Dell EMC Data Domain® Operating System

Version 6.1

Administrationshandbuch

302-003-761

REV. 04

DELL EMC

Stand Juli 2018

EMC Deutschland GmbH
Am Kronberger Hang 2a 65824 Schwalbach/Taunus
Tel.: +49 6196 4728-0
www.DellEMC.com/de-de/index.htm

INHALT

Vorwort

Data Domain möchte seine Produktserien fortlaufend verbessern und veröffentlicht daher regelmäßig neue Software- und Hardwareversionen. Aus diesem Grund werden einige in diesem Dokument beschriebene Funktionen eventuell nicht von allen Versionen der von Ihnen verwendeten Software oder Hardware unterstützt. Aktuelle Informationen zu Produktfunktionen, Softwareupdates, Kompatibilitätsleitfäden für Software und Informationen zu Data Domain-Produkten, -Lizenzierung und -Service finden Sie in den entsprechenden Produktversionshinweisen.

Wenden Sie sich an Ihren Experten für technischen Support, wenn ein Produkt nicht ordnungsgemäß oder nicht wie in diesem Dokument beschrieben funktioniert.

Hinweis

Dieses Dokument war zum Veröffentlichungszeitpunkt korrekt. Prüfen Sie auf der Website des Online Support (https://support.emc.com), ob Sie die aktuelle Version dieses Dokuments verwenden.

Zweck

In diesem Handbuch wird beschrieben, wie Sie Data Domain®-Systeme managen. Der Schwerpunkt liegt dabei auf Verfahren, für die Data Domain System Manager (DD System Manager), eine browserbasierte grafische Benutzeroberfläche (GUI), verwendet wird. Wenn eine wichtige administrative Aufgabe nicht in DD System Manager unterstützt wird, werden die Befehle der Befehlszeilenoberfläche (CLI) beschrieben.

Hinweis

- DD System Manager war früher unter dem Namen Enterprise Manager bekannt.
- In einigen Fällen bietet ein CLI-Befehl möglicherweise mehr Optionen als die entsprechende DD System Manager-Funktion. Eine vollständige Beschreibung eines Befehls und seiner Optionen finden Sie im *Data Domain Operating System Command Reference Guide*.

Zielgruppe

Dieses Handbuch richtet sich an Systemadministratoren, die mit Standardbackupsoftware-Paketen und der allgemeinen Backupadministration vertraut sind.

Zugehörige Dokumentation

In den folgenden Dokumenten zum Data Domain-System finden Sie zusätzliche Informationen:

- Installations- und Einrichtungshandbuch für Ihr System, z. B. *Data Domain DD9300 System Installation Guide*
- *Data Domain Hardware Features and Specifications Guide*
- *Data Domain Operating System USB Installation Guide*
- *Data Domain Operating System DVD Installation Guide*
- *Data Domain Operating System Release Notes*

- *Data Domain Operating System Initial Configuration Guide*
- *Data Domain Security Configuration Guide*
- *Data Domain Operating System High Availability White Paper*
- *Data Domain Operating System Command Reference Guide*
- *Data Domain Operating System MIB Quick Reference*
- *Data Domain Operating System Offline Diagnostics Suite User's Guide*
- Handbücher zum Austausch von Ersatzteilen für Ihre Systemkomponenten, z. B. *Field Replacement Guide, Data Domain DD4200, DD4500, and DD7200 Systems, IO Module and Management Module Replacement or Upgrade*
- *Data Domain, System Controller Upgrade Guide*
- *Data Domain Expansion Shelf, Hardware Guide* (für Einschubmodell ES30/FS15 oder DS60)
- *Data Domain Boost for Partner Integration Administration Guide*
- *Data Domain Boost for OpenStorage Administration Guide*
- *Data Domain Boost for Oracle Recovery Manager Administration Guide*
- *Statement of Volatility for the Data Domain DD2500 System*
- *Statement of Volatility for the Data Domain DD4200, DD4500, or DD7200 System*
- *Statement of Volatility for the Data Domain DD6300, DD6800, or DD9300 System*
- *Statement of Volatility for the Data Domain DD9500 or DD9800 System*

Wenn Sie über den optionalen RSA Data Protection (DPM) Key Manager verfügen, finden Sie weitere Informationen in der neuesten Version des *RSA Data Protection Manager Server Administrator's Guide*, der mit dem RSA Key Manager-Produkt verfügbar ist.

In diesem Dokument verwendete Konventionen für spezielle Hinweise
Data Domain verwendet folgende Konventionen für spezielle Hinweise:

HINWEIS

Ein Hinweis weist auf Inhalte hin, die vor potenziellen Geschäfts- oder Datenverlusten warnen.

Hinweis

Ein Hinweis bietet Informationen, die zum Thema gehören, aber keine zentrale Rolle in diesem Thema spielen. Hinweise können eine Erläuterung, einen Kommentar, eine Verdeutlichung für einen Punkt im Text oder einen Zusatz bieten.

Typografische Konventionen
Data Domain verwendet in diesem Dokument die folgenden Schriftstile:

Tabelle 1 Typografie

Fett	Gibt Bezeichnungen von Benutzeroberflächenelementen an, wie Namen von Fenstern, Dialogfeldern, Schaltflächen, Feldern, Registerkarten, Schlüsseln und Menüpfaden (die vom Benutzer speziell ausgewählt oder angeklickt werden)
Kursiv	Verweist auf die Titel von Veröffentlichungen, auf die im Text Bezug genommen wird.

Tabelle 1 Typografie (Fortsetzung)

`Monospace`	Zeigt Systeminformationen an, z. B.: • Systemcode • Systemausgaben (z. B. Fehlermeldungen oder Skripte) • Pfad- und Dateinamen, Aufforderungen und Syntax • Befehle und Optionen
Kursive Monospace-Schrift	Hebt einen Variablennamen hervor, der durch einen variablen Wert ersetzt werden muss.
`Fette Monospace-Schrift`	Zeigt Text für Benutzereingabe an.
[ ]	Eckige Klammern schließen optionale Werte ein
|	Vertikaler Balken: alternative Auswahlmöglichkeiten (Balken bedeutet „oder“)
{ }	Geschweifte Klammern: Inhalte, die der Benutzer angeben muss (x oder y oder z)
...	Auslassungspunkte verweisen auf unwichtige Informationen, die im Beispiel ausgelassen wurden.

Hier erhalten Sie Hilfe

Auf Support, Produkt- und Lizenzierungsinformationen für Data Domain kann wie folgt zugegriffen werden:

Produktinformationen

Dokumentation, Versionshinweise, Softwareupdates und Informationen zu Data Domain-Produkten finden Sie auf der Onlinesupport-Website unter https://support.emc.com.

Technischer Support

Wechseln Sie zur Online Support-Website und klicken Sie auf „Service-Center“. Es werden daraufhin verschiedene Optionen für die Kontaktaufnahme mit dem technischen Support angezeigt. Um einen Service-Request öffnen zu können, müssen Sie über einen gültigen Support-Vertrag verfügen. Wenden Sie sich an Ihren Vertriebsmitarbeiter, wenn Sie eine gültige Supportvereinbarung benötigen oder Fragen zu Ihrem Konto haben.

Ihre Kommentare

Ihre Vorschläge helfen uns, die Genauigkeit, Gestaltung und Gesamtqualität der Benutzerdokumente zu verbessern. Senden Sie Ihr Feedback zu diesem Dokument an: DPAD.Doc.Feedback@emc.com.

KAPITEL 1

Data Domain-Systemfunktionen und -integration

Inhalt dieses Kapitels:

Revisionsverlauf

Im Revisionsverlauf werden die größten Änderungen am Dokument aufgeführt, die im Zuge der Veröffentlichung von DD OS Version 6.1 vorgenommen wurden.

Tabelle 2 Dokumentrevisionsverlauf

Version	Datum	Beschreibung
04 (6.1.2)	Juli 2018	Diese Version enthält Informationen über diese neuen Funktionen: • Coredump-Dateiaufteilung • Unterstützung für die Verwendung mehrerer Secure Remote Services-Gateways • Open LDAP-Unterstützung für NFSv4-ID-Zuordnung • DD Cloud Tier-Unterstützung für Microsoft Azure Cool Storage und AWS S3-Speicherklassen für unregelmäßigen Zugriff • Unterstützung großer Objektgrößen für DD Cloud Tier • Zertifikatbasierte Anmeldung für Data Domain System Manager • KMIP-Verbesserungen
03 (6.1.1)	Februar 2018	Diese Version enthält Informationen über diese Themen: • Automatic Multi-Streaming (AMS) für MTree-Replikation • Option `crepl-gc-gw-optim` zur Verbesserung des Durchsatzes für die Sammelreplikation • Dateisystembereinigung mit Sammelreplikation

02 (6.1.1)	Januar 2018	Diese Version enthält Informationen über diese neuen Funktionen:
		• Cloud-Tier:
		  ▪ Unterstützung für Azure Government Cloud
		  ▪ Unterstützung für S3 Flexible-Cloudanbieter
		• DD Boost:
		  ▪ Konfigurieren des DD Boost-Authentifizierungsmodus und der Verschlüsselungsstärke auf Systemebene oder Clientebene
		• DD VTL:
		  ▪ Anzeigen und Konfigurieren von VTL-Band in Cloudeinstellungen
		  ▪ Manuelles Migrieren von VTL-Bändern in DD Cloud-Tier

Tabelle 2 Dokumentrevisionsverlauf (Fortsetzung)

Version	Datum	Beschreibung
		▪ Manuelles Abrufen von VTL-Bändern aus DD Cloud-Tier • SNMP: ▪ Anzeigen und Konfigurieren von SNMP-Engine-IDs für SNMPv3 • Systemupgrades: ▪ Anzeigen von Upgradepaketprüfsummen
01 (6.1)	Juni 2017	Diese Version enthält Informationen über diese neuen Funktionen: • Cloud-Tier: ▪ VTL-Band-zu-Cloud ▪ Speicher für gelegentlichen Zugriff ▪ Direkte Wiederherstellung und verbesserte Abruferfahrung ▪ DD SM-Dateiabrufverbesserungen ▪ Unterstützung für gelegentlichen Zugriff für Virtustream • NFS: ▪ Version 4-Unterstützung für DD OS ▪ Neukonzeption der Exporte ▪ Verwaltbarkeitsverbesserungen ▪ Serverskalierungsverbesserungen • Sicherheit: ▪ Key Management Interoperability Protocol(KMIP)-Unterstützung

Übersicht über Data Domain-Systeme

Data Domain-Systeme sind festplattenbasierte Appliances für die Inline-Deduplizierung, die Datensicherheit und Disaster Recovery (DR) für die Unternehmensumgebung bereitstellen.

Auf allen Systemen wird das DD OS (Data Domain Operating System) ausgeführt, das sowohl eine Befehlszeilenoberfläche (CLI) für die Durchführung aller Systemvorgänge als auch die grafische Benutzeroberfläche (GUI) von Data Domain System Manager (DD System Manager) für Konfiguration, Management und Monitoring bereitstellt.

Hinweis

DD System Manager war früher unter dem Namen Enterprise Manager bekannt.

Systeme bestehen aus Appliances, deren Speicherkapazität und Datendurchsatz unterschiedlich sind. Die Systeme werden in der Regel mit Erweiterungsgehäusen konfiguriert, die Speicherplatz hinzufügen.

Data Domain-Systemfunktionen

Data Domain-Systemfunktionen ermöglichen Datenintegrität und eine zuverlässige Wiederherstellung, eine effiziente Ressourcennutzung sowie ein einfaches Management. Mit lizenzierten Funktionen können Sie die Systemfunktionen an Ihre Anforderungen und an Ihr Budget anpassen.

Datenintegrität

Die DD OS Data Invulnerability Architecture™ schützt vor Datenverlust durch Hardware- und Softwareausfälle.

- Bei Schreibvorgängen auf das Laufwerk erstellt das DD OS Prüfsummen und selbstbeschreibende Metadaten für alle empfangenen Daten und speichert diese. Nachdem die Daten auf das Laufwerk geschrieben wurden, berechnet das DD OS die Prüfsummen und Metadaten erneut und überprüft sie.
- Eine append-only-Schreib-Policy schützt vor dem Überschreiben gültiger Daten.
- Nach Abschluss eines Backups wird in einem Validierungsprozess überprüft, welche Daten auf das Laufwerk geschrieben wurden, ob alle Dateisegmente innerhalb des Dateisystems logisch korrekt sind und ob die Daten vor und nach dem Schreibvorgang auf das Laufwerk identisch sind.
- Im Hintergrund wird durch eine Onlineüberprüfung kontinuierlich überprüft, ob die Daten auf den Laufwerken korrekt sind und seit dem letzten Validierungsprozess nicht verändert wurden.
- In den meisten Data Domain-Systemen wird Speicher in einer RAID-6-Konfiguration mit doppelter Parität eingerichtet (2 Paritätslaufwerke). Außerdem umfassen die meisten Konfigurationen ein Hot Spare in jedem Gehäuse, mit Ausnahme der Systeme der DD1xx-Serien, die acht Laufwerke verwenden. Jede Paritäts-Stripe verfügt über Blockprüfsummen, damit die Daten korrekt sind. Prüfsummen werden während der Onlineüberprüfung und während der Datenlesevorgänge vom Data Domain-System kontinuierlich verwendet. Mit doppelter Parität kann das System Fehler auf bis zu zwei Laufwerken gleichzeitig beheben.
- Damit Daten auch während eines Hardware- oder Stromausfalls synchronisiert sind, verwendet das Data Domain-System NVRAM (nicht flüchtigen RAM), um ausstehende I/O-Vorgänge nachzuverfolgen. Eine NVRAM-Karte mit vollständig aufgeladenen Batterien (der typische Zustand) kann Daten über einen Zeitraum von mehreren Stunden aufbewahren, welcher von der verwendeten Hardware festgelegt wird.
- Wenn Daten bei einem Wiederherstellungsvorgang zurückgelesen werden, verwendet das DD OS mehrere Konsistenzprüfungen, um zu überprüfen, ob die wiederhergestellten Daten korrekt sind.
- Beim Schreiben auf SSD-Cache führt DD OS Folgendes durch:
  - Erstellt eine SL-Prüfsumme für jeden im Cache gespeicherten Datensatz zum Erkennen von Beschädigungen an Cachedaten. Diese Prüfsumme wird für jeden gelesenen Cache validiert.

- Behandelt Beschädigungen an Cachedaten als Cachefehler, wodurch kein Datenverlust verursacht wird. Aus diesem Grund können Cacheclients die neueste Kopie der Daten ohne einen anderen Backupmechanismus wie NVRAM oder HDD nicht speichern.
- Macht Inlineverifizierung von Cacheschreibvorgängen überflüssig, da Cacheclients fehlgeleitete und verlorene Schreibvorgänge erkennen und bearbeiten können. Hierdurch wird auch I/O-Bandbreite eingespart.
- Macht SSD-Scrubbing des Dateisystems überflüssig, da sich die Daten im Cache häufig ändern und bereits durch SAS Background Media Scan (BMS) bereinigt wurden.

Datendeduplizierung

Bei der DD OS-Datendeduplizierung werden redundante Daten während eines Backups erkannt und eindeutige Daten werden nur einmal gespeichert.

Die Speicherung von eindeutigen Daten ist für die Backupsoftware nicht sichtbar und erfolgt unabhängig vom Datenformat. Daten können strukturiert sein, z. B. Datenbanken, oder unstrukturiert, z. B. Textdateien. Daten können aus Dateisystemen oder von Raw Volumes stammen.

Typische Deduplizierungsverhältnisse sind im Durchschnitt 20 zu 1 über viele Wochen. Bei diesem Verhältnis wird davon ausgegangen, dass es wöchentliche komplette Backups und tägliche inkrementelle Backups gibt. Ein Backup, das viele doppelte oder ähnliche Dateien enthält (mehrmals kopierte Dateien mit wenig Änderungen), profitiert am meisten von der Deduplizierung.

Je nach Backupvolumen, Größe, Aufbewahrungsfrist und Änderungsrate kann die Menge der Deduplizierung variieren. Die beste Deduplizierung geschieht mit Backupvolumengrößen von mindestens 10 MiB (MiB ist das Base 2-Äquivalent von MB).

Um den vollen Nutzen aus mehreren Data Domain-Systemen zu ziehen, muss ein Standort mit mehr als einem Data Domain-System konsistent dasselbe Clientsystem oder dieselben Daten in dasselbe Data Domain-System sichern. Wenn beispielsweise ein vollständiges Backup aller Vertriebsdaten auf Data Domain-System A geht, wird eine maximale Deduplizierung erreicht, wenn die inkrementellen Backups und die zukünftigen kompletten Backups der Vertriebsdaten ebenfalls auf das Data Domain-System A gehen.

Wiederherstellungsvorgänge

Dateiwiederherstellungsvorgänge erzeugen nur geringfügige oder überhaupt keine Konflikte mit Backup- oder anderen Wiederherstellungsvorgängen.

Beim Backup auf Festplatten in einem Data Domain-System sind inkrementelle Backups immer zuverlässig und es kann einfach auf sie zugegriffen werden. Mit Bandbackups sind für den Wiederherstellungsvorgang ggf. mehrere Bänder erforderlich, die inkrementelle Backups enthalten. Je mehr inkrementelle Backups an einem Standort auf mehreren Bändern gespeichert werden, desto zeitaufwendiger und riskanter ist zudem der Wiederherstellungsvorgang. Ein ungültiges Band kann die Wiederherstellung unmöglich machen.

Mit einem Data Domain-System können Sie vollständige Backups ohne die Beeinträchtigung, redundante Daten speichern zu müssen, häufiger durchführen. Im Gegensatz zu Bandlaufwerksbackups können mehrere Prozesse gleichzeitig auf ein Data Domain-System zugreifen. Mit einem Data Domain-System kann Ihr Standort sichere, benutzergesteuerte Wiederherstellungsvorgänge einzelner Dateien anbieten.

Data Domain Replicator

Der Data Domain Replicator konfiguriert und managt die Replikation von Backupdaten zwischen den beiden Data Domain-Systemen.

Ein DD Replicator-Paar besteht aus einem Quell- und einem Zielsystem und repliziert einen ganzen Datensatz oder ein ganzes Verzeichnis vom Quellsystem zum Zielsystem. Ein einzelnes Data Domain-System kann ein Teil von mehreren Replikationspaaren sein und als Quelle für ein oder mehrere Paare sowie als Ziel für ein oder mehrere Paare dienen. Nachdem die Replikation gestartet wurde, sendet das Quellsystem automatisch alle neuen Backupdaten an das Zielsystem.

Multipath und Lastenausgleich

In einer Fibre-Channel-Multipath-Konfiguration werden zwischen einem Data Domain-System und einem Backupserver oder einem Zielarray für Backups mehrere Pfade eingerichtet. Wenn mehrere Pfade vorhanden sind, verteilt das System die Backuplast automatisch auf die verfügbaren Pfade.

Zum Erstellen einer Multipath-Konfiguration sind mindestens zwei HBA-Ports erforderlich. Wenn eine Verbindung mit einem Backupserver vorhanden ist, werden alle HBA-Ports im Multipath mit einem eigenen Port auf dem Backupserver verbunden.

Hohe Verfügbarkeit

Die HA-Funktion (hohe Verfügbarkeit) ermöglicht es Ihnen, zwei Data Domain-Systeme als Aktiv-Stand-by-Paar zu konfigurieren und so Redundanz bei einem Systemausfall bereitzustellen. HA synchronisiert die aktiven und Stand-by-Systeme, sodass bei Ausfall des aktiven Node aufgrund von Hardware- oder Softwareproblemen der Stand-by-Node übernehmen und dort fortfahren kann, wo der ausgefallene Node aufgehört hat.

Die HA-Funktion:

- Unterstützt Failover von Backup-, Wiederherstellungs-, Replikations- und Managementservices in einem System mit zwei Nodes. Automatisches Failover erfordert keinen Benutzereingriff.
- Bietet ein vollständig redundantes Design ohne Single-Point-of-Failure innerhalb des Systems bei Konfiguration gemäß den Empfehlungen.
- Stellt ein Aktiv-Stand-by-System ohne Performanceverlust beim Failover bereit.
- Führt das Failover innerhalb von 10 Minuten für die meisten Vorgänge durch. CIFS, DD VTL und NDMP müssen manuell neu gestartet werden.

  Hinweis

  Die Recovery von DD Boost-Anwendungen kann länger als 10 Minuten dauern, da die Boost-Anwendungs-Recovery erst beginnen kann, wenn das DD-Server-Failover abgeschlossen ist. Darüber hinaus kann die Boost-Anwendungs-Recovery erst starten, wenn die Anwendung die Boost-Bibliothek aufruft. Gleichermaßen kann die NFS-Recovery zusätzlich Zeit erfordern.

- Unterstützt einfaches Management und einfache Konfiguration über DD OS-CLIs.
- Gibt Warnmeldungen für fehlerhafte Hardware aus.
- Behält Performance und Skalierbarkeit eines Node in einer HA-Konfiguration im normalen und heruntergestuften Modus bei.

- Unterstützt den gleichen Funktionssatz wie eigenständige DD-Systeme.

  Hinweis

  DD Extended Retention und vDisk werden nicht unterstützt.

- Unterstützt Systeme mit allen SAS-Laufwerken. Dies schließt Legacy-Systeme ein, die auf Systeme mit allen SAS-Laufwerken aktualisiert wurden.

  Hinweis

  Im Überblick über die Hardware und in den Installationshandbüchern für Data Domain-Systeme, die HA unterstützen, wird beschrieben, wie ein neues HA-System zu installieren ist. In *Upgrade von Data Domain mit einem Node auf HA* wird beschrieben, wie ein Upgrade eines vorhandenen Systems auf ein HA-Paar durchgeführt wird.

- Hat keine Auswirkung auf die mögliche Skalierung des Produkts.
- Unterstützt unterbrechungsfreie Softwareupdates.

HA wird auf den folgenden Data Domain-Systemen unterstützt:

- DD6800
- DD9300
- DD9500
- DD9800

HA-Architektur

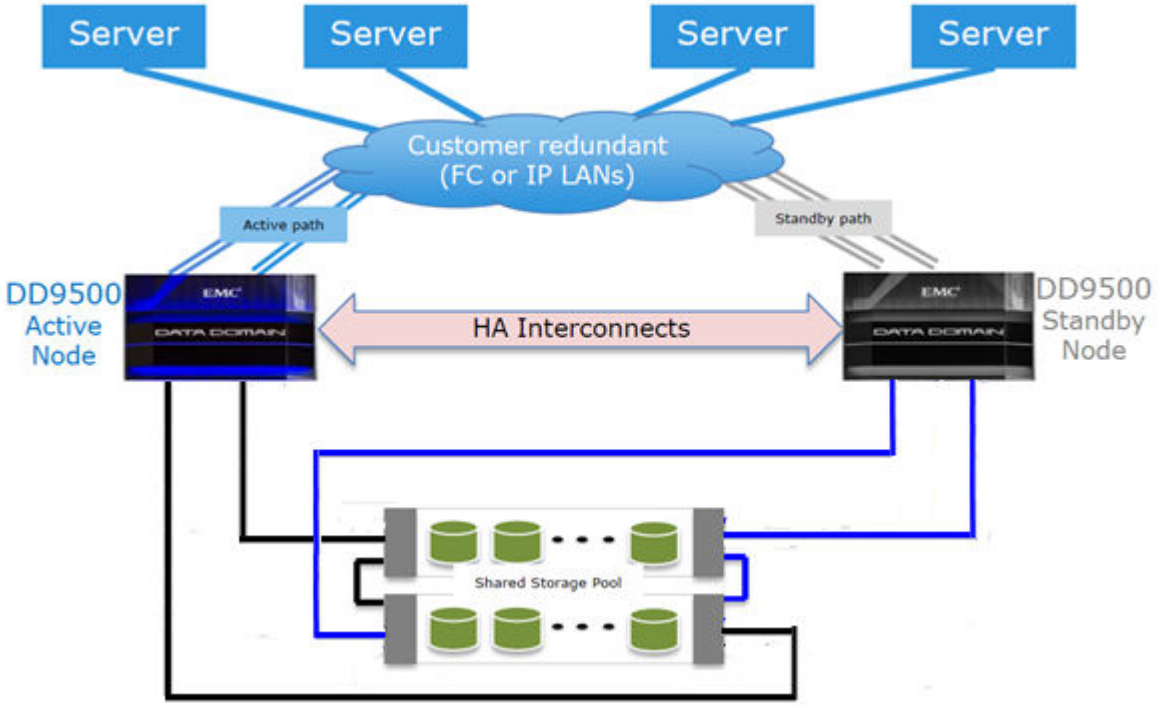
HA-Funktionalität ist für IP- und Fibre-Channel-Verbindungen verfügbar. Beide Nodes müssen Zugriff auf dieselben IP-Netzwerke, Fibre-Channel-SANs sowie Hosts haben, um hohe Verfügbarkeit für die Umgebung zu erreichen.

Über IP-Netzwerke verwendet HA Floating IP-Adressen für den Datenzugriff auf das Data Domain-HA-Paar, unabhängig davon, welcher physische Node der aktive Node ist.

Über Fibre-Channel-SANs verwendet HA NPIV, um die Fibre-Channel-WWNs zwischen Nodes zu verschieben, sodass die Fibre-Channel-Initiatoren nach einem Failover Verbindungen erneut herstellen können.

