓		
Datendeduplizierungsfunktion ohne Zusatzkosten	✓	✓		
Inklusive Replikationsverarbeitung ohne Zusatzkosten		✓		
Datendeduplizierung sowohl auf dem Quellenserver als auch auf dem Zielserver		✓		
Kostengünstige Skalierbarkeit, für die langfristige Aufbewahrung optimiert				✓
Effizienz und Kosten				
Für Hochgeschwindigkeitssicherungsoperationen im Speicherbereichsnetz optimiert			✓	✓
Für Hochgeschwindigkeitsoperationen im lokalen Netz (LAN) optimiert	✓	✓	✓	
Globale Datendeduplizierung für alle Datentypen und Quellen	✓	✓	✓	
Bandbreiteneffiziente Replikation		✓	✓	
Niedrigere Energiekosten				✓

	Plattenspeicher an einem einzelnen Standort	Plattenspeicher an mehreren Standorten	Appliances an mehreren Standorten	Band
				
Option einer zweiten Kopie ohne weitere Plattenhardware				✓
Verfügbarkeit				
Möglichkeit von Kopien an einem anderen Standort		✓	✓	✓
Appliance-basierte Replikation			✓	
Clientwiederherstellung von einem Hochverfügbarkeitsserver		✓		
Replikationsziel in der Cloud		✓		
Unabhängige Verwaltung von Aufbewahrungsmaßnahmen für Replikationsdaten; Möglichkeit, am Wiederherstellungsstandort mehr oder weniger Daten aufzubewahren		✓		
Replikation auf Anwendungsebene; Möglichkeit, die Systeme und Anwendungen auszuwählen, die repliziert werden		✓		
Skalierbarkeit				
Globale Datendeduplizierung für alle Server			✓	
Direkte SAN-optimierte Sicherung auf Band für große Datentypen				✓
Skalierbarkeit von Einzelinstanzen im Petabytebereich				✓

Nächste Schritte

Lesen Sie die für die Lösungen verfügbare Dokumentation (siehe Kapitel 9, „Roadmap für die Implementierung einer Datenschutzlösung", auf Seite 53).

Zugehörige Verweise:

Kapitel 4, „Plattenbasierte Implementierung einer Datenschutzlösung für einen einzelnen Standort", auf Seite 43

Kapitel 5, „Plattenbasierte Implementierung einer Datenschutzlösung für mehrere Standorte", auf Seite 45

Kapitel 7, „Appliance-basierte Implementierung einer Datenschutzlösung für mehrere Standorte", auf Seite 49

Kapitel 6, „Bandbasierte Implementierung einer Datenschutzlösung", auf Seite 47

Kapitel 9. Roadmap für die Implementierung einer Datenschutzlösung

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

Plattenspeicherlösung für einen einzelnen Standort

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

Plattenspeicherlösung für mehrere Standorte

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

Bandspeicherlösung

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

Appliance-Lösung für mehrere Standorte

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

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

   Eine Anleitung zur Verbesserung der Systemleistung finden Sie in Bewährte Verfahren bei der Konfiguration.
4. Konfigurieren Sie Maßnahmen zum Schützen Ihrer Daten. Lesen Sie die Informationen in Maßnahmen anpassen.
5. Definieren Sie Clientzeitpläne. Lesen Sie die Informationen in Sicherungs- und Archivierungsoperationen planen.
6. Installieren und konfigurieren Sie Clients. Ausführliche Informationen zur Bestimmung des Typs der erforderlichen Client-Software finden Sie in Clients hinzufügen.

7. Konfigurieren Sie die Überwachung für Ihr System. Lesen Sie die Informationen in Speicherlösungen überwachen.

Zugehörige Verweise:

Kapitel 8, „Vergleich der Datenschutzlösungen", auf Seite 51

Kapitel 4, „Plattenbasierte Implementierung einer Datenschutzlösung für einen einzelnen Standort", auf Seite 43

Kapitel 5, „Plattenbasierte Implementierung einer Datenschutzlösung für mehrere Standorte", auf Seite 45

Kapitel 7, „Appliance-basierte Implementierung einer Datenschutzlösung für mehrere Standorte", auf Seite 49

Kapitel 6, „Bandbasierte Implementierung einer Datenschutzlösung", auf Seite 47

Teil 3. Anhänge und Schlussteil

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/releasenotes.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 diesem Dokument 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 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 Quellensprache geschrieben sind und Programmiertechniken 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 International Business Machines Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Herstellern 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 der 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 der zugehörigen Tochtergesellschaften in den USA und/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 oder anderen Ländern.

Bedingungen für die 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 weder weitergeben oder anzeigen noch 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 Genehmi-

gung 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 Veröffentlichungen. 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

Für die IBM Spectrum Protect-Produktfamilie steht ein Glossar mit Begriffen und Definitionen zur Verfügung.

Siehe das Glossar für IBM Spectrum Protect.

Index

O

P

R

S

T

U

V

W

Z

Programmnummer: 5725-W98
5725-W99
5725-X15

Gedruckt in Deutschland