In Abbildung 1 auf Seite 28 ist die HA-Architektur dargestellt.

Abbildung 1 HA-Architektur



Zufällige I/O-Verarbeitung

Die zufälligen in DD OS enthaltenen I/O-Optimierungen bieten verbesserte Performance für Anwendungen und Anwendungsbeispiele, die größere Mengen der zufälligen Lese- und Schreibvorgänge als sequenzielle Lese- und Schreibvorgänge erzeugen.

DD OS wurde zur Verarbeitung von Workloads optimiert, die aus zufälligen Lese- und Schreibvorgängen, wie z. B. sofortiger Zugriff auf virtuelle Maschinen und sofortiger Wiederherstellung, und kontinuierlichen inkrementellen von Anwendungen wie Avamar erzeugten Backups bestehen. Diese Optimierungen:

- verbessern die zufälligen Lese- und Schreiblatenzen.
- verbessern die Benutzer-IOPS mit kleineren Lesegrößen.
- unterstützen gleichzeitige I/O-Vorgänge innerhalb eines einzigen Streams.
- bieten den Spitzenlesedurchsatz und Spitzenschreibdurchsatz bei kleineren Streams.

Hinweis

Die maximale Anzahl für zufällige I/O-Streams ist auf die maximale Anzahl an Wiederherstellungsstreams eines Data Domain-Systems beschränkt.

Die zufälligen I/O-Verbesserungen ermöglichen dem Data Domain-System die Unterstützung der Funktion zum sofortigen Zugriff/zur sofortigen Wiederherstellung für Backupanwendungen wie Avamar und Networker.

Systemadministratorzugriff

Systemadministratoren können zur Konfiguration oder für das Management über eine Befehlszeilenoberfläche oder über eine grafische Benutzeroberfläche auf das System zugreifen.

- DD OS-CLI: Eine Befehlszeilenoberfläche, die über eine serielle Konsole oder über Ethernetverbindungen mithilfe von SSH oder Telnet verfügbar ist. CLI-Befehle werden zum Durchführen der Erstkonfiguration des Systems und von Änderungen von einzelnen Einstellungen sowie zum Anzeigen des Betriebsstatus des Systems verwendet.
- DD System-Manager: Eine browserbasierte grafische Benutzeroberfläche, die über Ethernetverbindungen verfügbar ist. Verwenden Sie DD System Manager, um die Erstkonfiguration des Systems durchzuführen, Konfigurationsänderungen nach der Erstkonfiguration vorzunehmen, System- und Komponentenstatus anzuzeigen und Berichte und Diagramme zu erzeugen.

Hinweis

Einige Systeme unterstützen den Zugriff mithilfe einer Tastatur und einem Monitor, die direkt an dem System angeschlossen sind.

Lizenzierte Funktionen

Dank der Funktionslizenzen ist es möglich, dass Sie nur die Funktionen erwerben, die Sie tatsächlich nutzen möchten. Einige Beispiele für Funktionen, die eine Lizenz erfordern: DD Extended Retention, DD Boost und die Funktion zur Erweiterung der Speicherkapazität.

Wenden Sie sich an Ihren Vertriebsmitarbeiter, um Informationen zum Erwerb von lizenzierten Funktionen zu erhalten.

Tabelle 3 Funktionen, für die Lizenzen erforderlich sind

Funktionsname	Lizenzname in Software	Beschreibung
Data Domain ArchiveStore	ARCHIVESTORE	Lizenziert Data Domain-Systeme für die Archivverwendung, z. B. Datei- und E-Mail-Archivierung, File Tiering sowie Inhalts- und Datenbankarchivierung.
Data Domain Boost	DDBOOST	Ermöglicht die Verwendung eines Data Domain-Systems mit den folgenden Anwendungen: Avamar, NetWorker, Oracle RMAN, Quest vRanger, Symantec Veritas NetBackup (NBU) und Backup Exec. Für die DD Boost-Funktion Managed File Replication (MFR) ist außerdem die DD Replicator-Lizenz erforderlich.
Data Domain Capacity on Demand	CONTROLLER-COD	Ermöglicht nach Bedarf die Erweiterung der Kapazität für 4-TB-DD2200-Systeme auf 7,5 TB oder 13,18 TB. Für die Erweiterung auf 13,18 TB ist zudem die Lizenz EXPANDED-STORAGE erforderlich.

Tabelle 3 Funktionen, für die Lizenzen erforderlich sind (Fortsetzung)

Funktionsname	Lizenzname in Software	Beschreibung
Data Domain Cloud Tier	CLOUDTIER-CAPACITY	Ermöglicht einem Data Domain-System, Daten zur langfristigen Aufbewahrung vom aktiven Tier zu einem kostengünstigen Objektspeicher mit hoher Kapazität in der Public, Private oder Hybrid Cloud zu verschieben.
Data Domain Encryption	ENCRYPTION	Ermöglicht die Verschlüsselung von Daten auf Systemlaufwerken oder externen Laufwerken während der Speicherung und die Sperrung, wenn das System an einen anderen Speicherort verschoben wird.
Data Domain Expansion Storage	EXPANDED-STORAGE	Ermöglicht die Erweiterung des Data Domain-Systemspeichers über die im Basissystem bereitgestellte Größe.
Data Domain Extended Retention (ehemals DD Archiver)	EXTENDED-RETENTION	Lizenziert die DD Extended Retention-Speicherfunktion.
Data Domain I/OS (für IBM i-Betriebsumgebungen)	I/OS	Eine I/OS-Lizenz ist erforderlich, wenn DD VTL zur Sicherung von Systemen in der IBM i-Betriebsumgebung verwendet wird. Wenden Sie diese Lizenz an, bevor Sie virtuelle Bandlaufwerke zu Bibliotheken hinzufügen.
Data Domain Replicator	REPLICATION	Fügt DD Replicator zur Datenreplikation zwischen Data Domain-Systemen hinzu. Auf jedem System ist eine Lizenz erforderlich.
Data Domain Retention Lock Compliance Edition	RETENTION-LOCK-COMPLIANCE	Erfüllt die strengsten Vorschriften zur Datenaufbewahrung seitens Regulierungsstandards, z. B. SEC17a-4.
Data Domain Retention Lock Governance Edition	RETENTION-LOCK-GOVERNANCE	Schützt ausgewählte Dateien vor Änderung und Löschung, bevor eine bestimmte Aufbewahrungsfrist abgelaufen ist.
Data Domain Shelf Capacity-Active Tier	CAPACITY-ACTIVE	Ermöglicht einem Data Domain-System, die Speicherkapazität des aktiven Tier mit einem zusätzlichen Gehäuse oder einer Spindel in einem Gehäuse zu erweitern.
Data Domain Shelf Capacity-Archive Tier	CAPACITY-ARCHIVE	Ermöglicht einem Data Domain-System, die Speicherkapazität des Archiv-Tier mit einem zusätzlichen Gehäuse oder einer Spindel in einem Gehäuse zu erweitern.
Data Domain Storage Migration	STORAGE-MIGRATION-FOR-DATADOMAIN-SYSTEMS	Ermöglicht die Migration von Daten von einem Gehäuse auf ein anderes für den Austausch von älteren Gehäusen mit niedrigerer Kapazität.

Tabelle 3 Funktionen, für die Lizenzen erforderlich sind (Fortsetzung)

Funktionsname	Lizenzname in Software	Beschreibung
Data Domain Virtual Tape Library (DD VTL)	Virtuelle Bandbibliothek	Ermöglicht die Verwendung eines Data Domain-Systems als virtuelle Bandbibliothek über ein Fibre Channel-Netzwerk. Mit dieser Lizenz wird auch die Funktion „NDMP Tape Server“ aktiviert, für die bisher eine separate Lizenz erforderlich war.
HA	HA-AKTIV-PASSIV	Aktiviert die HA-Funktion in einer Aktiv-Stand-by-Konfiguration. Sie müssen nur eine HA-Lizenz erwerben; die Lizenz wird auf dem aktiven Node ausgeführt und auf dem Stand-by-Node gespiegelt.

Integration der Speicherumgebung

Data Domain-Systeme lassen sich problemlos in vorhandene Rechenzentren integrieren.

- Alle Data Domain-Systeme können als Speicherziele für führende Backup- und Archivierungsanwendungen mithilfe von NFS-, CIFS-, DD Boost- oder DD VTL-Protokollen konfiguriert werden.
- Suchen Sie nach *Kompatibilitätsdokumenten* unter https://support.emc.com, um Informationen zu den Anwendungen zu erhalten, die mit den verschiedenen Konfigurationen verwendet werden können.
- Mehrere Backupserver können ein Data Domain-System gemeinsam nutzen.
- Ein Data Domain-System kann mehrere gleichzeitige Backup- und Wiederherstellungsvorgänge verarbeiten.
- Mehrere Data Domain-Systeme können mit einem oder mehreren Backupservern verbunden werden.

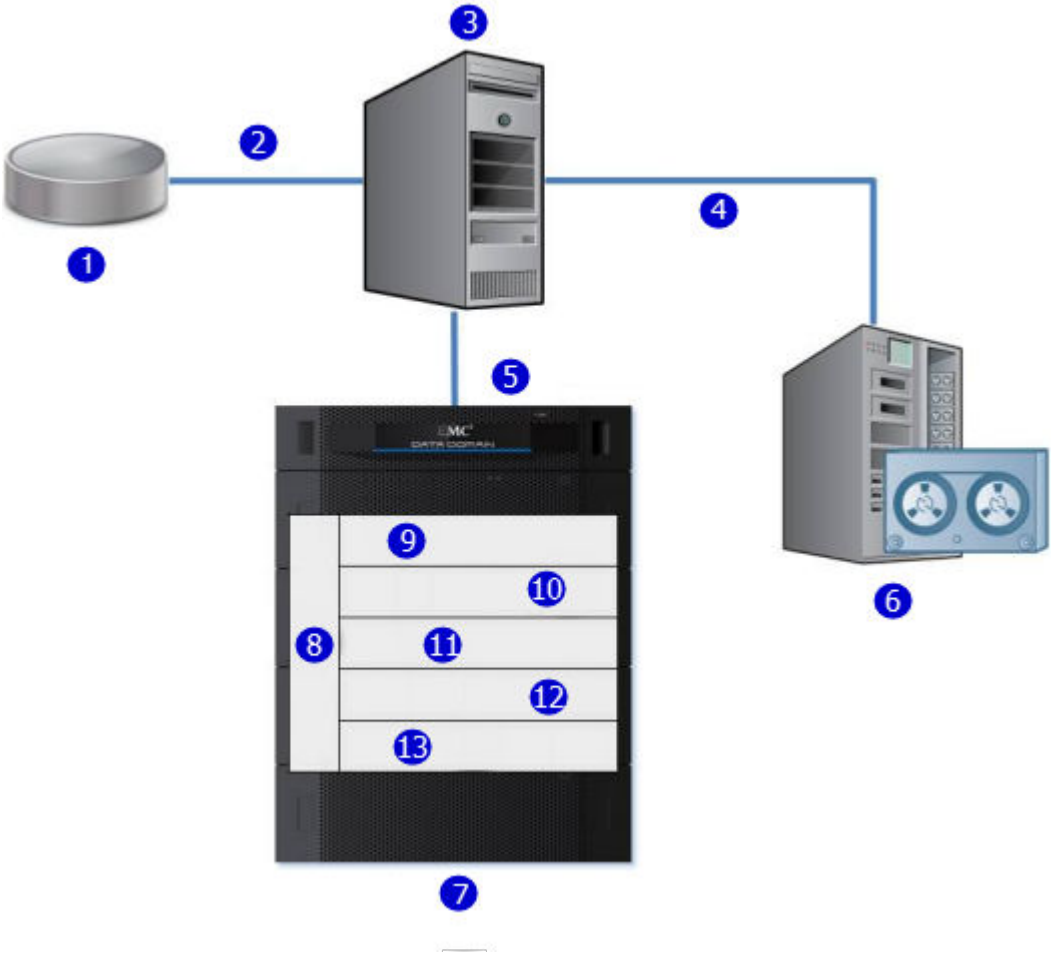
Zur Verwendung als ein Backupziel kann ein Data Domain-System entweder als Festplattenspeichereinheit mit einem Dateisystem konfiguriert werden, auf das über eine Ethernetverbindung zugegriffen wird, oder als virtuelle Bandbibliothek, auf die über eine Fibre-Channel-Verbindung zugegriffen wird. Mit der DD VTL-Funktion können Data Domain-Systeme in Umgebungen integriert werden, in denen bereits eine Backupsoftware für Bandbackups konfiguriert ist. Dadurch werden Unterbrechungen minimiert.

Die Konfiguration wird sowohl in DD OS durchgeführt, wie in den entsprechenden Abschnitten dieses Leitfadens beschrieben, als auch in der Backupanwendung, wie in den Administratorhandbüchern der Backupanwendung und den anwendungsbezogenen Data Domain-Leitfäden und technischen Hinweisen beschrieben.

- Alle Backupanwendungen können als NFS- oder CIFS-Dateisystem auf dem Data Domain-Festplattengerät auf ein Data Domain-System zugreifen.
- Die folgenden Anwendungen können über die DD Boost-Schnittstelle mit einem Data Domain-System verwendet werden: Avamar, NetWorker, Oracle RMAN, Quest vRanger, Symantec Veritas NetBackup (NBU) und Backup Exec.

In der folgenden Abbildung ist ein Data Domain-System dargestellt, das in eine vorhandene Basisbackupkonfiguration integriert ist.

Abbildung 2 In eine Speicherumgebung integriertes Data Domain-System



1. Primärer Speicher
2. Ethernet
3. Backupserver
4. SCSI/Fibre Channel
5. Gigabit Ethernet oder Fibre Channel
6. Bandsystem
7. Data Domain-System
8. Management
9. NFS/CIFS/DD VTL/DD Boost
10. Datenüberprüfung
11. Dateisystem
12. Globale Deduplizierung und Komprimierung
13. RAID

Wie in Abbildung 2 auf Seite 32 gezeigt, fließen die Daten an ein Data Domain-System über eine Ethernet- oder eine Fibre-Channel-Verbindung. Die Datenüberprüfungsprozesse beginnen unmittelbar und werden fortgesetzt, während sich die Daten auf dem Data Domain-System befinden. Im Dateisystem deduplizieren

und komprimieren die DD OS Global Compression™-Algorithmen die Daten für den Speicher. Die Daten werden dann an das RAID-Festplattensubsystem gesendet. Wenn ein Wiederherstellungsvorgang erforderlich ist, werden die Daten aus dem Data Domain-Speicher abgerufen, dekomprimiert, auf Konsistenz überprüft und über Ethernet (für NFS, CIFS, DD Boost) oder Fibre Channel (für DD VTL und DD Boost) an die Backupserver übertragen.

DD OS kann relativ große Streams mit sequenziellen Daten aus der Backupsoftware aufnehmen und ist für einen hohen Durchsatz, eine kontinuierliche Datenüberprüfung und eine hohe Komprimierung optimiert. DD OS kann auch die zahlreichen kleineren Dateien im Nearline-Speicher (DD ArchiveStore) aufnehmen.

Die Performance des Data Domain-Systems ist am besten, wenn Daten von Anwendungen gespeichert werden, die nicht speziell Backupsoftware unter den folgenden Bedingungen sind.

- Die Daten werden als sequenzielle Schreibvorgänge an das Data Domain-System gesendet (keine Überschreibung).
- Die Daten werden weder komprimiert noch verschlüsselt, bevor sie an das Data Domain-System gesendet werden.

KAPITEL 2

Erste Schritte

Dieses Kapitel enthält die folgenden Themen:

DD System Manager – Übersicht

DD System Manager ist eine browserbasierte grafische Benutzeroberfläche, die über Ethernetverbindungen für das Management eines Systems an jedem beliebigen Standort verfügbar ist. Mit DD System Manager erhalten Sie eine einzige, konsolidierte Managementoberfläche, die die Konfiguration und das Monitoring mehrerer Systemfunktionen und Systemeinstellungen ermöglicht.

Hinweis

Über Data Domain Management Center können Sie mehrere Systeme über ein einziges Browserfenster managen.

DD System Manager bietet Echtzeitdiagramme und Tabellen, mit denen Sie den Status der Hardwarekomponenten des Systems und der konfigurierten Funktionen überwachen können.

Darüber hinaus ist ein Befehlssatz, der sämtliche Systemfunktionen ausführt, für Benutzer auf der Befehlszeilenoberfläche (CLI) verfügbar. Mit Befehlen werden Systemeinstellungen konfiguriert und der Status der Systemhardware, die Funktionskonfiguration und Vorgänge angezeigt.

Die Befehlszeilenoberfläche ist über eine serielle Konsole oder über eine Ethernetverbindung mit SSH oder Telnet verfügbar.

Hinweis

Einige Systeme unterstützen den Zugriff mithilfe einer Tastatur und einem Monitor, die direkt an dem System angeschlossen sind.

An- und Abmelden bei DD System Manager

Melden Sie sich über einen Browser bei DD System Manager an.

Vorgehensweise

1. Öffnen Sie einen Webbrowser und geben Sie die IP-Adresse oder den Hostnamen ein, um eine Verbindung zu DD System Manager herzustellen. Folgende Eingaben sind möglich:
   - Einen vollständig qualifizierten Domainnamen, z. B. `http://dd01.emc.com`
   - Einen Hostnamen, z. B. `http://dd01`
   - Eine IP-Adresse, z. B. `http://10.5.50.5`

   Hinweis

   DD System Manager verwendet HTTP-Port 80 und HTTPS-Port 443. Da sich Ihr Data Domain-System hinter einer Firewall befindet, müssen Sie möglicherweise Port 80 aktivieren, wenn Sie HTTP verwenden, oder Port 443, wenn HTTPS verwendet wird, um das System zu erreichen. Die Portnummern können problemlos geändert werden, wenn Sicherheitsanforderungen dies erfordern.

2. Klicken Sie für eine sichere HTTPS-Anmeldung auf **Secure Login**.

Für die sichere Anmeldung mit HTTPS ist ein digitales Zertifikat erforderlich, um die Identität des DD OS-Systems zu validieren und eine bidirektionale Verschlüsselung zwischen DD System Manager und einem Browser zu unterstützen. DD OS enthält ein selbstsigniertes Zertifikat und mit DD OS können Sie ein eigenes Zertifikat importieren.

Die Standardeinstellungen der meisten Browser akzeptieren nicht automatisch ein selbstsigniertes Zertifikat. Dadurch wird nicht verhindert, dass Sie das selbstsignierte Zertifikat verwenden. Es bedeutet lediglich, dass Sie bei jeder Durchführung einer sicheren Anmeldung auf eine Warnmeldung antworten oder das Zertifikat in Ihrem Browser installieren müssen. Anweisungen zur Installation des Zertifikats in Ihrem Browser finden Sie in Ihrer Browserdokumentation.

3. Geben Sie den Ihren zugewiesenen Benutzernamen und das Ihnen zugewiesene Passwort ein.

Hinweis

Der anfängliche Benutzername lautet *sysadmin*. Das anfängliche Passwort entspricht der Seriennummer des Systems. Informationen zum Einrichten eines neuen Systems finden Sie im *Data Domain Operating System Initial Configuration Guide*.

4. Klicken Sie auf **Log In**.

   Wenn dies das erste Mal ist, das Sie sich angemeldet haben, wird die Ansicht "Home" im Informationsbereich angezeigt.

Hinweis

Wenn Sie 4-mal nacheinander ein falsches Passwort eingeben, wird der angegebene Benutzername 120 Sekunden lang vom System gesperrt. Die Zahl der Anmeldeversuche und die Sperrdauer sind konfigurierbar und können auf Ihrem System abweichen.

Hinweis

Wenn dies das erste Mal ist, dass Sie sich anmelden, müssen Sie Ihr Passwort evtl. ändern. Wenn der Systemadministrator Ihren Benutzernamen für eine Passwortänderung konfiguriert hat, müssen Sie das Passwort ändern, bevor Sie Zugriff auf DD System Manager haben.

5. Klicken Sie zum Abmelden auf die Schaltfläche "Log Out" im DD System Manager-Banner.

   Wenn Sie sich abmelden, zeigt das System die Anmeldeseite mit einer Meldung an, dass Ihre Abmeldung abgeschlossen ist.

Anmelden mit einem Zertifikat

Als Alternative zur Anmeldung mit einem Benutzernamen und Passwort können Sie sich bei DD System Manager mit einem Zertifikat von einer Zertifizierungsstelle (Certificate Authority, CA) anmelden.

Um sich mit einem Zertifikat anzumelden, müssen Sie über Autorisierungsberechtigungen für das Data Domain-System verfügen und das Data Domain-System muss dem CA-Zertifikat vertrauen. Ihr Benutzername muss im Feld „Common Name“ im Zertifikat angegeben werden.

Vorgehensweise

1. Stellen Sie sicher, dass Sie über ein Benutzerkonto auf dem Data Domain-System verfügen.

   Sie können ein lokaler Benutzer oder ein Namensservice-Benutzer (NIS/AD) sein. Für einen Namensservice-Benutzer muss Ihre Gruppe-zu-Rolle-Zuordnung auf dem Data Domain-System konfiguriert sein.

2. Verwenden Sie den folgenden CLI-Befehl, um den öffentlichen Schlüssel von der Zertifizierungsstelle zu importieren, die das Zertifikat ausgestellt hat: `adminaccess certificate import ca application login-auth`.

3. Laden Sie das Zertifikat im PKCS12-Format in Ihrem Browser.

   Sobald dem CA-Zertifikat vom Data Domain-System vertraut wird, wird der Link **Log in with certificate** auf dem HTTPS-Anmeldebildschirm angezeigt.

4. Klicken Sie auf **Log in with certificate** und wählen Sie das Zertifikat aus der Liste der Zertifikate, das vom Browser angefordert wird.

Ergebnisse

Das Data Domain-System validiert das Benutzerzertifikat mit dem vertrauenswürdigen Speicher. Basierend auf den Autorisierungsberechtigungen für Ihr Konto wird eine System Manager-Sitzung für Sie erstellt.

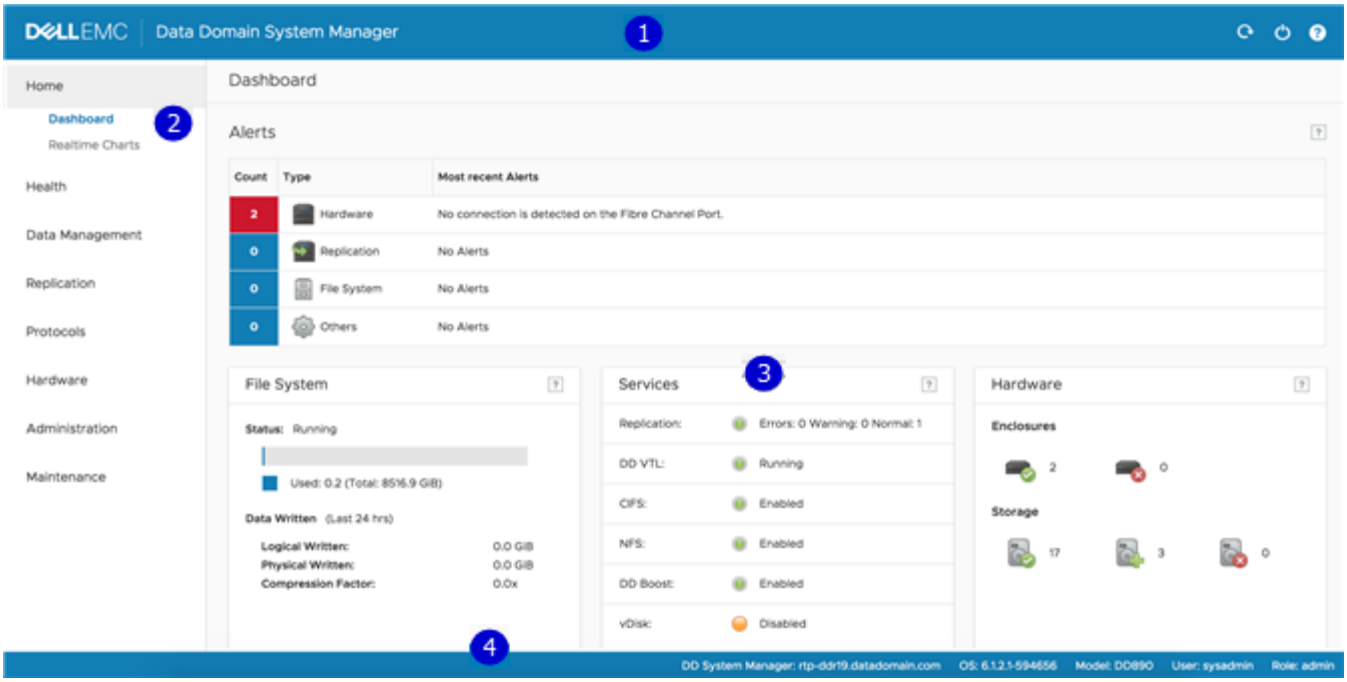
Die Benutzeroberfläche von DD System Manager

Die Benutzeroberfläche von DD System Manager enthält auf den meisten Seiten allgemeine Elemente, mit deren Hilfe Sie durch die Konfigurations- und Anzeigeoptionen navigieren und eine kontextsensitive Hilfe anzeigen können.

Seitenelemente

Die wichtigsten Seitenelemente sind der Banner, der Navigationsbereich, die Informationsbereiche und die Fußzeile.

Abbildung 3 Komponenten der DD System Manager-Seite



1. Banner
2. Navigationsbereich
3. Informationsbereiche
4. Fußzeile

Banner

Das DD System Manager-Banner zeigt den Programmnamen und die Schaltflächen für **Refresh**, **Log Out** und **Help** an.

Navigationsbereich

Der Navigationsbereich zeigt die Menüoptionen der obersten Ebene, die Sie verwenden können, um die Systemkomponente oder Aufgabe zu identifizieren, die Sie managen möchten.

Der Navigationsbereich zeigt die wichtigsten zwei Ebenen des Navigationssystems. Klicken Sie auf alle Titel der obersten Ebene, um die Titel der zweiten Ebene anzuzeigen. Registerkarten und Menüs im Informationsbereich bieten zusätzliche Navigationssteuerelemente.

Informationsbereich

Der Informationsbereich zeigt Informationen und Steuerelemente zum ausgewählten Element im Navigationsbereich an. Im Informationsbereich finden Sie Informationen zum Systemstatus. Ferner können Sie hier das System konfigurieren.

Abhängig von der Funktion oder Aufgabe, die Sie im Navigationsbereich ausgewählt haben, werden im Informationsbereich möglicherweise eine Registerkartenleiste, Themenbereiche, Steuerungselemente für die Tabellenansicht und das Menü „More Tasks“ angezeigt.

Registerkartenleiste
Registerkarten bieten Zugriff auf verschiedene Aspekte des Themas, das im Navigationsbereich ausgewählt wurde.

Themenbereiche
Themenbereiche unterteilen den Informationsbereich in Abschnitte, die verschiedene Aspekte des ausgewählten Themas im Navigationsbereich oder in der übergeordneten Registerkarte darstellen.

Für Systeme mit hoher Verfügbarkeit (HA) gibt die Registerkarte „HA Readiness“ im System Manager-Dashboard an, ob das HA-System für das Failover vom aktiven Node zum Stand-by-Node bereit ist. Klicken Sie auf **HA Readiness**, um zum Bereich **High Availability** unter **HEALTH** zu navigieren.

Optionen für die Arbeit mit der Tabellenansicht
Viele der Ansichten mit Tabellen von Elementen enthalten Steuerelemente zum Filtern, Navigieren und Sortieren der Informationen in der Tabelle.

So verwenden Sie gängige Steuerungselemente für Tabellen:

- Klicken Sie auf das rautenförmige Symbol in einer Spaltenüberschrift, um die Sortierreihenfolge der Elemente in der Spalte umzukehren.
- Klicken Sie auf die Pfeile **<** und **>** unten rechts in der Ansicht, um sich in den Seiten vor- und zurückzubewegen. Um zum Anfang einer Reihe von Seiten zu springen, klicken Sie auf **<**. Um zum Ende zu springen, klicken Sie auf **>**.
- Verwenden Sie die Bildlaufleiste, um alle Elemente in einer Tabelle anzuzeigen.
- Geben Sie Text in das Feld **Filter By** ein, um nach Elementen zu suchen oder die Auflistung dieser Elemente zu priorisieren.
- Klicken Sie auf **Update**, um die Liste zu aktualisieren.
- Klicken Sie auf **Reset**, um zur ursprünglichen Auflistung zurückzukehren.

Menü „More Tasks“
Einige Seiten verfügen über ein Menü „More Tasks“ oben rechts in der Ansicht, das Befehle enthält, die sich auf die aktuelle Ansicht beziehen.

Fußzeile

Die DD System Manager-Fußzeile zeigt wichtige Informationen über die Managementsitzung.

Folgende Informationen werden im Banner angezeigt.

- Hostname des Systems
- DD OS-Version
- Die Modellnummer des ausgewählten Systems
- Den Benutzername und die Rolle des derzeit angemeldeten Benutzers

Hilfe-Schaltflächen

Hilfe-Schaltflächen werden mit einem Fragezeichen (?) im Banner, im Titel vieler Bereiche des Informationsbereichs und in vielen Dialogfeldern angezeigt. Klicken Sie auf die Hilfe-Schaltfläche, um ein Hilfefenster zur aktuell verwendeten Funktion anzuzeigen.

Im Hilfefenster werden Schaltflächen für den Inhalt und die Navigation über der Hilfe angezeigt. Klicken Sie auf die Schaltfläche für den Inhalt, um den Inhalt der Leitfäden

und eine Suchschaltfläche anzuzeigen, mit der Sie die Hilfe durchsuchen können. Verwenden Sie die Pfeilschaltflächen, um der Reihe durch die Hilfethemen zu blättern.

Anwenderlizenzvereinbarung

Wenn Sie die Anwenderlizenzvereinbarung (EULA, End User License Agreement) anzeigen möchten, wählen Sie **Maintenance** > **System** > **View EULA**.

Konfigurieren des Systems mit dem Konfigurationsassistenten

Es gibt zwei Assistenten, einen DD System Manager-Konfigurationsassistenten und einen CLI-Konfigurationsassistenten. Die Konfigurationsassistenten führen Sie durch eine vereinfachte Konfiguration Ihres Systems, um Ihr System rasch betriebsbereit zu machen.

Nachdem Sie die Basiskonfiguration mit einem Assistenten abgeschlossen haben, können Sie zusätzliche Konfigurationssteuerelemente in DD System Manager und der Befehlszeilenoberfläche verwenden, um Ihr System weiter zu konfigurieren.

Hinweis

Das folgenden Verfahren beschreibt, wie Sie den DD System Manager-Konfigurationsassistenten starten und die Erstkonfiguration des Systems vornehmen. Eine Anleitung zum Ausführen des Konfigurationsassistenten beim Systemstart finden Sie im *Data Domain Operating System Initial Configuration Guide*.

Hinweis

Wenn Sie Ihr System für HA konfigurieren möchten, müssen Sie diesen Vorgang mithilfe des CLI-Konfigurationsassistenten ausführen. Weitere Informationen finden Sie im *Data Domain DD9500/DD9800 Hardware Overview and Installation Guide* und im *Data Domain Operating System Initial Configuration Guide*.

Vorgehensweise

1. Wählen Sie **Maintenance** > **System** > **Configure System** aus.
2. Mithilfe der Steuerelemente unten im Dialogfeld des Konfigurationsassistenten können Sie festlegen, welche Funktionen Sie konfigurieren möchten, um im Assistenten weiterzukommen. Um Hilfe für eine Funktion aufzurufen, klicken Sie auf das Hilfesymbol (Fragezeichen) in der linken unteren Ecke des Dialogfelds.

Seite „License“

Auf der Seite „License“ werden alle installierten Lizenzen angezeigt. Klicken Sie auf **Yes**, um eine Lizenz hinzuzufügen, zu verändern oder zu löschen, oder auf **No**, um die Lizenzinstallation zu überspringen.

Lizenzkonfiguration

Im Abschnitt **Licenses Configuration** können Sie Lizenzen von einer Lizenzdatei hinzufügen, ändern oder löschen. Data Domain Operating System 6.0 und höher

unterstützt ELMS-Lizenzierung, wodurch Sie mehrere Funktionen in einen einzigen Dateiupload einschließen können.

Bei Verwendung des Konfigurationsassistenten auf einem System ohne konfigurierten Lizenzen wählen Sie den Lizenztyp aus der Drop-down-Liste aus und klicken Sie auf die Schaltfläche **...** Navigieren Sie zum Verzeichnis, in dem sich die Lizenzdatei befindet, und wählen Sie es für das Hochladen auf das System aus.

Tabelle 4 Werte Lizenzkonfigurationsseite

Element	Beschreibung
Add Licenses	Wählen Sie diese Option aus, um Lizenzen aus eine Lizenzdatei hinzuzufügen.
Replace Licenses	Wenn Lizenzen bereits konfiguriert sind, wechselt die Auswahl **Add Licenses** zu **Replace Licenses**. Wählen Sie diese Option aus, um bereits hinzugefügte Lizenzen zu ersetzen.
Delete Licenses	Wählen Sie diese Option aus, um bereits auf dem System konfigurierte Lizenzen zu löschen.

Netzwerk

Im Abschnitt **Network** können Sie die Netzwerkeinstellungen konfigurieren. Klicken Sie auf **Yes**, um die Netzwerkeinstellungen zu konfigurieren, oder klicken Sie auf **No**, um die Netzwerkkonfiguration zu überspringen.

Seite „Network General“

Auf der Seite „General“ können Sie Netzwerkeinstellungen konfigurieren, die definieren, wie das System an einem IP-Netzwerk beteiligt ist.

Zum Konfigurieren dieser Netzwerkeinstellungen außerhalb des Konfigurationsassistenten wählen Sie **Hardware** > **Ethernet** aus.

Tabelle 5 Einstellungen auf der Seite „General“

Element	Beschreibung
Obtain Settings using DHCP	Wählen Sie diese Option aus, um anzugeben, dass das System Netzwerkeinstellungen von einem DHCP-Server (Dynamic Host Control Protocol) sammelt. Wenn Sie die Netzwerkschnittstellen konfigurieren, muss mindestens eine der Schnittstellen für die Verwendung von DHCP konfiguriert werden.
Manually Configure	Wählen Sie diese Option aus, um die Netzwerkeinstellungen zu verwenden, die im Bereich „Settings“ auf dieser Seite definiert sind.
Hostname	Gibt den Netzwerkhostnamen für dieses System an

Tabelle 5 Einstellungen auf der Seite „General“ (Fortsetzung)

Element	Beschreibung
	Hinweis Wenn Sie die Netzwerkeinstellungen über DHCP abrufen, können Sie den Hostnamen manuell unter **Hardware** > **Ethernet** > **Settings** oder mit dem Befehl `net set hostname` konfigurieren. Sie müssen den Hostnamen manuell konfigurieren, wenn Sie DHCP über IPv6 verwenden.
Domain-Name	Gibt die Netzwerkdomain an, zu der dieses System gehört
Default IPv4 Gateway	Gibt die IPv4-Adresse des Gateways an, an das das System Netzwerkanforderungen weiterleitet, wenn kein Routeneintrag für das Zielsystem vorhanden ist
Default IPv6 Gateway	Gibt die IPv6-Adresse des Gateways an, an das das System Netzwerkanforderungen weiterleitet, wenn kein Routeneintrag für das Zielsystem vorhanden ist

Seite „Network Interfaces“

Auf der Seite „Interfaces“ können Sie Netzwerkeinstellungen konfigurieren, die definieren, wie die einzelnen Schnittstellen an einem IP-Netzwerk beteiligt sind.

Zum Konfigurieren dieser Netzwerkeinstellungen außerhalb des Konfigurationsassistenten wählen Sie **Hardware** > **Ethernet** > **Interfaces**.

Tabelle 6 Einstellungen auf der Seite „Interfaces“

Element	Beschreibung
Interface	Listet die in Ihrem System verfügbaren Schnittstellen auf
Enabled	Zeigt, ob jede Schnittstelle aktiviert (aktiviertes Kontrollkästchen) oder deaktiviert) ist (nicht aktiviert). Klicken Sie auf das Kontrollkästchen, um zwischen dem aktiven und deaktivierten Status für die Schnittstelle zu wechseln.
DHCP	Zeigt die aktuelle DHCP-Konfiguration (Dynamic Host Control Protocol) für die einzelnen Schnittstellen an. Wählen Sie **v4** für IPv4 DHCP-Verbindungen, **v6** für IPv6-Verbindungen oder **no** zur Deaktivierung von DHCP aus.
IP Address	Gibt eine IPv4- oder IPv6-Adresse für dieses System an. Um die IP-Adresse zu konfigurieren, müssen Sie DHCP auf **No** festlegen. **Hinweis** Die Systeme DD140, DD160, DD610, DD620 und DD630 bieten keinen Support für IPv6 auf der Schnittstelle eth0a (eth0 auf Systemen mit Legacy-Portnamen) oder auf einem beliebigen VLAN, das auf dieser Schnittstelle erstellt wurde.

Tabelle 6 Einstellungen auf der Seite „Interfaces“ (Fortsetzung)

Element	Beschreibung
Netmask	Gibt die Netzwerkmaske für dieses System an. Zum Konfigurieren der Netzwerkmaske müssen Sie DHCP auf **No** festlegen.
Link	Zeigt an, ob die Ethernetverbindung aktiv („Yes“) ist oder nicht („No“).

Seite „Network DNS“

Auf der Seite „DNS“ können Sie können konfigurieren, wie das System IP-Adressen für DNS-Server in einem Domain Name System (DNS) erhält.

Zum Konfigurieren dieser Netzwerkeinstellungen außerhalb des Konfigurationsassistenten wählen Sie **Hardware** > **Ethernet** > **Settings**.

Tabelle 7 Einstellungen auf der Seite „DNS“

Element	Beschreibung
Obtain DNS using DHCP.	Wählen Sie diese Option aus, um anzugeben, dass das System DNS-IP-Adressen von einem DHCP-Server (Dynamic Host Control Protocol) sammelt. Wenn Sie die Netzwerkschnittstellen konfigurieren, muss mindestens eine der Schnittstellen für die Verwendung von DHCP konfiguriert werden.
Manually configure DNS list.	Wählen Sie diese Option aus, wenn Sie die DNS-Server-IP-Adressen manuell eingeben möchten.
Schaltfläche „Add“ (+)	Klicken Sie auf diese Schaltfläche, um ein Dialogfeld aufzurufen, in dem Sie eine DNS-IP-Adresse zur Liste der DNS-IP-Adressen hinzufügen können. Sie müssen **Manually configure DNS list** auswählen, bevor Sie DNS-IP-Adressen hinzufügen oder löschen können.
Schaltfläche „Delete“ (X)	Klicken Sie auf diese Schaltfläche, um eine DNS-IP-Adresse aus der Liste der DNS-IP-Adressen zu löschen. Sie müssen die zu löschende IP-Adresse auswählen, bevor diese Schaltfläche aktiviert wird. Sie müssen außerdem **Manually configure DNS list** auswählen, bevor Sie DNS-IP-Adressen hinzufügen oder löschen können.
Kontrollkästchen für die IP-Adresse	Aktivieren Sie ein Kontrollkästchen für eine DNS-IP-Adresse, die Sie löschen möchten. Aktivieren Sie das Kontrollkästchen „DNS IP Address“, wenn Sie alle IP-Adressen löschen möchten. Sie müssen **Manually configure DNS list** auswählen, bevor Sie DNS-IP-Adressen hinzufügen oder löschen können.

Dateisystem

Im Abschnitt **File System** können Sie den aktiven und den Cloud-Tier-Speicher konfigurieren. Jedes verfügt über eine separate Assistentenseite. Sie können das

Dateisystem auch in diesem Abschnitt erstellen. Auf die Konfigurationsseiten kann nicht zugegriffen werden, wenn das Dateisystem bereits erstellt wurde.

Jedes Mal, wenn Sie den Abschnitt **File System** anzeigen und das Dateisystem nicht erstellt wurde, zeigt das System eine Fehlermeldung an. Fahren Sie mit dem Verfahren zum Erstellen des Dateisystems fort.

Konfigurieren von Storage-Tier-Seiten

Die Seiten zur Konfiguration des Storage Tier unterstützen Sie bei der Konfiguration von Speicher für jedes lizenzierte Tier im System, im aktiven Tier, im Archiv-Tier und im DD Cloud-Tier. Jeder Tier verfügt über eine separate Assistentenseite. Auf die Seiten für die Storage-Tier-Konfiguration kann nicht zugegriffen werden, wenn das Dateisystem bereits erstellt wurde.

Konfigurieren von aktivem Tier

Der Abschnitt zur Konfiguration eines aktiven Tier unterstützt Sie bei der Konfiguration von aktiven Storage-Tier-Geräten. Im aktiven Tier befinden sich gesicherte Daten. Um dem aktiven Tier Speicher hinzuzufügen, wählen Sie ein oder mehrere Geräte aus und fügen Sie diese auf dem Tier hinzu. Sie können Speichergeräte bis zu den installierten Kapazitätslizenzen hinzufügen.

Das DD3300-System benötigt 4-TB-Geräte für den aktiven Tier.

Tabelle 8 Hinzufügbarer Speicher

Element	Beschreibung
ID (Device in DD VE)	Die Festplattenkennung, die eine der Folgenden sein kann. • Gehäuse- und Festplattennummer (in Form des Gehäusesteckplatzes oder Gerätepakets für DS60-Einschübe) • Gerätenummer für ein logisches Gerät (wie von VTL und vDisk verwendete Geräte) • Eine LUN
Disks	Die Festplatten, die die Spindel oder die LUN bilden. Dies gilt nicht für DD VE-Instanzen.
Model	Der Typ des Festplatteneinschubs. Dies gilt nicht für DD VE-Instanzen.
Disk Count	Die Anzahl der Festplatten in der Spindel oder der LUN. Dies gilt nicht für DD VE-Instanzen.
Disk Size (Size in DD VE)	Die Datenspeicherkapazität der Festplatte bei Verwendung auf einem Data Domain-System.[a]
License Needed	Die erforderliche lizenzierte Kapazität, um den Speicher auf dem Tier hinzuzufügen.
Failed Disks	Fehlgeschlagene Festplatten in der Spindel oder der LUN. Dies gilt nicht für DD VE-Instanzen.
Typ	SCSI. Dies gilt nur für DD VE-Instanzen.

a. Die Data Domain-Konvention für Computing-Speicherplatz definiert ein Gibibyte als 230 Byte und gibt damit eine andere Festplattenkapazität an als die Bewertung des Herstellers.

Tabelle 9 Werte des aktiven Tier

Element	Beschreibung
ID (Device in DD VE)	Die Festplattenkennung, die eine der Folgenden sein kann. • Gehäuse- und Festplattennummer (in Form des Gehäusesteckplatzes oder Gerätepakets für DS60-Einschübe). Dies gilt nicht für DD VE-Instanzen. • Gerätenummer für ein logisches Gerät (wie von VTL und vDisk verwendete Geräte) • Eine LUN
Disks	Die Festplatten, die die Spindel oder die LUN bilden. Dies gilt nicht für DD VE-Instanzen.
Model	Der Typ des Festplatteneinschubs. Dies gilt nicht für DD VE-Instanzen.
Disk Count	Die Anzahl der Festplatten in der Spindel oder der LUN. Dies gilt nicht für DD VE-Instanzen.
Disk Size (Size in DD VE)	Die Datenspeicherkapazität der Festplatte bei Verwendung auf einem Data Domain-System.[a]
License Used	Die vom Speicher verbrauchte lizenzierte Kapazität.
Failed Disks	Fehlgeschlagene Festplatten in der Spindel oder der LUN. Dies gilt nicht für DD VE-Instanzen.
Configured	Neuer oder vorhandener Speicher. Dies gilt nicht für DD VE-Instanzen.
Typ	SCSI. Dies gilt nur für DD VE-Instanzen.

a. Die Data Domain-Konvention für Computing-Speicherplatz definiert ein Gibibyte als 230 Byte und gibt damit eine andere Festplattenkapazität an als die Bewertung des Herstellers.

Konfigurieren von Archiv-Tier

Der Abschnitt zur Konfiguration eines Archiv-Tier unterstützt Sie bei der Konfiguration von Archivspeicher-Tier-Geräten. Im Archiv-Tier befinden sich mit der DD Extended Retention-Funktion archivierte Daten. Um dem Archiv-Tier Speicher hinzuzufügen, wählen Sie ein oder mehrere Geräte aus und fügen Sie diese auf dem Tier hinzu. Sie können Speichergeräte bis zu den installierten Kapazitätslizenzen hinzufügen.

Archiv-Tier-Speicher ist auf dem DD3300-System oder auf DD VE-Instanzen nicht verfügbar.

Tabelle 10 Hinzufügbarer Speicher

Element	Beschreibung
ID	Die Festplattenkennung, die eine der Folgenden sein kann. • Gehäuse- und Festplattennummer (in Form des Gehäusesteckplatzes oder Gerätepakets für DS60-Einschübe) • Gerätenummer für ein logisches Gerät (wie von VTL und vDisk verwendete Geräte)

Tabelle 10 Hinzufügbarer Speicher (Fortsetzung)

Element	Beschreibung
	• Eine LUN
Disks	Die Festplatten, die die Spindel oder die LUN bilden.
Model	Der Typ des Festplatteneinschubs.
Disk Count	Die Anzahl der Festplatten in der Spindel oder der LUN.
Disk Size (Size in DD VE)	Die Datenspeicherkapazität der Festplatte bei Verwendung auf einem Data Domain-System.[a]
License Needed	Die erforderliche lizenzierte Kapazität, um den Speicher auf dem Tier hinzuzufügen.
Failed Disks	Fehlgeschlagene Festplatten in der Spindel oder der LUN.

a. Die Data Domain-Konvention für Computing-Speicherplatz definiert ein Gibibyte als 230 Byte und gibt damit eine andere Laufwerkskapazität an als die Bewertung des Herstellers.

Tabelle 11 Werte des Archiv-Tier

Element	Beschreibung
ID	Die Festplattenkennung, die eine der Folgenden sein kann. • Gehäuse- und Festplattennummer (in Form des Gehäusesteckplatzes oder Gerätepakets für DS60-Einschübe). Dies gilt nicht für DD VE-Instanzen. • Gerätenummer für ein logisches Gerät (wie von VTL und vDisk verwendete Geräte) • Eine LUN
Disks	Die Festplatten, die die Spindel oder die LUN bilden.
Model	Der Typ des Festplatteneinschubs.
Disk Count	Die Anzahl der Festplatten in der Spindel oder der LUN.
Disk Size (Size in DD VE)	Die Datenspeicherkapazität der Festplatte bei Verwendung auf einem Data Domain-System.[a]
License Used	Die vom Speicher verbrauchte lizenzierte Kapazität.
Failed Disks	Fehlgeschlagene Festplatten in der Spindel oder der LUN.
Configured	Neuer oder vorhandener Speicher.

a. Die Data Domain-Konvention für Computing-Speicherplatz definiert ein Gibibyte als 230 Byte und gibt damit eine andere Laufwerkskapazität an als die Bewertung des Herstellers.

Konfigurieren von Cloud-Tier

Der Abschnitt zur Konfiguration eines Cloud-Tier unterstützt Sie bei der Konfiguration von Cloud-Storage-Tier-Geräten. Um dem Cloud-Tier Speicher hinzuzufügen, wählen Sie ein oder mehrere Geräte aus und fügen Sie diese auf dem Tier hinzu. Sie können Speichergeräte bis zu den installierten Kapazitätslizenzen hinzufügen.

Das DD3300-System erfordert 1-TB-Geräte für DD Cloud-Tier.

Tabelle 12 Hinzufügbarer Speicher

Element	Beschreibung
ID (Device in DD VE)	Die Festplattenkennung, die eine der Folgenden sein kann. • Gehäuse- und Festplattennummer (in Form des Gehäusesteckplatzes oder Gerätepakets für DS60-Einschübe) • Gerätenummer für ein logisches Gerät (wie von VTL und vDisk verwendete Geräte) • Eine LUN
Disks	Die Festplatten, die die Spindel oder die LUN bilden. Dies gilt nicht für DD VE-Instanzen.
Model	Der Typ des Festplatteneinschubs. Dies gilt nicht für DD VE-Instanzen.
Disk Count	Die Anzahl der Festplatten in der Spindel oder der LUN. Dies gilt nicht für DD VE-Instanzen.
Disk Size (Size in DD VE)	Die Datenspeicherkapazität der Festplatte bei Verwendung auf einem Data Domain-System.[a]
License Needed	Die erforderliche lizenzierte Kapazität, um den Speicher auf dem Tier hinzuzufügen.
Failed Disks	Fehlgeschlagene Festplatten in der Spindel oder der LUN. Dies gilt nicht für DD VE-Instanzen.
Typ	SCSI. Dies gilt nur für DD VE-Instanzen.

a. Die Data Domain-Konvention für Computing-Speicherplatz definiert ein Gibibyte als 230 Byte und gibt damit eine andere Festplattenkapazität an als die Bewertung des Herstellers.

Tabelle 13 Cloud-Tier-Werte

Element	Beschreibung
ID (Device in DD VE)	Die Festplattenkennung, die eine der Folgenden sein kann. • Gehäuse- und Festplattennummer (in Form des Gehäusesteckplatzes oder Gerätepakets für DS60-Einschübe). Dies gilt nicht für DD VE-Instanzen. • Gerätenummer für ein logisches Gerät (wie von VTL und vDisk verwendete Geräte) • Eine LUN
Disks	Die Festplatten, die die Spindel oder die LUN bilden. Dies gilt nicht für DD VE-Instanzen.
Model	Der Typ des Festplatteneinschubs. Dies gilt nicht für DD VE-Instanzen.
Disk Count	Die Anzahl der Festplatten in der Spindel oder der LUN. Dies gilt nicht für DD VE-Instanzen.
Disk Size (Size in DD VE)	Die Datenspeicherkapazität der Festplatte bei Verwendung auf einem Data Domain-System.[a]

Tabelle 13 Cloud-Tier-Werte (Fortsetzung)

Element	Beschreibung
License Used	Die vom Speicher verbrauchte lizenzierte Kapazität.
Failed Disks	Fehlgeschlagene Festplatten in der Spindel oder der LUN. Dies gilt nicht für DD VE-Instanzen.
Configured	Neuer oder vorhandener Speicher. Dies gilt nicht für DD VE-Instanzen.
Typ	SCSI. Dies gilt nur für DD VE-Instanzen.

a. Die Data Domain-Konvention für Computing-Speicherplatz definiert ein Gibibyte als 230 Byte und gibt damit eine andere Festplattenkapazität an als die Bewertung des Herstellers.

Seite „Create File System“

Auf der Seite „Create File System“ wird die zulässige Größe der einzelnen Speicher-Tiers im Dateisystem angezeigt und das Dateisystem kann automatisch aktiviert werden, nachdem es erstellt wurde.

Systemeinstellungen

Im Abschnitt **System Settings** können Sie Systemkennwörter und E-Mail-Einstellungen konfigurieren. Klicken Sie auf **Yes**, um die Systemeinstellungen zu konfigurieren, oder klicken Sie auf **No**, um die Systemeinstellungskonfiguration zu überspringen.

Seite „System Settings Administrator“

Auf der Seite „Administrator“ können Sie das Administratorpasswort und die Kommunikation zwischen System und Administrator konfigurieren.

Tabelle 14 Einstellungen auf der Seite „Administrator“

Element	Beschreibung
Benutzername	Das Standardadministratorpasswort lautet *sysadmin*. Der sysadmin-Benutzer kann nicht umbenannt oder gelöscht werden.
Old Password	Geben Sie das alte Passwort für den sysadmin-Benutzer ein.
Neues Passwort	Geben Sie das neue Passwort für den sysadmin-Benutzer ein.
Verify New Password	Geben Sie das neue Passwort für den sysadmin-Benutzer erneut ein.
Admin Email	Geben Sie die E-Mail-Adresse an, an die vom DD System Manager Warnmeldungen und Autosupport-Meldungen gesendet werden.
Send Alert Notification Emails to this address	Aktivieren Sie diese Option, um DD System Manager so zu konfigurieren, dass Warnmeldungen an die E-Mail-Adresse des Administrators gesendet werden, wenn Ereignisse mit dem Schweregrad „Alert“ auftreten.

Tabelle 14 Einstellungen auf der Seite „Administrator“ (Fortsetzung)

Element	Beschreibung
Send Daily Alert Summary Emails to this address	Aktivieren Sie diese Option, um DD System Manager so zu konfigurieren, dass am Ende jedes Tages Warnmeldungszusammenfassungen an die E-Mail-Adresse des Administrators gesendet werden.
Send Autosupport Emails to this address	Aktivieren Sie diese Option, um DD System Manager so zu konfigurieren, dass Autosupport-E-Mails an den Administratorbenutzer gesendet werden. Diese E-Mails sind tägliche Berichte, in denen die Systemaktivität und der Status von Dokumenten erfasst werden.

Seite „System Settings Email/Location“

Auf der Seite „Email/Location“ können Sie den Mailservernamen konfigurieren, steuern, welche Systeminformationen an Data Domain gesendet werden, und einen Standortnamen angeben, um Ihr System zu identifizieren.

Tabelle 15 Einstellungen auf der Seite „Email/Location“

Element	Beschreibung
Mail Server	Geben Sie den Namen des Mailservers an, der E-Mails an und vom System managt.
Send Alert Notification Emails to Data Domain	Aktivieren Sie die Option, um DD System Manager so zu konfigurieren, dass E-Mails mit Warnmeldungen an Data Domain gesendet werden.
Send Vendor Support Notification Emails to Data Domain	Aktivieren Sie die Option, um DD System Manager so zu konfigurieren, dass E-Mails mit Benachrichtigungen des Anbietersupports an Data Domain gesendet werden.
Location	Verwenden Sie dieses optionale Attribut nach Bedarf, um den Standort Ihres Systems aufzuzeichnen. Wenn Sie einen Standort angeben, werden diese Informationen als SNMP-Systemstandort gespeichert.

DD Boost-Protokoll

Im Abschnitt **DD Boost Protocol** können Sie die DD Boost-Protokolleinstellungen konfigurieren. Klicken Sie auf **Yes**, um die DD Boost-Protokolleinstellungen zu konfigurieren, oder klicken Sie auf **No**, um die DD Boost-Konfiguration zu überspringen.

Seite „DD Boost Protocol Storage Unit“

Auf der Seite „Storage Unit“ können Sie DD Boost-Speichereinheiten konfigurieren.

Zum Konfigurieren dieser Einstellungen außerhalb des Konfigurationsassistenten wählen Sie **Protocols** > **DD Boost** > **Storage Units** > **+ (Pluszeichen)** aus, um eine Speichereinheit hinzuzufügen, **Bleistift**, um eine Speichereinheit zu ändern, oder **X**, um eine Speichereinheit zu löschen.

Tabelle 16 Einstellungen auf der Seite „Storage Unit“

Element	Beschreibung
Storage Unit	Der Name Ihrer DD Boost-Speichereinheit. Sie können diesen Namen optional ändern.
User	Als DD Boost-Standardbenutzer wählen Sie entweder einen vorhandenen Benutzer aus oder wählen Sie „Create a new Local User“ aus und geben Sie den Benutzernamen, das Passwort und eine Managementrolle ein. Folgende Rollen sind möglich: • *Admin role*: Ermöglicht die Konfiguration und Überwachung des gesamten Data Domain-Systems. • *User role*: Mit dieser Rolle können Sie Data Domain-Systeme überwachen und Ihr eigenes Passwort ändern. • *Security role*: Zusätzlich zu den Rechten der Benutzerrolle können Sie mit dieser Rolle Konfigurationen für Security Officer einrichten und andere Security Officer-Bediener managen. • *Backup-operator role*: Zusätzlich zu den Rechten der Benutzerrolle können Sie mit dieser Rolle Snapshots erstellen, Bänder in eine DD VTL importieren und aus ihr exportieren sowie Bänder innerhalb einer DD VTL verschieben. • *None role*: Nur für die Authentifizierung von DD Boost gedacht, sodass Sie kein Data Domain-System überwachen oder konfigurieren können. „None“ ist auch die übergeordnete Rolle für die Rollen SMT Tenant-Admin und Tenant-User. „None“ ist auch der bevorzugte Benutzertyp für DD Boost-Speichereigentümer. Bei dem Erstellen eines neuen lokalen Benutzers hier kann dieser Benutzer nur die Rolle „None“ haben.

Seite „DD Boost Protocol Fibre Channel“

Auf der Seite „Fibre Channel“ können Sie DD Boost-Zugriffsgruppen über Fibre Channel konfigurieren.

Um diese Einstellungen außerhalb des Konfigurationsassistenten zu konfigurieren, wählen Sie **Protocols** > **DD Boost** > **Fibre Channel** > **+ (Pluszeichen)** , um eine Zugriffsgruppe hinzuzufügen, **das Stiftsymbol** , um eine Zugriffsgruppe zu ändern, oder **X** aus, um eine Zugriffsgruppe zu löschen.

Tabelle 17 Einstellungen auf der Seite „Fibre Channel“

Element	Beschreibung
Configure DD Boost over Fibre Channel	Aktivieren Sie das Kontrollkästchen, wenn Sie DD Boost über Fibre Channel konfigurieren möchten.
Group Name (1 bis 128 Zeichen)	Erstellen Sie eine Zugriffsgruppe. Geben Sie einen eindeutigen Namen ein. Duplizierte Zugriffsgruppen werden nicht unterstützt.

Tabelle 17 Einstellungen auf der Seite „Fibre Channel“ (Fortsetzung)

Element	Beschreibung
Initiators	Wählen Sie einen oder mehrere Initiatoren aus. Optional können Sie den Initiatornamen ersetzen, indem Sie einen neuen Namen eingeben. Ein Initiator ist ein Backupclient, der mit dem System verbunden ist, um Daten mithilfe des Fibre Channel-Protokolls (FC) zu lesen und zu schreiben. Ein bestimmter Initiator kann DD Boost über Fibre Channel oder DD VTL unterstützen, aber nicht beides.
Geräte	Die zu verwendenden Geräte werden aufgelistet. Sie sind auf allen Endpunkten verfügbar. Ein Endpunkt ist das logische Ziel auf dem Data Domain-System, zu dem der Initiator eine Verbindung herstellt.

CIFS-Protokoll

Im Einstellungsabschnitt **CIFS Protocol** können Sie die CIFS-Protokolleinstellungen konfigurieren. Klicken Sie auf **Yes**, um die CIFS-Protokolleinstellungen zu konfigurieren, oder klicken Sie auf **No**, um die CIFS-Konfiguration zu überspringen.

Data Domain-Systeme verwenden den Begriff MTree zum Beschreiben von Verzeichnissen. Wenn Sie einen Verzeichnispfad konfigurieren, erstellt DD OS einen MTree, in denen sich die Daten befinden werden.

Seite „CIFS Protocol Authentication“

Auf der Seite „Authentication“ können Sie Active Directory und die Arbeitsgruppe für Ihr System konfigurieren.

Um diese Einstellungen außerhalb des Konfigurationsassistenten zu konfigurieren, wählen Sie**Administration** > **Access** > **Authentication**.

Tabelle 18 Einstellungen auf der Seite „Authentication“

Element	Beschreibung
Active Directory/Kerberos Authentication	Blenden Sie diesen Bereich ein, um die Active Directory-Kerberos-Authentifizierung zu aktivieren, deaktivieren und konfigurieren.
Workgroup Authentication	Blenden Sie diesen Bereich ein, um die Arbeitsgruppenauthentifizierung zu konfigurieren.

Seite „CIFS Protocol Share“

Auf der Seite „Share“ können Sie einen CIFS-Freigabenamen und einen Verzeichnispfad für Ihr System konfigurieren.

Zum Konfigurieren dieser Einstellungen außerhalb des Konfigurationsassistenten wählen Sie **Protocols** > **CIFS** > **Shares** > **Create** aus.

Tabelle 19 Einstellungen auf der Seite „Share“

Element	Beschreibung
Share Name	Geben Sie einen Namen für die Share ein.
Directory Path	Geben Sie einen Verzeichnispfad für das System ein.
Schaltfläche „Add“ (+)	Klicken Sie auf „+“, um einen Systemclient einzugeben.
Bleistiftsymbol	Ändern Sie einen Client.
Schaltfläche „Delete“ (X)	Klicken Sie auf „X“, um einen ausgewählten Client zu löschen.

NFS-Protokoll

Im Einstellungsabschnitt **NFS Protocol** können Sie die NFS-Protokolleinstellungen konfigurieren. Klicken Sie auf **Yes**, um die NFS-Protokolleinstellungen zu konfigurieren, oder klicken Sie auf **No**, um die NFS-Konfiguration zu überspringen.

Data Domain-Systeme verwenden den Begriff MTree zum Beschreiben von Verzeichnissen. Wenn Sie einen Verzeichnispfad konfigurieren, erstellt DD OS einen MTree, in denen sich die Daten befinden werden.

Seite „NFS Protocol Export“

Auf der Seite „Export“ können Sie einen Verzeichnispfad, Netzwerkclients und NFSv4-Referrals für Exporte mittels NFS konfigurieren.

Um diese Einstellungen außerhalb des Konfigurationsassistenten zu konfigurieren, wählen Sie **Protocols** > **NFS** > **Create**.

Tabelle 20 Einstellungen auf der Seite „Export“

Element	Beschreibung
Directory Path	Geben Sie einen Pfadnamen für den Export ein.
Schaltfläche „Add“ (+)	Klicken Sie auf +, um einen Systemclient oder ein NFSv4-Referral einzugeben.
Bleistiftsymbol	Ändern Sie einen Client oder ein NFSv4-Referral.
Schaltfläche „Delete“ (X)	Klicken Sie auf „X“, um einen ausgewählten Client oder ein NFSv4-Referral zu löschen.

DD VTL-Protokoll

Im Einstellungsabschnitt **DD VTL Protocol** können Sie die Einstellungen der Data Domain Virtual Tape Library konfigurieren. Klicken Sie auf **Yes**, um die DD VTL-Einstellungen zu konfigurieren, oder klicken Sie auf **No**, um die DD VTL-Konfiguration zu überspringen.

Seite „VTL Protocol Library“

Auf der Seite „Library“ können Sie die DD VTL-Protokolleinstellungen für eine Bibliothek konfigurieren.

Zum Konfigurieren dieser Einstellungen außerhalb des Konfigurationsassistenten wählen Sie **PROTOCOLS** > **VTL** > **Virtual Tape Libraries** > **VTL Service** > **Libraries** > **More Tasks** > **Library** > **Create** aus.

Tabelle 21 Einstellungen auf der Seite „Library“

Element	Beschreibung
Library Name	Geben Sie einen Namen mit einer Länge zwischen 1 und 32 alphanumerischen Zeichen ein.
Number of Drives	Anzahl der unterstützten Bandlaufwerke
Drive Model	Wählen Sie das gewünschte Modell aus der Drop-down-Liste aus: • IBM-LTO-1 • IBM-LTO-2 • IBM-LTO-3 • IBM-LTO-4 • IBM-LTO-5 (Standard) • HP-LTO-3 • HP-LTO-4
Number of Slots	Geben Sie die Anzahl der Steckplätze pro Bibliothek ein: • Bis zu 32.000 Steckplätze pro Bibliothek • Bis zu 64.000 Steckplätze pro System • Dieser Wert sollte größer oder gleich der Anzahl von Laufwerken sein.
Number of CAPs	(Optional) Geben Sie die Anzahl der CAPs (Cartridge Access Ports) ein: • Bis zu 100 CAPs pro Bibliothek • Bis zu 1.000 CAPs pro System
Changer Model Name	Wählen Sie das gewünschte Modell aus der Drop-down-Liste aus: • L180 (Standard) • RESTORER-L180 • TS3500 • I2000 • I6000 • DDVTL
Starting Barcode	Geben Sie den gewünschten Strichcode für das erste Band im Format A990000LA ein.
Tape Capacity	(Optional) Geben Sie die Bandkapazität ein. Wenn dieser Wert nicht angegeben ist, wird Kapazität aus dem letzten Zeichen des Strichcodes abgeleitet.

Seite „VTL Protocol Access Group“

Auf der Seite „Access Group“ können Sie DD VTL-Protokolleinstellungen für eine Zugriffsgruppe konfigurieren.

Um diese Einstellungen außerhalb des Konfigurationsassistenten zu konfigurieren, wählen Sie **PROTOCOLS** > **VTL** > **Access Groups** > **Groups** > **More Tasks** > **Group** > **Create**.

Tabelle 22 Einstellungen auf der Seite „Access Group“

Element	Beschreibung
Gruppenname	Geben Sie einen eindeutigen Namen ein, der zwischen 1 und 128 Zeichen aufweist. Duplizierte Zugriffsgruppen werden nicht unterstützt.
Initiators	Wählen Sie einen oder mehrere Initiatoren aus. Optional können Sie den Initiatornamen ersetzen, indem Sie einen neuen Namen eingeben. Ein Initiator ist ein Backupclient, der mit einem System verbunden ist, um Daten mithilfe des FC-Protokolls (Fibre Channel) zu lesen und schreiben. Ein bestimmter Initiator kann DD Boost über Fibre Channel oder DD VTL unterstützen, aber nicht beides.
Geräte	Die zu verwendenden Geräte (Laufwerke und Wechsler) werden aufgelistet. Sie sind auf allen Endpunkten verfügbar. Ein Endpunkt ist das logische Ziel auf dem Data Domain-System, zu dem der Initiator eine Verbindung herstellt.

Data Domain-Befehlszeilenoberfläche

Bei der Befehlszeilenoberfläche (CLI, Command Line Interface) handelt es sich um eine textgesteuerte Oberfläche, die anstelle von oder zusätzlich zu DD System Manager verwendet werden kann. Die meisten Managementaufgaben können in DD System Manager oder über die Befehlszeilenoberfläche durchgeführt werden. In einigen Fällen bietet die Befehlszeilenoberfläche Konfigurationsoptionen und Berichte, die in DD System Manager noch nicht unterstützt werden.

Jeder Data Domain-Systembefehl, der eine Liste akzeptiert, z. B. eine Liste von IP-Adressen, akzeptiert Einträge, die durch Kommas, durch Leerzeichen oder beides getrennt sind.

Mit der Tabulatortaste können folgende Aktionen durchgeführt werden:

- Abschließen eines Befehlseintrags, wenn dieser Eintrag eindeutig ist. Die Vervollständigung mithilfe der Tabulatortaste wird für alle Schlüsselwörter unterstützt. Wenn Sie beispielsweise`syst` Tabulator `sh` Tabulator `st` Tabulator eingeben, wird der Befehl `system show stats` angezeigt.
- Anzeigen der nächsten verfügbaren Option, wenn Sie keine Zeichen eingeben, bevor Sie die Tabulatortaste drücken
- Anzeigen partiell übereinstimmender Token oder Abschließen eines eindeutigen Eintrags, wenn Sie Zeichen eingeben, bevor Sie die Tabulatortaste drücken

Im *Data Domain Operating System Command Reference Guide* finden Sie Informationen über die jeweiligen CLI-Befehle. Eine Onlinehilfe ist verfügbar und stellt die vollständige Syntax für jeden Befehl bereit.

Anmelden bei der CLI

Sie können auf die Befehlszeilenoberfläche (CLI) mithilfe einer direkten Verbindung mit dem System oder über eine Ethernetverbindung mittels SSH oder Telnet zugreifen.

Bevor Sie beginnen

Damit Sie die Befehlszeilenoberfläche verwenden können, müssen Sie eine lokale oder Remoteverbindung mit dem System mithilfe einer der folgenden Methoden einrichten.

- Wenn Sie eine Verbindung über einen seriellen Konsolenport im System herstellen, schließen Sie eine Terminalkonsole an den Port an und verwenden Sie die folgenden Kommunikationseinstellungen: 9600 Baud, 8 Datenbits, keine Parität und 1 Stopbit.
- Wenn das System mit Tastatur- und Monitorports ausgestattet ist, schließen Sie eine Tastatur und einen Bildschirm an diese Ports an.
- Wenn Sie eine Verbindung über Ethernet herstellen, schließen Sie einen Computer mit SSH- oder Telnet-Clientsoftware an ein Ethernetnetzwerk an, das mit dem System kommunizieren kann.

Vorgehensweise

1. Wenn Sie für den Zugriff auf die Befehlszeilenoberfläche eine SSH- oder Telnet-Verbindung verwenden, starten Sie den SSH- oder Telnet-Client und geben Sie die IP-Adresse oder den Hostnamen des Systems an.

   Informationen zum Initiieren der Verbindung finden Sie in der Dokumentation zur Clientsoftware. Das System fordert Sie auf, Ihren Benutzernamen einzugeben.

2. Geben Sie Ihren Benutzernamen für das System ein, wenn Sie dazu aufgefordert werden.
3. Geben Sie Ihr Passwort für das System ein, wenn Sie dazu aufgefordert werden.

Im folgenden Beispiel ist die SSH-Anmeldung bei einem System mit dem Namen *mysystem* mithilfe der SSH-Clientsoftware dargestellt.

```
# ssh -l sysadmin mysystem.mydomain.com
Data Domain OS 5.6.0.0-19899
Password:
```

Richtlinien zur Onlinehilfe der Befehlszeilenoberfläche

Die Befehlszeilenoberfläche zeigt zwei Hilfetypen an: eine reine Syntaxhilfe und eine Hilfe zu den Befehlsbeschreibungen, die die Befehlssyntax umfasst. Beide Hilfetypen enthalten Funktionen, mit deren Hilfe Sie die benötigten Informationen schneller finden.

In den folgenden Richtlinien wird beschrieben, wie Sie die Hilfe nur für die Syntax verwenden.

- Um die CLI-Befehle des obersten Levels aufzulisten, geben Sie ein Fragezeichen (`?`) ein oder geben Sie den Befehl `help` an der Befehlszeilenaufforderung ein.

- Um alle Formen eines Befehls auf oberstem Level aufzulisten, geben Sie den Befehl an der Eingabeaufforderung ohne Optionen ein oder geben Sie den Befehl `?` ein.
- Um alle Befehle aufzulisten, die ein bestimmtes Schlüsselwort verwenden, geben Sie `help`*keyword* oder `?`*keyword* ein.
  `? password` beispielsweise zeigt alle Data Domain-Systembefehle an, die das Passwortargument verwenden.

In den folgenden Richtlinien wird beschrieben, wie Sie die Befehlsbeschreibungshilfe verwenden.

- Um die CLI-Befehle des obersten Levels aufzulisten, geben Sie ein Fragezeichen (`?`) ein oder geben Sie den Befehl `help` an der Befehlszeilenaufforderung ein.
- Um alle Formen eines Befehls auf oberstem Level mit einer Einleitung aufzulisten, geben Sie `help`command oder `?`*command* ein.
- Das Ende jeder Hilfebeschreibung ist als `END` markiert. Drücken Sie die Eingabetaste, um zur CLI-Eingabeaufforderung zurückzukehren.
- Wenn die vollständige Hilfebeschreibung nicht in die Anzeige passt, wird die Doppelpunkt-Eingabeaufforderung (`:`) am unteren Rand der Anzeige angezeigt. Die folgenden Richtlinien beschreiben, was Sie tun können, wenn diese Eingabeaufforderung angezeigt wird.
  - Um durch die Hilfeanzeige zu blättern, verwenden Sie die Pfeiltasten nach oben und unten.
  - Um die aktuelle Hilfe zu beenden und zur CLI-Eingabeaufforderung zurückzuwechseln, drücken Sie auf **q**.
  - Um die Hilfe zum Navigieren in der Hilfeanzeige anzuzeigen, drücken Sie auf **h**.
  - Um nach Text in der Hilfeanzeige zu suchen, geben Sie einen Schrägstrich (`/`) gefolgt von einem als Suchkriterium zu verwendenden Muster ein und drücken Sie die Eingabetaste. Übereinstimmungen werden hervorgehoben.

KAPITEL 3

Managen von Data Domain-Systemen

Dieses Kapitel enthält Folgendes:

Überblick über das Systemmanagement

Mit DD System Manager können Sie das System managen, auf dem DD System Manager installiert ist.

- Um die Replikation zu sichern, unterstützt DD System Manager das Hinzufügen von Systemen, die die beiden vorherigen Versionen, die aktuelle Version und die nächsten beiden Versionen ausführen, wenn sie verfügbar werden. Für Release 6.0 unterstützt DD System Manager also das Hinzufügen von Systemen für die Replikation für DD OS Version 5.6 bis 5.7 sowie die nächsten beiden Versionen.

Hinweis

Bei der Verarbeitung einer hohen Auslastung kann ein System weniger reaktionsschnell sein als normal. In diesem Fall kann es länger dauern, bis die entweder von DD System Manager oder über die Befehlszeilenoberfläche ausgegebenen Managementbefehle vollständig ausgeführt sind. Wenn die Dauer die zulässigen Grenzwerte überschreitet, wird ein Timeout-Fehler zurückgegeben, selbst wenn der Vorgang abgeschlossen wurde.

Die folgende Tabelle empfiehlt die maximale Anzahl von Benutzersitzungen, die von DD System Manager unterstützt werden:

Tabelle 23 Maximale Anzahl an Benutzern, die von DD System Manager unterstützt werden

Systemmodell	Aktive Benutzer maximal	Angemeldete Benutzer maximal
4-GB-Modelle[a]	5	10
8-GB-Modelle[b]	10	15
16-GB-Modelle und größere Modelle[c]	10	20

a. Umfasst DD140 und DD2200 (4 TB)
b. Umfasst DD610 und DD630
c. Umfasst DD670, DD860, DD890, DD990, DD2200 (> 7,5 TB), DD4200, DD4500, DD6300, DD6800, DD7200, DD9300, DD9500 und DD9800

Hinweis

Die Ersteinrichtung des HA-Systems kann nicht über DD System Manager erfolgen, der Status eines bereits konfigurierten HA-Systems kann jedoch über DD System Manager angezeigt werden.

Überblick über das HA-Systemmanagement

Die HA-Beziehung zwischen den zwei Nodes, einem aktiven Node und einem Stand-by-Node, wird über DDSH-CLIs eingerichtet.

Die Ersteinrichtung kann auf beiden Nodes ausgeführt werden, aber nur einzeln. Es ist eine Voraussetzung für HA, dass der System-Interconnect und identische Hardware zunächst auf beiden Nodes eingerichtet werden.

Hinweis

Beide DDRs müssen identische Hardware aufweisen, die während der Einrichtung und dem Systemstart validiert wird.

Wenn die Einrichtung von einer Neuinstallation von Systemen erfolgt, muss der `ha create`-Befehl auf dem Node mit der installierten Lizenz ausgeführt werden. Wenn die Einrichtung von einem vorhandenen System und einem neuen System (Upgrade) erfolgt, sollte sie auf dem vorhandenen System ausgeführt werden.

Geplante Wartung für HA-System

Die HA-Architektur bietet ein sequenzielles Upgrade, das Ausfallzeiten für Wartungsvorgänge für ein DD OS-Upgrade reduziert.

Mit einem sequenziellen Upgrade wird ein Upgrade für die HA-Nodes nacheinander, koordiniert und automatisch durchgeführt. Der Stand-by-Node wird neu gestartet und das Upgrade wird zuerst auf ihm durchgeführt. Der neu aktualisierte Node übernimmt die aktive Rolle über ein HA-Failover. Nach dem Failover wird der zweite Node neu gestartet und übernimmt die Rolle des Stand-by-Node nach dem Upgrade.

Systemupgradevorgänge, die Datenkonvertierung erfordern, können nicht gestartet werden, bis beide Systeme auf dieselbe Ebene aktualisiert wurden und der HA-Status vollständig wiederhergestellt ist.

Neustart eines Systems

Starten Sie ein System neu, wenn eine Konfigurationsänderung, beispielsweise das Ändern der Zeitzone, den Neustart des Systems erforderlich macht.

Vorgehensweise

1. Wählen Sie **Maintenance** > **System** > **Reboot System** aus.
2. Klicken Sie zur Bestätigung auf **OK**.

Ein- und Ausschalten eines Systems

Beim Ein- und Ausschalten eines System müssen Sie ordnungsgemäß vorgehen, um die Integrität von Dateisystem und Konfiguration zu wahren.

Verwenden Sie nicht den Gehäusenetzschalter, um das System auszuschalten. Damit würde die Fernsteuerung für die Ein- und Ausschaltung mit IPMI verhindert. Verwenden Sie stattdessen den Befehl `system poweroff` . Der Befehl `system poweroff` fährt das System herunter und schaltet es aus.

Die IMPI-Remotefunktion zur Systemabschaltung fährt DD OS nicht ordnungsgemäß herunter. Verwenden Sie diese Funktion nur dann, wenn der Befehl `system poweroff` nicht erfolgreich war.

Für HA-Systeme ist eine Verbindung zu beiden Nodes erforderlich.

Führen Sie die folgenden Schritte durch, um ein Data Domain-System auszuschalten:

Vorgehensweise

1. Stellen Sie sicher, dass I/O auf das System beendet wurde.

   Führen Sie folgende Befehle aus:

   - `cifs show active`

- `nfs show active`
- `system show stats view sysstat interval 2`
- `system show perf`

2. Überprüfen Sie für HA-Systeme die Integrität der HA-Konfiguration.

   Führen Sie den folgenden Befehl aus:
   `ha status`

```
HA System Name: apollo-ha3a.emc.com
HA System Status: highly available
Node Name                  Node ID   Role      HA State
-------------------------- --------- --------- --------
apollo-ha3a-p0.emc.com       0       active    online
apollo-ha3a-p1.emc.com       1       standby   online
-------------------------- --------- --------- --------
```

Hinweis

Dieses Ausgabebeispiel stammt von einem ordnungsgemäß funktionierenden System. Wenn das System heruntergefahren wird, um eine fehlerhafte Komponente zu ersetzen, wird der HA-Systemstatus wird heruntergestuft und ein Node oder beide Nodes werden für den HA-Status offline angezeigt.

3. Führen Sie den Befehl `alerts show current` aus. Führen Sie für HA-Paare den Befehl zuerst auf dem aktiven Node und dann auf dem Stand-by-Node aus.
4. Führen Sie für HA-Systeme den Befehl `ha offline` aus, wenn das System in einem hochverfügbaren Zustand ist und beide Nodes online sind. Überspringen Sie diesen Schritt, wenn der HA-Status heruntergestuft ist.
5. Führen Sie den Befehl `system poweroff` aus. Führen Sie für HA-Paare den Befehl zuerst auf dem aktiven Node und dann auf dem Stand-by-Node aus.

   Mit diesem Befehl werden automatisch DD OS-Prozesse ordnungsgemäß heruntergefahren. Er ist nur für Administratorbenutzer verfügbar.
6. Entfernen Sie die Netzkabel von den Netzteilen auf dem Controller oder den Controllern.
7. Überprüfen Sie, dass die blaue Betriebs-LED auf dem Controller oder den Controllern nicht leuchtet, um zu bestätigen, dass das System ausgeschaltet ist.

Einschalten eines Systems

Stellen Sie Stromversorgung zum Data Domain-System wieder her, wenn die Ausfallzeit des Systems abgeschlossen ist.

Vorgehensweise

1. Schalten Sie ggf. Erweiterungseinschübe ein, bevor Sie den Data Domain-Controller einschalten. Warten Sie rund drei Minuten, nachdem Sie alle Erweiterungseinschübe eingeschaltet haben.

   Hinweis

   Ein Controller ist das Gehäuse und jeder interne Speicher. Ein *Data Domain-System* bezieht sich auf den Controller und jeden optionalen externen Speicher.

2. Schließen Sie das Netzkabel für den Controller an. Wenn der Controller einen Netzschalter hat, drücken Sie den Netzschalter des Controllers (wie im

Installations- und Einrichtungshandbuch für Ihr Data Domain-System dargestellt). Schalten Sie für HA-Systeme zuerst den aktiven Node und dann den Stand-by-Node ein.

3. Überprüfen Sie für HA-Systeme die Integrität der HA-Konfiguration. Führen Sie den folgenden Befehl aus:
   `ha status`

```
HA System Name: apollo-ha3a.emc.com
HA System Status: highly available
Node Name                  Node ID   Role      HA State
-------------------------- --------- --------- --------
apollo-ha3a-p0.emc.com       0       active    online
apollo-ha3a-p1.emc.com       1       standby   offline
-------------------------- --------- --------- --------
```

4. Wenn einer der Nodes als offline angezeigt wird, führen Sie für HA-Systeme den Befehl `ha online` auf diesem Node aus, um die HA-Konfiguration wiederherzustellen.
5. Führen Sie den Befehl `alerts show current` aus. Führen Sie für HA-Paare den Befehl zuerst auf dem aktiven Node und dann auf dem Stand-by-Node aus.

Management von Systemupgrades

Um ein Upgrade für ein DD OS-System durchzuführen, müssen Sie überprüfen, ob für die neue Software genügend Platz auf dem Zielsystem vorhanden ist, die Software auf das System übertragen, das aktualisiert werden soll, und dann das Upgrade starten. Übertragen Sie bei HA-Systemen die Software auf den aktiven Node und starten Sie das Upgrade vom aktiven Node.

Verwenden Sie für HA-Systeme die Floating IP-Adresse für den Zugriff auf DD System Manager, um Softwareupgrades durchzuführen.

⚠ ACHTUNG

DD OS 6.0 verwendet Secure Remote Support-Version 3 (ESRSv3). Beim Upgrade eines Systems mit DD OS 5.X auf DD OS 6.0 wird die vorhandene ConnectEMC-Konfiguration aus dem System entfernt. Nachdem das Upgrade abgeschlossen ist, konfigurieren Sie ConnectEMC manuell neu.

Wenn das System MD5-signierte Zertifikate verwendet, erzeugen Sie die Zertifikate mit einem stärkeren Hash-Algorithmus während des Upgrades erneut.

Upgrade mit möglichst wenigen Störungen

Mit der Funktion zum Upgrade mit möglichst wenigen Störungen (MDU, Minimally Disruptive Upgrade) können Sie die spezifischen Softwarekomponenten aktualisieren oder Fehlerkorrekturen anwenden, ohne einen Neustart des Systems durchführen zu müssen. Nur Services, die von der gerade aktualisierten Komponente abhängig sind, werden unterbrochen, damit die MDU-Funktion nennenswerte Ausfallzeiten während bestimmter Softwareupgrades verhindern kann.

Nicht alle Softwarekomponenten eignen sich für ein Upgrade mit möglichst wenigen Störungen. Diese Komponenten müssen im Rahmen eines regulären DD OS-Systemsoftwareupgrades aktualisiert werden. Ein Upgrade der DD OS-Software verwendet ein großes RPM (Upgrade-Bundle), das Upgrades für alle Komponenten des DD OS durchführt. MDU verwendet kleinere Komponenten-Bundles, die Upgrades von spezifischen Komponenten einzeln durchführen.

RPM-Signaturverifizierung

Die RPM-Signaturverifizierung überprüft Data Domain-RPMs, die Sie für das Upgrade herunterladen. Wenn das RPM nicht manipuliert wurde, ist die digitale Signatur gültig

und Sie können das RPM wie gewohnt verwenden. Wenn das RPM manipuliert wurde, wird die digitale Signatur durch die Beschädigung ungültig und das RPM wird von DD OS abgelehnt. Es wird eine entsprechende Fehlermeldung angezeigt.

Hinweis

Führen Sie beim Upgrade von 5.6.0.x auf 6.0 zunächst ein Upgrade des 5.6.0.x-Systems auf 5.6.1.x (oder höher) vor dem Upgrade auf 6.0 durch.

Supportsoftware
DD OS 6.1 führt ein Softwarepaket ein, die sogenannte Supportsoftware. Supportsoftware wird vom Data Domain Support Engineering für bestimmte Aspekte bereitgestellt. Standardmäßig lässt das Data Domain-System die Installation der Supportsoftware auf dem System nicht zu. Kontaktieren Sie den Support, um weitere Informationen zu Supportsoftware zu erhalten.

Anzeigen von Upgradepaketen auf dem System

Mit DD System Manager können Sie bis zu fünf Upgradepakete auf einem System anzeigen und managen. Bevor Sie ein Upgrade für ein System durchführen können, müssen Sie ein Upgradepaket von der Onlinesupport-Website auf einen lokalen Computer herunterladen und danach auf das Zielsystem hochladen.

Vorgehensweise

1. Wählen Sie **Maintenance** > **System**.
2. Wählen Sie optional ein Aktualisierungspaket aus und klicken Sie auf **View Checksum**, um die MD5- und SHA256-Prüfsummen des Aktualisierungspakets anzuzeigen.

Ergebnisse

Für jedes im System gespeicherte Paket zeigt DD System Manager Dateiname, Dateigröße und Datum der letzten Änderung in der Liste mit folgendem Titel an: Upgrade Packages Available on Data Domain System.

Erhalten und Überprüfen von Upgradepaketen

Sie können mithilfe von DD System Manager nach Upgradepaketdateien auf der Data Domain-Supportwebsite suchen und Kopien dieser Dateien auf ein System hochladen.

Hinweis

Sie können FTP oder NFS verwenden, um ein Upgradepaket auf ein System zu kopieren. DD System Manager ist auf das Managen von fünf Systemupgradepaketen beschränkt, aber es gibt keine Einschränkungen mit Ausnahme von Speicherplatzbeschränkungen, wenn Sie die Dateien direkt im Verzeichnis `/ddvar/releases` managen. FTP ist standardmäßig deaktiviert. Zum Verwenden von NFS muss `/ddvar` exportiert und von einem externen Host gemountet werden.

Vorgehensweise

1. Wählen Sie **Maintenance** > **System**.
2. Um ein Upgradepaket zu erhalten, klicken Sie auf den Link **EMC Online Support**, klicken Sie auf „Downloads“ und verwenden Sie die Suchfunktion, um nach dem Paket zu suchen, das Supportmitarbeiter für Ihr System empfehlen. Speichern Sie das Upgradepaket auf dem lokalen Computer.

3. Vergewissern Sie sich, dass nicht mehr als vier Pakete in der Liste „Upgrade Packages Available on Data Domain System“ aufgeführt sind.

   DD System Manager kann bis zu fünf Upgradepakete managen. Wenn fünf Pakete in der Liste angezeigt werden, entfernen Sie mindestens ein Paket, bevor Sie das neue Paket hochladen.

4. Klicken Sie auf **Upload Upgrade Package**, um die Übertragung des Upgradepakets an das System zu initiieren.
5. Klicken Sie im Dialogfeld „Upload Upgrade Package“ auf **Browse**, um das Dialogfeld „Choose File to Upload“ zu öffnen. Navigieren Sie zu dem Ordner mit der heruntergeladenen Datei, wählen Sie die Datei aus und klicken Sie auf **Open**.
6. Klicken Sie auf **OK**.

   Ein Dialogfeld mit dem Uploadfortschritt wird angezeigt. Nach erfolgreichem Abschluss des Hochladens wird die heruntergeladene Datei (mit der Erweiterung RPM) in der Liste mit folgendem Titel angezeigt: Upgrade Packages Available on Data Domain System.

7. Klicken Sie zum Überprüfen der Upgradepaketintegrität auf **View Checksum** und vergleichen Sie die berechnete Prüfsumme, die im Dialogfeld angezeigt wird, mit der maßgeblichen Prüfsumme auf der Onlinesupport-Website.
8. Wählen Sie ein Upgradepaket und klicken Sie auf **Upgrade Precheck**, um manuell eine Vorabprüfung des Upgrades zu initiieren.

Überlegungen zum Upgrade für HA-Systeme

HA-Systeme erfordern eine eindeutige Vorprüfung vor dem Initiieren des Upgradevorgangs und eine eindeutige Nachprüfung, nachdem das Upgrade abgeschlossen ist.

Das HA-System muss sich in einem hochverfügbaren Status befinden, wobei beide Nodes vor dem Ausführen des DD OS-Upgrades online sein müssen. Führen Sie den Befehl `ha status` zur Verifizierung des Status des HA-Systems aus.

```
# HA-Status
HA System Name: apollo-ha3a.emc.com
HA System Status: highly available
Node Name                   Node ID   Role      HA State
--------------------------- --------- --------- --------
apollo-ha3a-p0.emc.com       0       active    online
apollo-ha3a-p1.emc.com       1       standby   online
--------------------------- --------- --------- --------
```

DD OS erkennt das HA-System automatisch und führt den Upgradevorgang auf beiden Nodes aus.

Führen Sie nach Abschluss des Upgrades den Befehl `ha status` erneut aus, um zu überprüfen, ob das System in einem hochverfügbaren Zustand ist und ob beide Nodes online sind.

Upgrade eines Data Domain-Systems

Wenn auf einem System eine Upgradepaketdatei vorhanden ist, können Sie mit DD System Manager und diesem Upgradepaket ein Upgrade durchführen.

Bevor Sie beginnen

Lesen Sie die DD OS-Versionshinweise für die vollständigen Anweisungen zum Upgrade und die Abdeckung aller Probleme, die sich auf das Upgrade auswirken können.

Im Folgenden wird beschrieben, wie Sie ein Upgrade mit DD System Manager initiieren. Melden Sie sich bei allen Data Domain-CLI-Sitzungen auf dem System ab, auf dem das Upgrade durchgeführt werden soll, bevor Sie für das System mit DD System Manager ein Upgrade durchführen.

Hinweis

Upgradepaketdateien verwenden die .rpm-Dateierweiterung. In diesem Thema wird davon ausgegangen, dass Sie nur DD OS aktualisieren. Wenn Sie Änderungen an der Hardware vornehmen, beispielsweise Schnittstellenkarten hinzufügen, austauschen oder verschieben, müssen Sie die DD OS-Konfiguration aktualisieren, damit sie mit den Hardwareänderungen übereinstimmt.

Vorgehensweise

1. Melden Sie sich bei DD System Manager auf dem System an, auf dem das Upgrade durchgeführt werden soll.

   Hinweis

   Bei den meisten Versionen sind Upgrades von bis zu zwei früheren Hauptversionen zulässig. Bei Version 6.0 sind Upgrades von den Versionen 5.6 und 5.7 zulässig.

   Hinweis

   Wie in den Versionshinweisen empfohlen, starten Sie das Data Domain-System neu, bevor Sie ein Upgrade durchführen, um zu überprüfen, ob die Hardware bereinigt ist. Wenn Probleme während des Neustarts erkannt werden, beheben Sie diese Probleme vor dem Start des Upgrades. Für ein MDU-Upgrade ist ein Neustart möglicherweise nicht erforderlich.

2. Wählen Sie **Data Management** > **File System** aus und stellten Sie sicher, dass das Dateisystem aktiviert ist und ausgeführt wird.
3. Wählen Sie **Maintenance** > **System**.
4. Wählen Sie in der Liste „Upgrade Packages Available on Data Domain System“ das Paket aus, das für das Upgrade verwendet werden soll.

   Hinweis

   Sie müssen ein Upgradepaket für eine neuere Version von DD OS auswählen. DD OS unterstützt keine Downgrades auf frühere Versionen.

5. Klicken Sie auf **Perform System Upgrade**.

   Das Dialogfeld „System Upgrade“ wird angezeigt und zeigt Informationen über das Upgrade und eine Liste der Benutzer an, die derzeit bei dem System angemeldet sind, für das das Upgrade durchgeführt werden soll.

6. Überprüfen Sie die Version des Upgrade-Image und klicken Sie auf **OK**, um mit dem Upgrade fortzufahren.

   Im Dialogfeld „System Upgrade“ werden der Upgradestatus und die verbleibende Zeit angezeigt.

   Wenn das Systemupgrade durchgeführt wird, müssen Sie warten, bis das Upgrade abgeschlossen ist, bevor Sie das System mithilfe von DD System

Manager managen. Wenn das System neu gestartet wird, wird das Upgrade möglicherweise nach dem Neustart fortgesetzt und DD System Manager zeigt den Updatestatus nach der Anmeldung an. Es empfiehlt sich, dass Sie das Fortschrittsdialogfeld für das Systemupgrade geöffnet lassen, bis das Upgrade abgeschlossen ist oder das System ausgeschaltet wird. Wenn Sie ein Upgrade von DD OS Version 5.5 oder höher auf eine neuere Version durchführen und für das Systemupgrade kein Ausschalten erforderlich ist, wird ein Link zum Anmelden angezeigt, wenn das Upgrade abgeschlossen ist.

Hinweis

Geben Sie den Befehl `system upgrade status` ein, um den Status eines Upgrades über die Befehlszeilenoberfläche anzuzeigen. Protokollmeldungen für das Upgrade werden in `/ddvar/log/debug/platform/upgrade-error.log` und `/ddvar/log/debug/platform/upgrade-info.log` gespeichert.

7. Wenn das System ausgeschaltet wird, müssen Sie den Wechselstrom aus dem System entfernen, um die vorherige Konfiguration zu entfernen. Trennen Sie alle Stromkabel für eine Dauer von 30 Sekunden und schließen Sie sie dann wieder an. Das System wird eingeschaltet und neu gestartet.
8. Wenn das System nicht automatisch hochgefahren wird und die Vorderseite über einen Netzschalter verfügt, drücken Sie auf den Netzschalter.

Weitere Erfordernisse

Für Umgebungen, die selbstsignierte SHA-256-Zertifikate verwenden, müssen die Zertifikate nach Abschluss des Upgradeprozesses erneut manuell erzeugt werden. Die Vertrauensbeziehungen zu externen Systemen, die eine Verbindung zum Data Domain-System herstellen, müssen wiederhergestellt werden.

1. Führen Sie den Befehl **`adminaccess certificate generate self-signed-cert regenerate-ca`** aus, um die selbstsignierten CA- und Hostzertifikate erneut zu erzeugen. Durch die erneute Erzeugung der Zertifikate werden die bestehenden Vertrauensbeziehungen mit externen Systemen beendet.
2. Führen Sie den Befehl **`adminaccess trust add host`** ***`hostname`*** **`type mutual`** aus, um die gegenseitigen Vertrauensbeziehungen zwischen dem Data Domain-System und dem externen System wiederherzustellen.

Entfernen eines Upgradepakets

Sie können maximal fünf Upgradepakete auf ein System mit DD System Manager hochladen. Wenn das System, für das Sie ein Upgrade durchführen, fünf Upgradepakete enthält, müssen Sie mindestens ein Paket entfernen, bevor das Upgrade für das System durchgeführt werden kann.

Vorgehensweise

1. Wählen Sie **Maintenance** > **System**.
2. Wählen Sie aus der Liste mit dem Titel „Upgrade Packages Available on Data Domain System“ das zu entfernende Paket aus. Sie können jeweils nur ein Paket entfernen.
3. Klicken Sie auf **Remove Upgrade Package**.

Managen von elektronischen Lizenzen

Fügen Sie elektronische Lizenzen zum Data Domain-System hinzu und entfernen Sie sie. Aktuelle Informationen zu Produktfunktionen, Softwareupdates, Kompatibilitätsleitfäden für Software und Informationen zu Produkten, Lizenzierung und Service finden Sie in den entsprechenden *Data Domain Operating System Release Notes*.

Lizenzmanagement für HA-System

HA ist eine lizenzierte Funktion. Der System-Lizenzierungsschlüssel wird registriert, indem Sie die Schritte zum Hinzufügen von Lizenzen zum DD-System durchführen.

Ein System wird als Aktiv-Stand-by konfiguriert, wobei ein Node als „Stand-by“ vorgesehen ist. Statt einzelnen Lizenzen für jeden Node ist nur ein Satz von Lizenzen erforderlich. Während des Failover wird für die Lizenzen auf einem Node ein Failover auf den anderen Node durchgeführt.

Management des Systemspeichers

Mit den Funktionen für das Management des Systemspeichers können Sie den Status und die Konfiguration Ihres Speicherplatzes anzeigen, zur Identifizierung von Festplatten eine Festplatten-LED aufleuchten lassen und die Speicherkonfiguration ändern.

Hinweis

Der verbundene oder vom Aktiv-Stand-by-HA-System mit zwei Nodes verwendete Speicher kann als ein System angezeigt werden.

Anzeigen von Systemspeicherinformationen

Der Bereich „Storage Status“ zeigt den aktuellen Status des Speichers, wie Operational oder Non-Operational, und den Speichermigrationsstatus. Unter dem Bereich „Status“ befinden sich Registerkarten, die organisieren, wie der Speicherbestand dargestellt wird.

Vorgehensweise

1. Um den Speicherstatus anzuzeigen, wählen Sie **Hardware** > **Storage**.
2. Wenn ein Warnmeldungslink nach dem Speicherstatus angezeigt wird, klicken Sie auf den Link, um die Speicherwarnmeldungen anzuzeigen.
3. Wenn der Speichermigrationsstatus „Not licensed“ ist, können Sie auf **Add License** klicken, um die Lizenz für diese Funktion hinzuzufügen.

Registerkarte Overview

Auf der Registerkarte „Overview“ werden Informationen für alle Festplatten des Data Domain-Systems nach Typ organisiert angezeigt. Die angezeigten Kategorien hängen von der verwendeten Art der Speicherkonfiguration ab.

Auf der Registerkarte „Overview“ wird der erkannte Speicher in einem oder mehreren der folgenden Abschnitte angezeigt.

- Aktiver Tier

Festplatten im aktiven Tier sind aktuell als für das Dateisystem nutzbar markiert. Festplatten in zwei Tabellen aufgelistet: „Disks in Use“ und „Disks Not in Use“.

- Aufbewahrungs-Tier
  Wenn die optionale Data Domain Extended Retention-Lizenz (ehemals DD Archiver) installiert ist, wird in diesem Abschnitt angezeigt, dass die Laufwerke für DD Extended Retention-Speicher konfiguriert sind. Festplatten sind in zwei Tabellen aufgelistet: „Disks in Use“ und „Disks Not in Use“. Weitere Informationen finden Sie im *Data Domain Extended Retention Administration Guide*.
- Cache-Tier
  SSDs im Cache-Tier werden für das Zwischenspeichern von Metadaten verwendet. Die SSDs können nicht vom Dateisystem verwendet werden. Festplatten sind in zwei Tabellen aufgelistet: „Disks in Use“ und „Disks Not in Use“.
- Cloud-Tier
  Festplatten im Cloud-Tier dienen zum Speichern der Metadaten für Daten, die sich im Cloudspeicher befinden. Die Festplatten können nicht vom Dateisystem verwendet werden. Festplatten sind in zwei Tabellen aufgelistet: „Disks in Use“ und „Disks Not in Use“.
- Hinzufügbarer Speicher
  Bei Systemen mit optionalen Gehäusen werden in diesem Abschnitt die Laufwerke und Gehäuse angezeigt, die dem System hinzugefügt werden können.
- Ausgefallene/fremde/fehlende Festplatten (ohne Systemfestplatten)
  Zeigt die Festplatten an, die sich in einem Fehlerzustand befinden; diese können den aktiven oder Aufbewahrungs-Tiers des Systems nicht hinzugefügt werden.
- Systemfestplatten
  Zeigt die Festplatten an, auf denen sich das DD OS befindet, wenn der Data Domain-Controller keine Datenspeicherfestplatten enthält.
- Migrationsverlauf
  Zeigt den Verlauf von Migrationen an.

In jeder Abschnittsüberschrift wird eine Zusammenfassung des für diesen Abschnitt konfigurierten Speichers angezeigt. In der Zusammenfassung werden Zähler für die Gesamtzahl der Festplatten, der verwendeten Festplatten, der Ersatzfestplatten, der Festplatten für die Wiederherstellung, der verfügbaren Festplatten und der bekannten Festplatten angezeigt.

Klicken Sie auf die Plusschaltfläche (+), um ausführliche Informationen anzuzeigen, oder klicken Sie auf die Minusschaltfläche (-), um die ausführlichen Informationen auszublenden.

Tabelle 24 Beschreibungen zu den Bezeichnungen in der Spalte „Disks In Use“

Element	Beschreibung
Disk Group	Name der Laufwerksgruppe, die vom Dateisystem erstellt wurde (z. B. dg1)
State	Status des Laufwerks (beispielsweise Normal, Warning)
Disks Reconstructing	Laufwerke, für die eine Wiederherstellung durchgeführt wird, nach Laufwerks-ID (z. B. 1.11)
Total Disks	Gesamtzahl der nutzbaren Laufwerke (z. B. 14)
Disks	Laufwerks-IDs der nutzbaren Laufwerke (z. B. 2.1 bis 2.14)
Größe	Die Größe der Laufwerksgruppe (z. B. 25,47 TiB).

Tabelle 25 Beschreibungen zu den Bezeichnungen in der Spalte „Disks Not In Use“

Element	Beschreibung
Festplatte	Festplattenkennung (siehe unten) • Gehäuse- und Festplattennummer (in der Form Gehäuse Steckplatz) • Gerätenummer für ein logisches Gerät (wie von VTL und vDisk verwendete Geräte) • eine LUN
Slot	Gehäuse, in dem sich die Festplatte befindet
Pack	Festplattenpaket, 1–4, innerhalb des Gehäuses, in dem sich die Festplatte befindet. Dieser Wert ist nur bei DS60-Erweiterungseinschüben 2–4.
State	Status des Laufwerks, z. B. „In Use“, „Available“, „Spare“
Größe	Die Datenspeicherkapazität der Festplatte bei Verwendung auf einem Data Domain-System.[a]
Typ	Die Verbindung und der Typ der Festplatte (z. B. SAS).

a. Die Data Domain-Konvention für Computing-Speicherplatz definiert ein Gibibyte als 230 Byte und gibt damit eine andere Festplattenkapazität an als die Bewertung des Herstellers.

Registerkarte „Enclosures“

Die Registerkarte „Enclosures“ zeigt eine zusammenfassende Tabelle der Details der mit dem System verbundenen Gehäuse an.

In der Tabelle „Enclosures“ finden Sie die folgenden Details.

Tabelle 26 Beschreibung der Spaltenbezeichnungen für die Tabelle „Enclosures“

Element	Beschreibung
Enclosure	Die Gehäusenummer. Gehäuse 1 ist die Haupteinheit.
Serial Number	Die Seriennummer des Gehäuses.
Disks	Die im Gehäuse enthaltenen Festplatten, im Format *<Enclosure-number>*.1-*<Enclosure-number>*.*<N>*.
Model	Das Gehäusemodell. Bei Gehäuse 1 ist das Modell die Haupteinheit.
Disk Count	Die Anzahl der Festplatten im Gehäuse.
Size	Die Datenspeicherkapazität der Festplatte bei Verwendung auf einem Data Domain-System.[a]
Failed Disks	Die fehlgeschlagenen Festplatten im Gehäuse.
Temperature Status	Der Temperaturstatus des Gehäuses.

a. Die Data Domain-Konvention für Computing-Speicherplatz definiert ein Gibibyte als 230 Byte und gibt damit eine andere Laufwerkskapazität an als die Bewertung des Herstellers.

Registerkarte „Disks““

Auf der Registerkarte „Disks“ werden Informationen zu den einzelnen Systemfestplatten angezeigt. Sie können die angezeigten Festplatten so filtern, dass alle Festplatten, Festplatten in einem bestimmten Tier oder Festplatten in einer bestimmten Gruppe angezeigt werden.

In der Tabelle „Disk State“ wird eine Statusübersicht aller Systemfestplatten angezeigt.

Tabelle 27 Beschreibungen zu den Bezeichnungen in der Spalte „Disks State“

Element	Beschreibung
Gesamt	Die Gesamtzahl der in den Bestand aufgenommenen Festplatten im Data Domain-System
In Use	Die Anzahl der Festplatten, die derzeit vom Dateisystem verwendet werden
Spare	Die Anzahl der Ersatzfestplatten (verfügbar, um fehlerhafte Festplatten zu ersetzen)
Spare (reconstructing)	Die Anzahl der Festplatten, die sich gerade in der Datenrekonstruktion befinden (die Ersatzfestplatten, die fehlerhafte Festplatten ersetzen)
Available	Die Anzahl der Festplatten, die für die Zuweisung zu einer aktiven oder DD Extended Retention-Storage Tier verfügbar sind
Known	Die Anzahl der bekannten nicht zugewiesenen Festplatten
Unbekannt	Die Anzahl der unbekannten nicht zugewiesenen Festplatten
Failed	Die Anzahl der fehlerhaften Festplatten
Foreign	Die Anzahl der fremden Datenträger
Absent	Die Anzahl der fehlenden Festplatten
Migrating	Die Anzahl der Festplatten, die als Quelle für eine Speichermigration dienen.
Destination	Die Anzahl der Festplatten, die als Ziel für eine Speichermigration dienen.
Not Installed	Die Anzahl der leeren Festplattensteckplätze, die das System erkennen kann.

Die Tabelle „Disks“ enthält spezielle Informationen zu jeder im System installierten Festplatte.

Tabelle 28 Beschreibung der Spaltenbezeichnungen für die Tabelle „Disks“

Element	Beschreibung
Disk	Die Festplattenkennung, die Folgendes sein kann: • die Gehäuse- und die Laufwerksnummer (in der Form *Gehäuse.Steckplatz*) • Gerätenummer für ein logisches Gerät, wie ein von DD VTL und vDisk verwendetes Gerät

Tabelle 28 Beschreibung der Spaltenbezeichnungen für die Tabelle „Disks“ (Fortsetzung)

Element	Beschreibung
	• eine LUN
Slot	Gehäuse, in dem sich die Festplatte befindet
Pack	Festplattenpaket, 1–4, innerhalb des Gehäuses, in dem sich die Festplatte befindet. Dieser Wert ist nur bei DS60-Erweiterungseinschüben 2–4.
State	Status der Festplatte. Dabei sind folgende Status möglich. • Absent. An der angegebenen Position ist keine Festplatte installiert. • Available. Eine verfügbare Festplatte ist dem aktiven oder dem Aufbewahrungs-Tier zugewiesen, wird jedoch derzeit nicht verwendet. • Copy Recovery. Die Festplatte weist eine hohe Fehlerrate auf, ist jedoch nicht defekt. RAID kopiert momentan den Inhalt auf ein Ersatzlaufwerk und sortiert das Laufwerk nach Abschluss der Wiederherstellung mittels Kopie aus. • Destination. Die Festplatte wird als Ziel für die Speichermigration verwendet. • Error. Die Festplatte weist eine hohe Fehlerrate auf, ist jedoch nicht defekt. Die Festplatte befindet sich in der Warteschlange zur Wiederherstellung mittels Kopie. Der Status ändert sich in „Copy Recovery“, sobald die Wiederherstellung mittels Kopie beginnt. • Foreign. Die Festplatte wurde einem Tier zugewiesen. Laut Festplattendaten befindet sich die Festplatte jedoch möglicherweise im Besitz eines anderen Systems. • In-Use. Die Festplatte wird als Backupdatenspeicher verwendet. • Known. Bei der Festplatte handelt es sich um eine unterstützte Festplatte, die für die Zuweisung verfügbar ist. • Migrating. Die Festplatte wird als Quelle für die Speichermigration verwendet. • Powered Off. Die Festplatte wurde vom Support entfernt. • Reconstruction. Die Festplatte wird als Reaktion auf einen `disk fail`-Befehl oder auf Anweisung von RAID/SSM wiederhergestellt. • Spare. Die Festplatte ist für die Verwendung als Ersatz verfügbar. • System. Auf Systemfestplatten werden DD OS-Daten und Systemdaten gespeichert. Backupdaten werden auf Systemfestplatten nicht gespeichert. • Unknown. Eine unbekannte Festplatte wird dem aktiven oder dem Aufbewahrungs-Tier nicht zugewiesen.

Tabelle 28 Beschreibung der Spaltenbezeichnungen für die Tabelle „Disks“ (Fortsetzung)

Element	Beschreibung
	Möglicherweise wurde sie vom Administrator oder vom RAID-System aussortiert.
Manufacturer/Model	Die Modellbezeichnung des Herstellers. Die Anzeige umfasst eine Modell-ID oder einen RAID-Typ oder anderen Daten, je nach Anbieterzeichenfolge, die vom Speicherarray gesendet wird.
Firmware	Die Firmwareversion, die vom Speicher-Controller der physischen Festplatte des Drittanbieters verwendet wird.
Serial Number	Die Seriennummer des Herstellers der Festplatte.
Disk Life Used	Der Prozentsatz der verbrauchten bewerteten Lebensdauer einer SSD.
Type	Die Verbindung und der Typ der Festplatte (z. B. SAS).

Registerkarte „Reconstruction“

Die Registerkarte „Reconstruction“ zeigt eine Tabelle, die zusätzliche Informationen zum Rekonstruieren von Festplatten enthält.

In der folgenden Tabelle werden die Einträge in der Tabelle „Reconstruction“ beschrieben.

Tabelle 29 Beschreibung der Spaltenbezeichnungen für die Tabelle „Reconstruction“

Element	Beschreibung
Festplatte	Identifiziert Festplatten, die gerade wiederhergestellt werden. Festplattenbezeichnungen haben das Format *enclosure.disk*. Gehäuse 1 ist das Data Domain-System und externe Gehäuse starten mit der Nummerierung bei Gehäuse 2. Beispielsweise ist die Bezeichnung 3.4 die vierte Festplatte im zweiten Gehäuse.
Disk Group	Zeigt die RAID-Gruppe (dg#) für die Wiederherstellungsfestplatte an
Tier	Der Name des Tier, in dem die fehlerhafte Festplatte wiederhergestellt wird
Time Remaining	Die Zeit vor Abschluss der Wiederherstellung
Percentage Complete	Der Prozentsatz der bereits abgeschlossenen Wiederherstellung.

Wenn eine Ersatzfestplatte verfügbar ist, ersetzt das Dateisystem automatisch eine fehlerhafte Festplatte durch eine Ersatzfestplatte und beginnt den Wiederherstellungsprozess, um die Ersatzfestplatte in die RAID-Festplattengruppe zu integrieren. Die Festplattenverwendung zeigt `Spare` an und der Status wird `Reconstructing`. Die Rekonstruction erfolgt jeweils auf einer Festplatte.

Physische Suche nach einem Gehäuse

Wenn Sie Probleme haben, zu bestimmen, welches physische Gehäuse einem Gehäuse in DD System Manager entspricht, können Sie die CLI-Beacon-Funktion verwenden. LEDs zur Gehäuse-Identifizierung und alle Festplatten-LEDs, die auf einen Normalbetrieb hinweisen, blinken.

Vorgehensweise

1. Stellen Sie eine CLI-Sitzung mit dem System her.
2. Geben Sie `enclosure beacon` *enclosure* ein.
3. Drücken Sie `Strg+C`, um das Blinken der LED zu stoppen.

Physische Suche nach einer Festplatte

Wenn Sie Schwierigkeiten haben, zu erkennen, welche physische Festplatte einer in DD System Manager angezeigten Festplatte entspricht, können Sie die Beacon-Funktion verwenden, um an der physischen Festplatte eine LED aufleuchten zu lassen.

Vorgehensweise

1. Wählen Sie **Hardware** > **Storage** > **Disks**.
2. Wählen Sie eine **Disks** aus der Tabelle aus und klicken Sie auf **Beacon**.

   Hinweis

   Sie können jeweils nur eine Festplatte auswählen.

   Das Dialogfeld „Beaconing Disk“ wird eingeblendet und das LED-Licht der Festplatte beginnt zu blinken.

3. Klicken Sie auf **Stop**, um das LED-Beaconing anzuhalten.

Konfigurieren eines Speichers

Mithilfe von Speicherkonfigurationsfunktionen können Sie Speichererweiterungsgehäuse zu den aktiven, den Aufbewahrungs- und den Cloud-Tiers hinzufügen bzw. daraus entfernen. Speicher in einem Erweiterungsgehäuse (manchmal Erweiterungseinschub) kann erst nach dem Hinzufügen zu einem Tier verwendet werden.

Hinweis

Für zusätzlichen Speicher sind die entsprechenden Lizenzen sowie genügend Arbeitsspeicher zur Unterstützung der neuen Speicherkapazität erforderlich. Es werden Fehlermeldungen angezeigt, wenn mehr Lizenzen oder Arbeitsspeicher erforderlich ist/sind.

DD6300-Systeme unterstützen die Option zur Verwendung von ES30-Gehäusen mit 4-TB-Laufwerken (43,6 TiB) bei 50 % Auslastung (21,8 TiB) im aktiven Tier, wenn die verfügbare lizenzierte Kapazität genau 21,8 TiB beträgt. Die folgenden Richtlinien gelten für die Verwendung von partiellen Kapazitätseinschüben.

- Für die Verwendung von partieller Kapazität werden keine anderen Gehäusetypen oder Laufwerksgrößen unterstützt.
- Ein partieller Einschub kann nur im aktiven Tier vorhanden sein.

- Im aktiven Tier kann nur ein partieller ES30 vorhanden sein.
- Sobald ein partieller Einschub in einem Tier vorhanden ist, können keine zusätzlichen ES30s in diesem Tier konfiguriert werden, bis der partielle Einschub bei voller Kapazität hinzugefügt wird.

Hinweis

Dies erfordert die Lizenzierung von ausreichend zusätzlicher Kapazität, um die verbleibenden 21,8 TiB des partiellen Einschubs zu verwenden.

- Wenn die verfügbare Kapazität 21,8 TB überschreitet, kann kein partieller Einschub hinzugefügt werden.
- Das Löschen einer 21-TiB-Lizenz konvertiert einen vollständig genutzen Einschub nicht automatisch in einen partiellen Einschub. Der Einschub muss entfernt und wieder als partieller Einschub hinzugefügt werden.

Vorgehensweise

1. Wählen Sie **Hardware** > **Storage** > **Overview** aus.
2. Erweitern Sie das Dialogfeld für einen der verfügbaren Storage Tiers:
   - **Aktiver Tier**
   - **Extended Retention-Tier**
   - **Cache-Tier**
   - **Cloud-Tier**
3. Klicken Sie auf **Configure**.
4. Wählen Sie im Dialogfeld „Configure Storage“ den hinzuzufügenden Speicher aus der Liste **Addable Storage** aus.
5. Wählen Sie in der Liste **Configure** entweder **Active Tier** oder **Retention Tier**.

   Die maximale Speichermenge, die zum aktiven Tier hinzugefügt werden kann, hängt vom verwendeten DD-Controller ab.

   Hinweis

   Die Leiste der lizenzierten Kapazität zeigt den Umfang der lizenzierten Kapazität (verwendet und verbleibend) für die installierten Gehäuse an.

6. Aktivieren Sie das Kontrollkästchen für den Einschub, der hinzugefügt werden soll.
7. Klicken Sie auf die Schaltfläche **Add to Tier**.
8. Klicken Sie auf **OK**, um den Speicher hinzuzufügen.

   Hinweis

   Wenn Sie einen hinzugefügten Einschub entfernen möchten, wählen Sie ihn in der Liste „Tier Configuration“ aus, klicken Sie **Remove from Configuration** und klicken Sie dann auf **OK**.

DD3300-Kapazitätserweiterung

Das DD3300-System ist in drei verschiedenen Kapazitätskonfigurationen verfügbar. Kapazitätserweiterungen von einer Konfiguration zu einer anderen werden unterstützt.

Das DD3300-System ist in den folgenden Kapazitätskonfigurationen verfügbar:

- 4 TB
- 16 TB
- 32 TB

Beachten Sie die folgenden Überlegungen zu Upgrades:

- Ein 4-TB-System kann auf 16 TB erweitert werden.
- Ein 16-TB-System kann auf 32 TB erweitert werden.
- Es besteht kein Upgradepfad von 4 TB auf 32 TB.

Wählen Sie **Maintenance** > **System**, um auf Informationen über die Kapazitätserweiterung zuzugreifen und um den Kapazitätserweiterungsprozess zu initiieren.

Die Kapazitätserweiterung ist ein einmaliger Prozess. Der Bereich **Capacity Expansion History** wird unabhängig davon angezeigt, ob das System bereits erweitert wurde. Wenn das System nicht erweitert wurde, klicken Sie auf die Schaltfläche **Capacity Expand**, um die Kapazitätserweiterung zu initiieren.

Alle Kapazitätserweiterungen erfordern die Installation von zusätzlichen Festplatten und zusätzlichem Arbeitsspeicher im System. Versuchen Sie nicht, die Kapazität zu erweitern, bis die Hardwareupgrades abgeschlossen sind. Die folgende Tabelle führt die Hardwareupgradeanforderungen für die Kapazitätserweiterung auf.

Kapazitätserweiterung	Zusätzlicher Speicher	Zusätzliche HDDs	Zusätzliche SSD
4 TB bis 16 TB	32 GB	6 x 4 TB große HDDs	1 x 480 GB große SSD
16 TB bis 32 TB	16 GB	6 x 4 TB große HDDs	–

Der *Data Domain DD3300 Field Replacement and Upgrade Guide* enthält detaillierte Anweisungen für die Kapazitätserweiterung des Systems.

Kapazitätserweiterung

Wählen Sie die Zielkapazität aus der Drop-down-Liste **Select Capacity** aus. Die Kapazitätserweiterung kann verhindert werden, wenn ein nicht ausreichender Arbeitsspeicher oder eine nicht ausreichende physische Kapazität (HDDs) vorliegen, wenn das System bereits erweitert wurde oder wenn das Ziel für die Kapazitätserweiterung nicht unterstützt wird. Wenn die Erweiterung der Speicherkapazität nicht abgeschlossen werden kann, wird der Grund hier angezeigt.

Kapazitätserweiterungsverlauf

Die Tabelle **Capactiy Expansion History** zeigt die Details zur Kapazität des Systems an. Die Tabelle enthält die Kapazität des Systems, zum Zeitpunkt der ursprünglichen Softwareinstallation und das Datum der ersten Softwareinstallation. Wenn die Kapazität erweitert wurde, enthält die Tabelle auch die erweiterte Kapazität und das Datum, an dem die Erweiterung durchgeführt wurde.

Erzeugen eines Laufwerksausfalls und Wiederinbetriebnahme

Mit der Funktion „Disk Fail“ können Sie eine Festplatte manuell auf einen fehlerhaften Zustand einstellen, um die Rekonstruktion der auf der Festplatte gespeicherten Daten zu erzwingen. Mit der Funktion „Disk Unfail“ können Sie eine Festplatte in einen fehlerhaften Zustand bringen und sie wieder in Betrieb nehmen.

Erzeugen eines Laufwerksausfalls

Erzeugt einen Laufwerksausfall und erzwingt eine Wiederherstellung. Wählen Sie **Hardware** > **Storage** > **Disks** > **Fail**.

Wiederinbetriebnahme einer Festplatte

Mit dem Befehl „Unfail a disk“ wird ein Laufwerk, dessen Status zuvor „Failed“ oder „Foreign“ lautete, für das System verwendbar. Wählen Sie **Hardware** > **Storage** > **Disks** > **Unfail**.

Netzwerkverbindungsmanagement

Mithilfe der Funktionen für das Management von Netzwerkverbindungen können Sie Netzwerkschnittstellen, allgemeine Netzwerkeinstellungen und Netzwerkrouten anzeigen und konfigurieren.

Netzwerkverbindungsmanagement für HA-System

Das HA-System basiert auf zwei verschiedenen Typen von IP-Adressen: Fixed und Floating. Jeder Typ hat bestimmte Verhaltensweisen und Beschränkungen.

Auf einem HA-System gilt für Fixed IP-Adressen Folgendes:

- Werden für das Node-Management über die CLI verwendet
- Sind mit dem Node verknüpft
- Können statisch oder DHCP, IPv6 SLAAC sein
- Konfiguration erfolgt auf dem Node mit dem optionalen Argument `type fixed`

Hinweis

Der gesamte Dateisystemzugriff sollte über eine Floating IP-Adresse erfolgen.

Floating IP-Adressen existieren nur auf dem HA-System mit zwei Nodes; während des Failover wird die IP-Adresse vom neuen aktiven Node übernommen und es gilt Folgendes:

- Nur auf dem aktiven Node konfiguriert
- Für Dateisystemzugriff und die meisten Konfiguration verwendet
- Nur statisch
- Konfiguration erfordert das Argument `type floating`

Management von Netzwerkschnittstellen

Mithilfe der Funktionen für das Management von Netzwerkschnittstellen können Sie die physischen Schnittstellen managen, über die das System mit einem Netzwerk

verbunden ist, und Sie können logische Schnittstellen erstellen, um Linkzusammenfassung, Lastenausgleich und Link- oder Node Failover zu unterstützen.

Anzeigen von Schnittstelleninformationen

Mit der Registerkarte „Interfaces“ können Sie physische und virtuelle Schnittstellen, VLANs, DHCP, DDNS und IP-Adressen und -Aliase managen.

Beachten Sie beim Managen von IPv6-Schnittstellen die folgenden Richtlinien.

- Die Befehlszeilenoberfläche (CLI) unterstützt IPv6 für grundlegende Data Domain-Netzwerk- und -Replikationsbefehle, aber nicht für Backup- und DD Extended Retention-Befehle (`archive`). CLI-Befehle managen die IPv6-Adressen. Sie können IPv6-Adressen über den DD System Manager anzeigen, IPv6 aber nicht mit dem DD System Manager managen.
- Sammel-, Verzeichnis- und MTree-Replikationen werden über IPv6-Netzwerke unterstützt, sodass Sie den IPv6-Adressbereich nutzen können. Eine gleichzeitige Replikation über IPv6- und IPv4-Netzwerke wird ebenfalls unterstützt, ebenso wie die gemanagte Dateireplikation über DD Boost.
- Es gelten einige Einschränkungen für Schnittstellen mit IPv6-Adressen. Beispielsweise ist die Minimum-MTU 1280. Wenn Sie versuchen, den MTU-Wert auf einer Schnittstelle mit einer IPv6-Adresse auf weniger als 1280 festzulegen, wird eine Fehlermeldung angezeigt und die Schnittstelle vom Service entfernt. Eine IPv6-Adresse kann sich auf eine Schnittstelle auswirken, selbst wenn sie sich in einem mit der Schnittstelle verbundenen VLAN und nicht direkt auf der Schnittstelle befindet.

Vorgehensweise

1. Wählen Sie**Hardware** > **Ethernet** > **Interfaces**.

   In der folgenden Tabelle sind die Informationen auf der Registerkarte „Interfaces“ beschrieben.

   Tabelle 30 Beschreibungen zu den Bezeichnungen der Registerkarte „Interface“

Element	Beschreibung
Schnittstelle	Name jeder mit dem ausgewählten System verbundenen Schnittstelle
Aktiviert	Ob die Schnittstelle aktiviert ist. • Wählen Sie **Yes** aus, um die Schnittstelle zu aktivieren und sie mit dem Netzwerk zu verbinden. • Wählen Sie **No** aus, um die Schnittstelle zu deaktivieren und sie vom Netzwerk zu trennen.
DHCP	Gibt an, ob die Schnittstelle manuell konfiguriert ist (`no`), von einem DHCP-IPv4-Server (Dynamic Host Configuration Protocol) (`v4`) oder von einem DHCP-IPv6-Server (`v6`).
IP-Adresse	Die mit der Schnittstelle verbundene IP-Adresse. Die Adresse wird vom Netzwerk verwendet, um die Schnittstelle zu identifizieren. Wenn die Schnittstelle über DHCP konfiguriert ist, wird nach diesem Wert ein Sternchen angezeigt.
Netzmaske	Die mit der Schnittstelle verbundene Netzmaske. Verwendet das Standardformat für IP-Netzwerkmasken. Wenn die Schnittstelle

Tabelle 30 Beschreibungen zu den Bezeichnungen der Registerkarte „Interface“ (Fortsetzung)

Element	Beschreibung
	über DHCP konfiguriert ist, wird nach diesem Wert ein Sternchen angezeigt.
Link	Gibt an, ob die Ethernetverbindung aktiv ist („Yes“/„No“).
Address Type	Auf einem HA-System sind die Adresstypen Fixed, Floating oder Interconnect.
Additional Info	Zusätzliche Einstellungen für die Schnittstelle. Beispielsweise der Bonding-Modus.
IPMI interfaces configured	Zeigt „Yes“ oder „No“ an und gibt an, ob die IPMI-Integritätsüberwachung und das Energiemanagement für die Schnittstelle konfiguriert sind.

2. Wenn Sie die Schnittstellenliste nach Schnittstellenname filtern möchten, geben Sie im Feld **Interface Name** einen Wert ein und klicken Sie auf **Update**.

   Filter unterstützen Platzhalter, z. B. „eth*“, „veth*“ oder „eth0*“.

3. Wenn Sie die Schnittstellenliste nach Schnittstellentyp filtern möchten, wählen Sie im Menü **Interface Type** einen Wert aus und klicken Sie auf **Update**.

   Auf einem HA-System gibt es ein Filter-Drop-down-Feld, um nach IP-Adresstyp (Fixed, Floating oder Interconnect) zu filtern.

4. Um in der Tabelle „Interfaces“ zur Standardliste zurückzukehren, klicken Sie auf **Reset**.
5. Wählen Sie eine Schnittstelle aus der Tabelle aus, um den Bereich mit den Schnittstellendetails zu füllen.

Tabelle 31 Beschreibungen zu den Bezeichnungen für Schnittstellendetails

Element	Beschreibung
Auto-generated Addresses	Zeigt die automatisch erzeugten IPv6-Adressen für die ausgewählte Schnittstelle an.
Auto Negotiate	Wenn diese Funktion `Enabled` anzeigt, verhandelt die Schnittstelle automatisch über Geschwindigkeits- und Duplexeinstellungen. Wenn diese Funktion `Disabled` anzeigt, müssen die Werte für Geschwindigkeit und Duplex manuell festgelegt werden.
Cable	Zeigt, ob die Schnittstelle Kupfer oder Glasfaser ist. **Hinweis** Einige Schnittstellen müssen in Betrieb sein, bevor der Kabelstatus gültig ist.
Duplex	Wird in Verbindung mit dem Geschwindigkeitswert verwendet, um das Datenübertragungsprotokoll festzulegen. Optionen sind „Unknown“, „Full“ und „Half“.
Hardware Address	Die MAC-Adresse der ausgewählten Schnittstelle. Beispiel: 00:02:b3:b0:8a:d2.

Tabelle 31 Beschreibungen zu den Bezeichnungen für Schnittstellendetails (Fortsetzung)

Element	Beschreibung
Interface Name	Name der ausgewählten Schnittstelle
Latent Fault Detection (LFD) – nur HA-Systeme	Das LFD-Feld weist den Link `View Configuration` mit einem Pop-up auf, das LFD-Adressen und -Schnittstellen auflistet.
Maximum Transfer Unit (MTU)	MTU-Wert, der der Schnittstelle zugewiesen ist.
Geschwindigkeit	Wird in Verbindung mit dem Duplexwert verwendet, um die Datenübertragungsrate festzulegen. Optionen sind „Unknown“, „10 Mb/s“, „100 Mb/s“, „1000 Mb/s“ und „10 Gb/s“. **Hinweis** Automatisch ausgehandelte Schnittstellen müssen konfiguriert werden, bevor die Werte für Geschwindigkeit, Duplex und unterstützte Geschwindigkeit angezeigt werden.
Supported Speeds	Listet alle Geschwindigkeiten auf, die die Schnittstelle verwenden kann.

6. Um die Konfiguration der IPMI-Schnittstelle und Managementoptionen anzuzeigen, klicken Sie auf **View IPMI Interfaces**.

   Dieser Link zeigt Informationen zu **Maintenance** > **IPMI**.

Namen und Einschränkungen physischer Schnittstellen

Das Format von Namen physischer Schnittstellen variieren auf verschiedenen Data Domain-Systemen und optionalen Karten und für einige Schnittstellen gelten bestimmte Einschränkungen:

- Für die meisten Systeme ist das Namensformat für physische Schnittstellen `eth`*xy*, wobei *x* die Steckplatznummer für einen integrierten Port oder eine optionale Karte ist und *y* eine alphanumerische Zeichenfolge. Beispiel: eth0a.
- Für die meisten integrierten vertikalen NIC-Schnittstellen wird die oberste Schnittstelle eth0a und die unterste Schnittstelle eth0b genannt.
- Für die meisten integrierten horizontalen NIC-Schnittstellen wird die linke Schnittstelle (von hinten betrachtet) eth0a und die rechte eth0b genannt.
- DD990-Systeme haben vier integrierte Schnittstellen: zwei oben und zwei unten. Die Schnittstelle oben links ist eth0a und die oben rechts eth0b, die unten links ist eth0c und die unten rechts eth0d.
- DD2200-Systeme haben vier integrierte 1G-Base-T-NIC-Ports: ethMa (oben links), ethMb (oben rechts), ethMc (unten links) und ethMd (unten rechts).
- DD2500-Systeme haben sechs integrierte Schnittstellen. Die vier integrierten 1G-Base-T-NIC-Ports sind ethMa (oben links), ethMb (oben rechts), ethMc (unten links) und ethMd (unten rechts). Die beiden integrierten 10G-Base-T-NIC-Ports sind ethMe (oben) und ethMf (unten).
- DD4200-, DD4500- und DD7200-Systeme haben einen integrierten Ethernetport, der ethMa ist.

- Bei Systemen zwischen DD140 und DD990 beginnen die Namen der physischen Schnittstellen für I/O-Module am oberen oder linken Rand des Moduls. Die erste Schnittstelle ist ethxa, die nächste ist ethxb, die nächste ist ethxc usw.
- Die Portnummern auf dem horizontalen DD2500-I/O-Modul werden sequenziell vom Ende gegenüber dem Modulgriff (links) bezeichnet. Der erste Port wird als 0 bezeichnet und entspricht dem Namen der physischen Schnittstelle ethxa, der nächste ist 1/ethxb, der nächste ist 2/ethxc usw.
- Die Portnummern auf den vertikalen DD4200-, DD4500- und DD7200-I/O-Modulen werden sequenziell vom Ende gegenüber dem Modulgriff (unten) bezeichnet. Der erste Port wird als 0 bezeichnet und entspricht dem Namen der physischen Schnittstelle ethxa, der nächste ist 1/ethxb, der nächste ist 2/ethxc usw.

Richtlinien zur allgemeinen Schnittstellenkonfiguration

Überprüfen Sie vor dem Konfigurieren von Systemschnittstellen die Richtlinien zur allgemeinen Schnittstellenkonfiguration.

- Wenn sowohl Backup- als auch Replikationsdatenverkehr unterstützt werden, verwenden Sie separate Schnittstellen für jede Datenverkehrsart (wenn möglich), damit diese sich nicht gegenseitig beeinträchtigen.
- Wenn der Replikationsdatenverkehr voraussichtlich weniger als 1 Gbit/s beträgt, verwenden Sie keine 10-GbE-Schnittstellen für den Replikationsdatenverkehr (wenn möglich), da 10-GbE-Schnittstellen für schnelleren Datenverkehr optimiert sind.
- Wenn ein Data Domain-Service einen nicht standardmäßigen Port verwendet und möchte, dass der Benutzer ein Upgrade auf DD OS 6.0 durchführt, oder der Benutzer einen Service in einen nicht standardmäßigen Port auf einem System mit DD OS 6.0 ändern möchte, fügen Sie eine Netzwerkfilterfunktion für alle Clients mit diesem Service hinzu, um den Client-IP-Adressen die Verwendung des neuen Ports zu ermöglichen.
- Bei DD4200-, DD4500- und DD7200-Systemen, die IPMI verwenden, reservieren Sie die Schnittstelle ethMa für IPMI-Datenverkehr und Management-Datenverkehr (mit Protokollen wie HTTP, Telnet und SSH), wenn möglich. Backupdatenverkehr sollten an andere Schnittstellen weitergeleitet werden.

Konfigurieren von physischen Schnittstellen

Sie müssen mindestens eine physische Schnittstelle konfigurieren, damit das System eine Verbindung mit einem Netzwerk herstellen kann.

Vorgehensweise

1. Wählen Sie **Hardware** > **Ethernet** > **Interfaces**.
2. Wählen Sie eine zu konfigurierende Schnittstelle aus.

   Hinweis

   Die Systeme DD140, DD160, DD610, DD620 und DD630 bieten keinen Support für IPv6 auf der Schnittstelle eth0a (eth0 auf Systemen mit Legacy-Portnamen) oder auf einem beliebigen VLAN, das auf dieser Schnittstelle erstellt wurde.

3. Klicken Sie auf **Konfigurieren**.

4. Bestimmen Sie im Dialogfeld „Configure Interface“, wie die IP-Adresse der Schnittstelle festgelegt werden soll:

   Hinweis

   In einem HA-System weist das Dialogfeld „Configure Interface“ ein Feld für das Festlegen der Floating IP auf (Yes/No). Bei Auswahl von **Yes** wird das Optionsfeld `Manually Configure IP Address` automatisch aktiviert; Floating IP-Schnittstellen können nur manuell konfiguriert werden.

   - Zuweisen der IP-Adresse mit DHCP: Wählen Sie im Bereich „IP Settings“ die Option **Obtain IP Address using DHCP** und dann entweder **DHCPv4** für IPv4-Zugriff oder **DHCPv6** für IPv6-Zugriff aus.
     Das Festlegen einer physischen Schnittstelle für die Verwendung von DHCP aktiviert die Schnittstelle automatisch.

     Hinweis

     Wenn Sie die Netzwerkeinstellungen über DHCP abrufen, können Sie den Hostnamen manuell unter **Hardware** > **Ethernet** > **Settings** oder mit dem Befehl `net set hostname` konfigurieren. Sie müssen den Hostnamen manuell konfigurieren, wenn Sie DHCP über IPv6 verwenden.

   - Manuelle Angabe der IP-Einstellungen: Wählen Sie im Bereich „IP Settings“ die Option **Manually configure IP Address**.
     Die Felder **IP Address** und **Netmask** werden aktiviert.

5. Wenn Sie die IP-Adresse manuell eingeben möchten, geben Sie eine IPv4- oder IPv6-Adresse ein. Wenn Sie eine IPv4-Adresse eingegeben haben, geben Sie eine Netzmaskenadresse ein.

   Hinweis

   Sie können einer Schnittstelle mit diesem Verfahren nur eine IP-Adresse zuweisen. Wenn Sie eine andere IP-Adresse zuweisen, ersetzt die neue IP-Adresse die alte IP-Adresse. Um einer Schnittstelle eine zusätzliche IP-Adresse hinzuzufügen, erstellen Sie einen IP-Alias.

6. Geben Sie Geschwindigkeits-/Duplexeinstellungen an.

   Die Kombination aus Geschwindigkeits- und Duplexeinstellungen definiert die Datenübertragungsrate für die Schnittstelle. Wählen Sie eine der folgenden Optionen:

   - **Autonegotiate Speed/Duplex**: Wählen Sie diese Option, um der Netzwerkschnittstelle das automatische Verhandeln der Übertragungsgeschwindigkeit und Duplexeinstellung für eine Schnittstelle zu ermöglichen. Autonegotiation wird auf den folgenden DD2500-, DD4200-, DD4500- und DD7200-I/O-Modulen *nicht* unterstützt:
     - Optisches 10GbE-SR-Modul mit zwei Ports und LC-Anschlüssen (mit SFPs)
     - Direct-Attached-10GbE-Modul aus Kupfer (SFP+-Kabel)
     - 1GbE-Modul aus Kupfer (RJ45) / optisches 1GbE-SR-Modul mit zwei Ports

- **Manually configure Speed/Duplex**: Wählen Sie diese Option, wenn Sie die Datenübertragungsrate für eine Schnittstelle manuell festlegen möchten. Wählen Sie Geschwindigkeit und Duplex in den Menüs aus.
  - Die Duplexoptionen sind „half-duplex“, „full-duplex“ und „unknown“.
  - Die aufgeführten Geschwindigkeitsoptionen sind auf die Funktionen des Hardware-Geräts begrenzt. Die Optionen sind 10 Mbit, 100 Mbit, 1000 Mbit (1 Gbit), 10 Gbit und „unknown“. Die 10G Base-T-Hardware unterstützt nur die Einstellungen 100 Mbit, 1000 Mbit und 10 Gbit.
  - Halbduplex ist nur für die Geschwindigkeiten 10 Mbit, 100 Mbit verfügbar.
  - Leitungsgeschwindigkeiten von 1000 Mbit und 10 Gbit benötigen Vollduplex.
  - Auf den 10GbE-I/O-Modulen DD2500, DD4200, DD4500 und DD7200 unterstützen die Kupferschnittstellen nur die 10-Gbit-Geschwindigkeitseinstellung.
  - Die Standardeinstellung für 10G Base-T-Schnittstellen ist „Autonegotiate Speed/Duplex“. Wenn Sie manuell die Geschwindigkeit auf 1000 Mbit oder 10 Gbit festlegen, müssen Sie die Duplexeinstellung auf „Full“ festlegen.

7. Geben Sie die MTU-Größe (maximale Übertragungseinheit) für die physische (Ethernet-)Schnittstelle an.

   Gehen Sie folgendermaßen vor:

   - Klicken Sie auf die Schaltfläche **Default**, um für diese Einstellung wieder den Standardwert zu verwenden.
   - Sorgen Sie dafür, dass alle Ihre Netzwerkkomponenten die für diese Größe eingestellte Option unterstützen.

8. Wählen Sie bei Bedarf die Option **Dynamic DNS Registration**.

   Dynamic DNS (DDNS) ist ein Protokoll, das lokale IP-Adressen auf einem Domain Name System(DNS)-Server registriert. In dieser Version unterstützt DD System Manager DDNS im Windows-Modus. Um DDNS im UNIX-Modus zu verwenden, verwenden Sie den Befehl `net ddns`.

   Das DDNS muss registriert werden, damit diese Option aktiviert wird.

   Hinweis

   Diese Option deaktiviert DHCP für diese Schnittstelle.

9. Klicken Sie auf **Next**.

   Die Übersichtsseite „Configure Interface Settings““ wird angezeigt. Die aufgelisteten Werte spiegeln den neuen System- und Schnittstellenstatus wider, der angewendet wird, nachdem Sie auf „Finish“ klicken.

10. Klicken Sie auf **Finish** und **OK.**

Werte für die MTU-Größe

Die MTU-Größe muss zur Optimierung der Performance einer Netzwerkverbindung sorgfältig festgelegt werden. Eine falsche MTU-Größe kann sich negativ auf die Performance der Schnittstelle auswirken.

Unterstützte Werte für das Festlegen der MTU-Größe (Maximum Transmission Unit) für die physische Schnittstelle (Ethernet) liegen zwischen 350 und 9000. Für 100 Base-T- und Gigabit-Netzwerke ist 1500 der Standardwert.

Hinweis

Die minimale MTU für IPv6-Schnittstellen ist 1280. Die Schnittstelle schlägt fehl, wenn Sie versuchen, die MTU auf einen niedrigeren Wert als 1280 festzulegen.

Verschieben einer statischen IP-Adresse

Eine bestimmte statische IP-Adresse darf nur einer Schnittstelle auf einem System zugewiesen werden. Eine statische IP-Adresse muss von einer Schnittstelle ordnungsgemäß entfernt werden. Erst dann kann sie auf einer anderen Schnittstelle konfiguriert werden.

Vorgehensweise

1. Wenn die Schnittstelle, die die statische IP-Adresse hostet, Teil einer DD Boost-Schnittstellengruppe ist, entfernen Sie die Schnittstelle aus dieser Gruppe.
2. Wählen Sie **Hardware** > **Ethernet** > **Interfaces**.
3. Entfernen Sie die statische IP-Adresse, die Sie verschieben möchten.
   a. Wählen Sie die Schnittstelle aus, die derzeit die IP-Adresse verwendet, die Sie verschieben möchten.
   b. Wählen Sie in der Spalte „Enabled“ die Option **No**, um die Schnittstelle zu deaktivieren.
   c. Klicken Sie auf **Configure**.
   d. Legen Sie die IP-Adresse auf 0 fest.

      Hinweis

      Legen Sie die IP-Adresse auf 0 fest, wenn keine andere IP-Adresse vorhanden ist, die der Schnittstelle zugewiesen werden soll. Die IP-Adresse darf nicht mehreren Schnittstellen zugewiesen werden.

   e. Klicken Sie auf **Next** und dann auf **Finish**.
4. Fügen Sie die entfernte statische IP-Adresse einer anderen Schnittstelle hinzu.
   a. Wählen Sie die Schnittstelle aus, in die die IP-Adressen verschoben werden sollen.
   b. Wählen Sie in der Spalte „Enabled“ die Option **No**, um die Schnittstelle zu deaktivieren.
   c. Klicken Sie auf **Configure**.
   d. Legen Sie die IP-Adresse auf die statische IP-Adresse fest, die Sie entfernt haben.
   e. Klicken Sie auf **Next** und dann auf **Finish**.
   f. Wählen Sie in der Spalte „Enabled“ die Option **Ja**, um die aktualisierte Schnittstelle zu aktivieren.

Richtlinien zur Konfiguration von virtuellen Schnittstellen

Die Richtlinien zur Konfiguration von virtuellen Schnittstellen gelten sowohl für virtuelle Failover-Schnittstellen als auch für aggregierte virtuelle Schnittstellen. Es

gibt weitere Richtlinien, die entweder für Failover-Schnittstellen oder für aggregierte Schnittstellen, aber nicht für beide gelten.

- Der *virtual-name* muss das Format `veth`*x* haben, wobei *x* eine Zahl ist. Die empfohlene höchste Zahl ist 99 aufgrund der Namengrößeneinschränkungen.
- Sie können beliebig viele virtuelle Schnittstellen erstellen, wie physische Schnittstellen vorhanden sind.
- Jede Schnittstelle, die in einer virtuellen Schnittstelle verwendet wird, muss zuerst deaktiviert werden. Eine Schnittstelle, die Teil einer virtuellen Schnittstelle ist, wird als deaktiviert für andere Optionen der Netzwerkkonfiguration angesehen.
- Nachdem eine virtuelle Schnittstelle gelöscht wurde, bleiben die zugehörigen physischen Schnittstellen deaktiviert. Sie müssen die physischen Schnittstellen manuell erneut aktivieren.
- Die Anzahl und der Typ der installierten Karten legen die Anzahl der verfügbaren Ethernetports fest.
- Jede physische Schnittstelle kann einer virtuellen Schnittstelle angehören.
- Ein System kann mehrere gemischte virtuelle Failover- und aggregierte Schnittstellen unterstützen, abhängig von den oben genannten Einschränkungen.
- Virtuelle Schnittstellen müssen aus identischen physischen Schnittstellen erstellt werden. Beispielsweise alle Kupfer, alle optisch, alle 1 Gbit oder alle 10 Gbit. 1-Gbit-Schnittstellen unterstützen jedoch die Verknüpfung einer Kombination aus Kupferkabelschnittstellen und optischen Schnittstellen. Dies gilt für virtuelle Schnittstellen auf mehreren Karten mit identischen physischen Schnittstellen, außer für Chelsio-Karten. Für Chelsio-Karten wird nur Failover unterstützt, und das nur für Schnittstellen auf derselben Karte.
- Failover- und aggregierte Links verbessern die Netzwerkperformance und Ausfallsicherheit, indem zwei oder mehr Netzwerkschnittstellen parallel genutzt werden. So werden die Geschwindigkeit für aggregierte Links und die Zuverlässigkeit einer einzigen Schnittstelle gesteigert.
- Die Entfernungsfunktion steht über die Schaltfläche **Configure** zur Verfügung. Klicken Sie auf eine virtuelle Schnittstelle in der Liste der Schnittstellen auf die Registerkarte „Interfaces“ und dann auf **Configure**. Deaktivierten Sie in der Liste der Schnittstellen im Dialogfeld das Kontrollkästchen für die zu entfernende Schnittstelle, um sie aus der Verknüpfung zu entfernen (Failover oder aggregiert) und klicken Sie auf **Next**.
- Für eine verknüpfte Schnittstelle wird die verknüpfte Schnittstelle mit den verbleibenden Slaves erstellt, wenn die Hardware für eine Slaveschnittstelle ausfällt. Wenn keine Slaves vorhanden sind, wird die verknüpfte Schnittstellen-ID ohne Slaves erstellt. Dieser Slavehardwareausfall generiert gemanagte Warnmeldungen, jeweils eine pro fehlgeschlagenem Slave.

  Hinweis

  Die Warnmeldung für einen fehlgeschlagenen Slave wird nicht mehr angezeigt, nachdem der fehlgeschlagene Slave aus dem System entfernt wurde. Wenn neue Hardware installiert ist, werden die Warnmeldungen nicht mehr angezeigt und die verknüpfte Schnittstelle verwendet die neue Slaveschnittstelle nach dem Neustart.

- Auf DD4200-, DD4500- und DD7200-Systemen unterstützt die ethMa-Schnittstelle weder Failover noch Linkzusammenfassungen.

Richtlinien für die Konfiguration einer virtuellen Schnittstelle für die Linkzusammenfassung

Die Linkzusammenfassung bietet verbesserte Netzwerkperformance und Ausfallsicherheit, indem eine oder mehrere Netzwerkschnittstellen parallel verwendet werden. Hierdurch wird die Geschwindigkeit und Zuverlässigkeit eines Links im Vergleich zu einer einzigen Schnittstelle gesteigert. Diese Richtlinien werden bereitgestellt, um Sie bei der Optimierung Ihrer Verwendung der Linkzusammenfassung zu unterstützen.

- Durch Änderungen an deaktivierten Ethernetschnittstellen wird die Routingtabelle gelöscht. Es wird empfohlen, Schnittstellenänderungen nur während geplanter Ausfallzeiten für Wartungsvorgänge vorzunehmen. Anschließend konfigurieren Sie die Routingregeln und Gateways neu.
- Aktivieren Sie die Zusammenfassung auf einer vorhandenen virtuellen Schnittstelle, indem Sie die physischen Schnittstellen, den Modus und eine IP-Adresse angeben.
- Optische 10-Gbit-Ethernetkarten mit einem Port unterstützen keine Linkzusammenfassung.
- 1-GbE- und 10-GbE-Schnittstellen können nicht zusammengefasst werden.
- Kupferkabelschnittstellen und optische Schnittstellen können nicht zusammengefasst werden.
- Auf den Systemen DD4200, DD4500 und DD7200 unterstützt die Schnittstelle „ethMA“ keine Linkzusammenfassung.

Richtlinien für die Konfiguration einer virtuellen Schnittstelle für Failover

Link-Failover bietet mehr Netzwerkstabilität und bessere Netzwerkperformance durch Erkennen von Backupschnittstellen, die Netzwerkverkehr unterstützen können, wenn die primäre Schnittstelle nicht betriebsbereit ist. Diese Richtlinien werden bereitgestellt, um Sie bei der Optimierung Ihrer Verwendung von Link-Failover zu unterstützen.

- Eine primäre Schnittstelle muss Teil des Failover sein. Wenn versucht wird, eine primäre Schnittstelle aus einem Failover zu entfernen, wird eine Fehlermeldung angezeigt.
- Wenn eine primäre Schnittstelle in einer Failover-Konfiguration verwendet wird, muss diese explizit angegeben werden und zudem muss eine Verknüpfung zur virtuellen Schnittstelle vorhanden sein. Wenn die primäre Schnittstelle ausfällt und mehrere Schnittstellen verfügbar sind, wird die nächste Schnittstelle nach dem Zufallsprinzip ausgewählt.
- Alle Schnittstellen in einer virtuellen Schnittstelle müssen sich im selben physischen Netzwerk befinden. Alle Netzwerkswitche in einer virtuellen Schnittstelle müssen sich im selben physischen Netzwerk befinden.
- Die empfohlene Anzahl physischer Schnittstellen für Failover ist höher als Eins. Sie können eine primäre Schnittstelle und eine oder mehrere Failover-Schnittstellen konfigurieren, mit folgenden Ausnahmen:
  - 10-Gbit-CX4-Ethernetkarten sind auf eine primäre Schnittstelle und eine Failover-Schnittstelle auf derselben Karte beschränkt.

  - Optische 10-Gbit-Ethernetkarten mit einem Port können nicht verwendet werden.
- Auf den Systemen DD4200, DD4500 und DD7200 unterstützt die Schnittstelle „ethMA“ kein Link-Failover.

Erstellen von virtuellen Schnittstellen

Erstellen Sie eine virtuelle Schnittstelle, um Linkzusammenfassung oder Link-Failover zu unterstützen. Die virtuelle Schnittstelle dient als Container für die Links, die für das Failover aggregiert oder zugeordnet werden sollen.

Erstellen einer virtuellen Schnittstelle zur Link Aggregation

Erstellen Sie eine virtuelle Schnittstelle zur Linkzusammenfassung, die als Container zum Zuordnen der an der Zusammenfassung beteiligten Links verwendet wird.

Eine Schnittstelle zur Linkzusammenfassung muss einen Linkverknüpfungsmodus angeben und erfordert möglicherweise eine Hash-Auswahl. Beispielsweise können Sie die Linkzusammenfassung auf der virtuellen Schnittstelle *veth1* mit den physischen Schnittstellen *eth1* und *eth2* im LACP-Modus (Link Aggregation Control Protocol) und Hash XOR-L2L3 aktivieren.

Vorgehensweise

1. Wählen Sie **Hardware** > **Ethernet** > **Interfaces**.
2. Deaktivieren Sie in der Tabelle „Interfaces“ die physische Schnittstelle, auf der die virtuelle Schnittstelle hinzugefügt werden soll, indem Sie in der Spalte **Enabled** auf **No** klicken.
3. Wählen Sie im Menü **Create** die Option **Virtual Interface**.
4. Geben Sie im Dialogfeld „Create Virtual Interface“ den Namen einer virtuellen Schnittstelle im Feld **veth** ein.

   Geben Sie einen virtuellen Schnittstellennamen im Format *veth* ein, wobei *x* eine eindeutige ID ist (in der Regel aus einem oder zwei Zeichen). Ein typischer vollständiger virtueller Schnittstellenname mit VLAN und IP-Alias ist *veth56.3999:199*. Die maximale Länge des vollständigen Namens beträgt 15 Zeichen. Sonderzeichen sind nicht zulässig. Zahlen müssen zwischen 0 und 4094 (einschließlich) liegen.

5. Wählen Sie unter **Bonding Type** die Option **Aggregate** aus.

   Hinweis

   Die Registrierungseinstellungen können sich von der Bonding-Konfiguration unterscheiden. Wenn Sie Schnittstellen zur virtuellen Schnittstelle hinzufügen, werden die Informationen erst beim Starten der virtuellen Schnittstelle und Zuweisen einer IP-Adresse an das Bonding-Modul gesendet. Bis dahin unterscheiden sich Registrierung und Bonding-Treiberkonfiguration.

6. Wählen Sie in der Liste **Modus** einen Bonding-Modus.

   Geben Sie den Modus an, der mit den Anforderungen des Systems kompatibel ist, mit dem die Schnittstellen direkt verbunden sind.

   - Round-robin
     Überträgt Pakete der Reihe nach vom ersten bis zum letzten verfügbaren Link in der zusammengefassten Gruppe

- Balanced
  Daten werden über die Schnittstellen gesendet, die durch die ausgewählte Hash-Methode festgelegt wurden. Dies erfordert, dass die zugehörigen Schnittstellen auf dem Switch in einem Etherkanal (Trunk) gruppiert werden und ihnen ein Hash über den Lastenausgleichsparameter zugewiesen wird.
- LACP
  Link Aggregation Control Protocol ist ähnlich wie „Balanced“, weist jedoch ein Kontrollprotokoll auf, das mit dem anderen Ende kommuniziert und koordiniert, welche Links in der Verknüpfung für die Verwendung verfügbar sind. LACP bietet eine Art Heartbeat Failover und muss an beiden Enden der Verbindung konfiguriert werden.

7. Wenn Sie den Modus „Balanced“ oder „LACP“ ausgewählt haben, geben Sie einen Bonding-Hash-Typ in der Liste **Hash** an.

   Optionen: XOR-L2, XOR-L2L3 oder XOR-L3L4.

   XOR-L2 überträgt über eine verknüpfte Schnittstelle mit einem XOR-Hash von Ebene 2 (ein- und ausgehende MAC-Adressen).

   XOR-L2L3 überträgt über eine verknüpfte Schnittstelle mit einem XOR-Hash von Ebene 2 (ein- und ausgehenden MAC-Adressen) und Ebene 3 (ein- und ausgehende IP-Adressen).

   XOR-L3L4 überträgt über eine verknüpfte Schnittstelle mit einem XOR-Hash von Ebene 3 (ein- und ausgehende IP-Adressen) und Ebene 4 (ein- und ausgehende Ports).

8. Um eine Schnittstelle auszuwählen und zur Aggregatkonfiguration hinzuzufügen, aktivieren Sie das Kontrollkästchen, das der Schnittstelle entspricht und klicken Sie dann auf **Next**.

   Das Dialogfeld „Create virtual interface *veth_name*“ wird angezeigt.

9. Geben Sie eine IP-Adresse ein oder geben Sie `0` ein, um keine IP-Adresse anzugeben.
10. Geben Sie eine Netzmasken-Adresse oder ein Präfix ein.
11. Geben Sie Geschwindigkeits-/Duplexoptionen an.

    Die Kombination aus Geschwindigkeits- und Duplexeinstellungen definiert die Datenübertragungsrate für die Schnittstelle. Wählen Sie entweder:

    - **Autonegotiate Speed/Duplex**
      Wählen Sie diese Option, um einer NIC das automatische Verhandeln der Übertragungsgeschwindigkeit und Duplexeinstellung für eine Schnittstelle zu ermöglichen.
    - **Manually configure Speed/Duplex**
      Wählen Sie diese Option, um die Datenübertragungsrate für eine Schnittstelle manuell festzulegen.
      - Duplex-Optionen sind Halbduplex oder Vollduplex.
      - Die aufgeführten Geschwindigkeitsoptionen sind auf die Funktionen des Hardware-Geräts begrenzt. Die Optionen sind 10 Mbit, 100 Mbit, 1000 Mbit und 10 Gbit.
      - Halbduplex ist nur für die Geschwindigkeiten 10 Mbit, 100 Mbit verfügbar.
      - Leitungsgeschwindigkeiten von 1000 Mbit und 10 Gbit benötigen Vollduplex.

- Optische Schnittstellen benötigen die Autonegotiate-Option.
- Der 10-GbE-Kupfer-NIC-Standard beträgt 10 Gbit. Wenn eine Kupferschnittstelle auf die Leitungsgeschwindigkeit 1000 Mbit oder 10 Gbit gesetzt wird, muss für Duplex Vollduplex festgelegt werden.

12. Legen Sie die MTU-Einstellung fest.
    - Klicken Sie auf **Default**, um den Standardwert (1500) zu wählen.
    - Um eine andere Einstellung auszuwählen, geben Sie die Einstellung im Feld **MTU** ein. Sorgen Sie dafür, dass alle Ihre Netzwerkkomponenten die für diese Größe eingestellte Option unterstützen.
13. Wählen Sie bei Bedarf die Option „Dynamic DNS Registration“.

    Dynamic DNS (DDNS) ist ein Protokoll, das lokale IP-Adressen auf einem Domain Name System(DNS)-Server registriert. In dieser Version unterstützt DD System Manager DDNS im Windows-Modus. Um DDNS im UNIX-Modus zu verwenden, verwenden Sie den Befehl `net ddns`.

    Das DDNS muss registriert werden, damit diese Option aktiviert wird.
14. Klicken Sie auf **Next**.

    Die Übersichtsseite „Configure Interface Settings“ wird angezeigt. Die aufgelisteten Werte spiegeln den neuen System- und Schnittstellenstatus wider.
15. Klicken Sie auf **Finish** und **OK.**

Erstellen einer virtuellen Schnittstelle zum Link-Failover

Erstellen Sie eine virtuelle Schnittstelle zum Link-Failover, die als Container zum Zuordnen der am Failover beteiligten Links verwendet wird.

Die Failover-aktivierte virtuelle Schnittstelle stellt eine Gruppe sekundärer Schnittstellen dar, von denen eine als primäre Schnittstelle angegeben werden kann. Das System verwendet die primäre Schnittstelle als aktive Schnittstelle, wann immer die primäre Schnittstelle betriebsbereit ist. Mit der konfigurierbaren Failover-Option „Down Delay“ können Sie eine Failover-Verzögerung in Intervallen von 900 Millisekunden konfigurieren. Die Failover-Verzögerung schützt vor mehreren Failovers, wenn ein Netzwerk instabil ist.

Vorgehensweise

1. Wählen Sie **Hardware** > **Ethernet** > **Interfaces**.
2. Deaktivieren Sie in der Tabelle "Interfaces" die physische Schnittstelle, der die virtuelle Schnittstelle hinzugefügt werden soll, indem Sie in der Spalte **Enabled** auf **No** klicken.
3. Wählen Sie im Menü **Create** die Option **Virtual Interface**.
4. Geben Sie im Dialogfeld „Create Virtual Interface“ den Namen einer virtuellen Schnittstelle im Feld **veth** ein.

   Geben Sie einen virtuellen Schnittstellennamen im Format `veth`*x* ein, wobei *x* eine eindeutige ID ist (in der Regel aus einem oder zwei Zeichen). Ein typischer vollständiger virtueller Schnittstellenname mit VLAN und IP-Alias ist *veth56.3999:199*. Die maximale Länge des vollständigen Namens beträgt 15 Zeichen. Sonderzeichen sind nicht zulässig. Zahlen müssen zwischen 0 und 4094 (einschließlich) liegen.

5. Wählen Sie unter **Bonding Type** die Option **Failover** aus.
6. Wählen Sie eine Schnittstelle zum Hinzufügen zur Failover-Konfiguration und klicken Sie auf **Next**. Virtuelle Gesamtschnittstellen können für Failover verwendet werden.

   Das Dialogfeld „Create virtual interface *veth_name*“ wird angezeigt.

7. Geben Sie eine IP-Adresse ein oder geben Sie `0` ein, um keine IP-Adresse anzugeben.
8. Geben Sie eine Netzmaske oder ein Präfix ein.
9. Geben Sie die Geschwindigkeits-/Duplexoptionen an.

   Die Kombination aus Geschwindigkeits- und Duplexeinstellungen definiert die Datenübertragungsrate für die Schnittstelle.

   - Wählen Sie **Autonegotiate Speed/Duplex**, um der Netzwerkschnittstellenkarte das automatische Verhandeln der Leitungsgeschwindigkeit und Duplexeinstellung für eine Schnittstelle zu ermöglichen.
   - Wählen Sie **Manually configure Speed/Duplex,** um die Datenübertragungsrate für eine Schnittstelle manuell festzulegen.
     - Duplexoptionen sind Halbduplex oder Vollduplex.
     - Die aufgeführten Geschwindigkeitsoptionen sind auf die Funktionen des Hardware-Geräts begrenzt. Die Optionen sind 10 Mbit, 100 Mbit, 1000 Mbit und 10 Gbit.
     - Halbduplex ist nur für die Geschwindigkeiten 10 Mbit und 100 Mbit verfügbar.
     - Leitungsgeschwindigkeiten von 1000 Mbit und 10 Gbit benötigen Vollduplex.
     - Optische Schnittstellen benötigen die Autonegotiate-Option.
     - Der Standardwert der Kupferschnittstelle beträgt 10 Gbit. Wenn eine Kupferschnittstelle auf eine Leitungsgeschwindigkeit von 1000 oder 10 Gbit eingestellt wird, muss das Duplex Vollduplex sein.

10. Geben Sie die MTU-Einstellung an.
    - Klicken Sie auf **Default**, um den Standardwert (1500) zu wählen.
    - Um eine andere Einstellung auszuwählen, geben Sie die Einstellung im Feld "MTU" ein. Sorgen Sie dafür, dass alle Ihre Netzwerkpfadkomponenten die für diese Größe eingestellte Option unterstützen.

11. Wählen Sie bei Bedarf die Option „Dynamic DNS Registration“.

    Dynamic DNS (DDNS) ist ein Protokoll, das lokale IP-Adressen auf einem Domain Name System(DNS)-Server registriert. In dieser Version unterstützt DD System Manager DDNS im Windows-Modus. Um DDNS im UNIX-Modus zu verwenden, verwenden Sie den Befehl `net ddns`.

    Das DDNS muss registriert werden, damit diese Option aktiviert wird.

    Hinweis

    Diese Option deaktiviert DHCP für diese Schnittstelle.

12. Klicken Sie auf **Next**.

    Die Übersichtsseite "Configure Interface Settings" wird angezeigt. Die aufgelisteten Werte spiegeln den neuen System- und Schnittstellenstatus wider.

13. Schließen Sie die Schnittstelle ab, klicken Sie auf **Finish** und dann auf **OK**.

Ändern einer virtuellen Schnittstelle

Nach dem Erstellen einer virtuellen Schnittstelle können Sie die Einstellungen aktualisieren, um auf Netzwerkänderungen zu reagieren oder um Probleme zu beheben.

Vorgehensweise

1. Wählen Sie **Hardware** > **Ethernet** > **Interfaces**.
2. Wählen Sie in der Spalte „Interfaces“ die Schnittstelle aus und deaktivieren Sie die virtuelle Schnittstelle, indem Sie auf **No** in der Spalte **Enabled** klicken. Klicken Sie im Warndialogfeld auf **OK**.
3. Wählen Sie in der Spalte **Interfaces** die Schnittstelle aus und klicken Sie auf **Configure**.
4. Ändern Sie die Einstellungen in Dialogfeld **Configure Virtual Interface**.
5. Klicken Sie auf **Next** und **Finish**.

Konfigurieren eines VLAN

Erstellen Sie eine neue VLAN-Schnittstelle entweder von einer physischen oder einer virtuellen Schnittstelle.

Die empfohlene Gesamtanzahl von VLAN-Schnittstellen ist 80. Sie können bis zu 100 Schnittstellen erstellen (minus der Anzahl an Pseudonymen, physischen und virtuellen Schnittstellen), bevor das System verhindert, dass Sie weitere erstellen.

Vorgehensweise

1. Wählen Sie **Hardware** > **Ethernet** > **Interfaces**.
2. Wählen Sie in der Tabelle die Schnittstelle aus, der Sie das VLAN hinzufügen möchten.

   Die ausgewählte Schnittstelle muss mit einer IP-Adresse konfiguriert werden, bevor Sie ein VLAN hinzufügen können.

3. Klicken Sie auf **Create** und wählen Sie **VLAN**.
4. Geben Sie im Dialogfeld „Create VLAN“ eine VLAN-ID an, indem Sie eine Nummer in das Feld **VLAN Id** eingeben.

   Der Bereich für die VLAN-ID liegt zwischen 1 und 4094 einschließlich.

5. Geben Sie eine IP-Adresse ein oder geben Sie `0` ein, um keine IP-Adresse anzugeben.

   Die Internet Protocol(IP)-Adresse ist die Nummer, die der Schnittstelle zugewiesen ist. Beispiel: 192.168.10.23.

6. Geben Sie eine Netzmaske oder ein Präfix ein.
7. Legen Sie die MTU-Einstellung fest.

   Die VLAN-MTU muss kleiner oder gleich der für die physische oder virtuelle Schnittstelle definierten MTU sein, der sie zugewiesen ist. Wenn die MTU, die

für die Unterstützung von physischen oder virtuellen Schnittstelle definiert ist, unter den konfigurierten VLAN-Wert reduziert wird, wird der VLAN-Wert automatisch reduziert, um der unterstützenden Schnittstelle zu entsprechen. Wenn der MTU-Wert für die unterstützende Schnittstelle über den konfigurierten VLAN-Wert erhöht wird, bleibt der VLAN-Wert unverändert.

- Klicken Sie auf **Default**, um den Standardwert (1500) auszuwählen.
- Um eine andere Einstellung auszuwählen, geben Sie die Einstellung im Feld „MTU“ ein. DD System Manager akzeptiert keine MTU-Größe, die höher als der definierte Wert für die physische oder die virtuelle Schnittstelle ist, der das VLAN zugewiesen ist.

8. Geben Sie die Option für die dynamische DNS-Registrierung an.

   Dynamic DNS (DDNS) ist ein Protokoll, das lokale IP-Adressen auf einem Domain Name System(DNS)-Server registriert. In dieser Version unterstützt DD System Manager DDNS im Windows-Modus. Um DDNS im UNIX-Modus zu verwenden, verwenden Sie den Befehl `net ddns`.

   Das DDNS muss registriert werden, damit diese Option aktiviert wird.

9. Klicken Sie auf **Next**.

   Die Übersichtsseite **Create VLAN** wird angezeigt.

10. Überprüfen Sie die Konfigurationseinstellungen und klicken Sie auf **Finish** und auf **OK.**

Ändern einer VLAN-Schnittstelle

Nach dem Erstellen einer VLAN-Schnittstelle können Sie die Einstellungen aktualisieren, um auf Netzwerkänderungen zu reagieren oder um Probleme zu beheben.

Vorgehensweise

1. Wählen Sie**Hardware** > **Ethernet** > **Interfaces**.
2. Aktivieren Sie in der Spalte **Interfaces** das Kontrollkästchen für die Schnittstelle und deaktivieren Sie die VLAN-Schnittstelle, indem Sie in der Spalte **Enabled** auf **No** klicken. Klicken Sie im Warndialogfeld auf **OK**.
3. Aktivieren Sie in der Spalte „Interfaces“ das Kontrollkästchen für die Schnittstelle und klicken Sie dann auf **Configure**.
4. Ändern Sie im Dialogfeld **Configure VLAN Interface** die Einstellungen.
5. Klicken Sie auf **Next** und **Finish**.

Konfigurieren eines IP-Alias

Ein IP-Alias weist einer physischen Schnittstelle, einer virtuellen Schnittstelle oder einem VLAN eine zusätzliche IP-Adresse zu.

Die empfohlene Gesamtzahl von IP-Aliasen für VLAN sowie physische und virtuelle Schnittstellen, die auf dem System vorhanden sein können, liegt bei 80. Obwohl bis zu 100 Schnittstellen unterstützt werden, verlangsamt sich möglicherweise die Anzeige, wenn die maximale Anzahl erreicht wird.

Hinweis

Bei Verwendung eines Data Domain-HA-Systems gilt Folgendes: Wenn ein Benutzer erstellt wird und sich beim Stand-by-Node anmeldet, ohne sich zunächst beim aktiven Node anzumelden, hat der Benutzer keinen Standard-Alias. Um Aliase auf dem Stand-by-Node verwenden zu können, sollte sich der Benutzer daher zuerst beim aktiven Node anmelden.

Vorgehensweise

1. Wählen Sie **Hardware** > **Ethernet** > **Interfaces**.
2. Klicken Sie auf **Create** und wählen Sie **IP Alias**.

   Das Dialogfeld „Create IP Alias“ wird angezeigt.
3. Geben Sie eine IP-Alias-ID an, indem Sie eine Zahl in das Feld **IP ALIAS Id** eingeben.

   Der Wertebereich liegt zwischen 1 und 4094 einschließlich.
4. Geben Sie eine IPv4- oder IPv6-Adresse ein.
5. Wenn Sie eine IPv4-Adresse eingegeben haben, geben Sie eine Netzmaskenadresse ein.
6. Geben Sie die Option für die dynamische DNS-Registrierung an.

   Dynamic DNS (DDNS) ist ein Protokoll, das lokale IP-Adressen auf einem Domain Name System(DNS)-Server registriert. In dieser Version unterstützt DD System Manager DDNS im Windows-Modus. Um DDNS im UNIX-Modus zu verwenden, verwenden Sie den Befehl `net ddns`.

   Das DDNS muss registriert werden, damit diese Option aktiviert wird.
7. Klicken Sie auf **Next**.

   Die Seite „Create IP Alias summary“ wird angezeigt.
8. Überprüfen Sie die Konfigurationseinstellungen und klicken Sie auf **Finish** und **OK**.

Ändern einer IP-Aliasschnittstelle

Nach dem Erstellen eines IP-Alias können Sie die Einstellungen aktualisieren, um auf Netzwerkänderungen zu reagieren oder um Probleme zu beheben.

Vorgehensweise

1. Wählen Sie **Hardware** > **Ethernet** > **Interfaces**.
2. Aktivieren Sie in der Spalte **Interfaces** das Kontrollkästchen für die Schnittstelle und deaktivieren Sie die IP-Aliasschnittstelle, indem Sie in der Spalte **Enabled** auf **No** klicken. Klicken Sie im Warndialogfeld auf **OK**.
3. Aktivieren Sie in der Spalte **Interfaces** das Kontrollkästchen für die Schnittstelle und klicken Sie dann auf **Configure**.
4. Ändern Sie im Dialogfeld „Configure IP Alias“ die Einstellungen, wie im Verfahren für das Erstellen eines IP-Alias beschrieben.
5. Klicken Sie auf **Next** und **Finish**.

Registrieren von Schnittstellen mit DDNS

Dynamic DNS (DDNS) ist ein Protokoll, das lokale IP-Adressen auf einem Domain Name System(DNS)-Server registriert.

In dieser Version unterstützt DD System Manager DDNS im Windows-Modus. Um DDNS im UNIX-Modus zu verwenden, verwenden Sie den Befehl `net ddns`. Sie können Folgendes tun:

- Registrieren Sie manuell konfigurierte Schnittstellen bei der DDNS-Registrierungsliste (fügen Sie sie hinzu).
- Entfernen Sie die Schnittstellen aus der DDNS-Registrierungsliste.
- Aktivieren oder deaktivieren Sie DNS-Aktualisierungen.
- Zeigen Sie an, ob die DDNS-Registrierung aktiviert ist.
- Zeigen Sie Schnittstellen in der DDNS-Registrierungsliste an.

Vorgehensweise

1. Wählen Sie **Hardware** > **Ethernet** > **Interfaces** > **DDNS Registration**.
2. Um eine Schnittstelle zu DDNS hinzuzufügen, klicken Sie im Dialogfeld „DDNS Windows Mode Registration“ auf **Add**.

   Das Dialogfeld „Add Interface“ wird angezeigt.

   a. Geben Sie einen Namen in das Feld **Interface** ein.

   b. Klicken Sie auf **OK**.
3. So können Sie optional eine Schnittstelle aus dem DDNS entfernen:

   a. Wählen Sie die zu entfernende Schnittstelle aus und klicken Sie auf **Remove**.

   b. Klicken Sie im Dialogfeld „Confirm Remove“ auf **OK**.
4. Geben Sie den DDNS-Status an.

   - Wählen Sie **Enable** aus, um Aktualisierungen für alle bereits registrierten Schnittstellen zu aktivieren.
   - Klicken Sie auf **Default**, um die Standardeinstellungen für DDNS-Aktualisierungen auszuwählen.
   - Deaktivieren Sie die Option **Enable**, um DDNS-Aktualisierungen für die registrierten Schnittstellen zu deaktivieren.
5. Klicken Sie auf **OK**, um die DDNS-Konfiguration abzuschließen.

Löschen einer Schnittstelle

Sie können DD System Manager verwenden, um virtuelle, VLAN- und IP-Aliasschnittstellen zu entfernen oder zu löschen.

Wenn eine virtuelle Schnittstelle gelöscht wird, löscht das System die virtuelle Schnittstelle, gibt ihre gebundene physische Schnittstelle frei und löscht alle VLANs oder Aliase, die an die virtuelle Schnittstelle angebunden sind. Wenn Sie eine VLAN-Schnittstelle löschen, löscht das Betriebssystem die VLAN-Schnittstelle und alle IP-Aliasschnittstellen, die darunter erstellt wurden. Wenn Sie ein IP-Alias löschen, löscht das Betriebssystem nur diese Aliasschnittstelle.

Vorgehensweise

1. Wählen Sie **Hardware** > **Ethernet** > **Interfaces**.

2. Aktivieren Sie das Kontrollkästchen neben jeder Schnittstelle, die gelöscht werden soll (virtuell oder VLAN oder IP-Alias).
3. Klicken Sie auf **Destroy**.
4. Klicken Sie zur Bestätigung auf **OK**.

Anzeigen einer Schnittstellenhierarchie in der Strukturansicht

Im Dialogfeld „Tree View“ wird die Zuordnung zwischen physischen und virtuellen Schnittstellen angezeigt.

Vorgehensweise

1. Wählen Sie **Hardware** > **Ethernet** > **Interfaces** > **Tree View**.
2. Klicken Sie im Dialogfeld „Tree View“ auf die Plus- oder Minusfelder, um die Strukturansicht, die die Hierarchie anzeigt, zu erweitern oder verkleinern.
3. Klicken Sie auf **Close**, um diese Ansicht zu verlassen.

Management von allgemeinen Netzwerkeinstellungen

Die Konfigurationseinstellungen für Hostname, Domainname, Suchdomains, Hostzuordnung und DNS-Liste werden auf der Registerkarte „Settings“ gemanagt.

Anzeigen von Netzwerkeinstellungsinformationen

Auf der Registerkarte „Settings“ wird die aktuelle Konfiguration für Hostname, Domainname, Suchdomains, Hostzuordnung und DNS angezeigt.

Vorgehensweise

1. Wählen Sie **Hardware** > **Ethernet** > **Settings**.

Ergebnisse

Auf der Registerkarte „Settings“ werden die folgenden Informationen angezeigt:

Host Settings

Hostname

Der Hostname des ausgewählten Systems

Domain-Name

Der vollständig qualifizierte Domainname, der dem ausgewählten System zugeordnet ist

Search Domain List

Search Domain

Eine Liste der Suchdomains, die vom ausgewählten System verwendet werden. Das System wendet die Suchdomain als Suffix für den Hostnamen an.

Hosts Mapping

IP-Adresse

Die IP-Adresse des Hosts, die aufgelöst werden muss.

Hostname

Mit der IP-Adresse verknüpfte IP-Adressen

DNS List

DNS IP Address

Aktuelle DNS-IP-Adressen, die dem ausgewählten System zugeordnet sind. Ein Sternchen (*) gibt an, dass die IP-Adressen über DHCP zugewiesen wurden.

Festlegen des DD System Manager-Hostnamens

Sie können den DD System Manager-Hostnamen und -Domainnamen manuell konfigurieren oder DD OS so konfigurieren, dass es den Host- und Domainnamen von einem DHCP-Server (Dynamic Host Configuration Protocol) automatisch erhält.

Ein Vorteil dafür, den Host- und Domainnamen manuell zu konfigurieren, liegt darin, dass Sie die Abhängigkeit von dem DHCP-Server und der Schnittstelle eliminieren, die zu dem DHCP-Server führt. Um das Risiko einer Betriebsunterbrechung zu minimieren, empfiehlt es sich, dass Sie den Host- und Domainnamen manuell konfigurieren.

Wenn Sie den Hostnamen und den Domainnamen konfigurieren, sollten Sie die folgenden Richtlinien beachten.

- Schließen Sie keinen Unterstrich in den Hostnamen ein; er ist u. U. mit einigen Browsern nicht kompatibel.
- Replikation und CIFS-Authentifizierung müssen neu konfiguriert werden, nachdem Sie die Namen geändert haben.
- Wenn ein System zuvor ohne einen vollständig qualifizierten Namen (kein Domainname) hinzugefügt wurde, macht eine Domainnamenänderung erforderlich, dass Sie das betroffene System entfernen und hinzufügen oder die Liste „Search Domain“ aktualisieren, damit der neue Domainname eingeschlossen ist.

Vorgehensweise

1. Wählen Sie **Hardware** > **Ethernet** > **Settings**.
2. Klicken Sie im Bereich **Host Settings** auf **Edit**. Das Dialogfeld „Configure Host“ wird angezeigt.
3. So konfigurieren Sie den Host- und Domainnamen manuell:
   a. Wählen Sie **Manually configure host** aus.
   b. Geben Sie einen Hostnamen in das Feld **Host Name** ein.

      Beispiel: `id##.yourcompany.com`

   c. Geben Sie einen Domainnamen im Feld **Domain Name** ein.

      Dies ist der Domainname, den Sie mit dem Domainnamen des Data Domain-Systems und in der Regel mit dem Domainnamen Ihres Unternehmens verknüpfen. z. B. */hrUnternehmen.de*

   d. Klicken Sie auf **OK**.

      Das System zeigt Fortschrittsmeldungen an, während die Änderungen angewendet werden.
4. Um die Host- und Domainnamen von einem DHCP-Server abzurufen, wählen Sie **Obtain Settings using DHCP** und klicken Sie auf **OK**.

   Mindestens eine Schnittstelle muss zur Verwendung von DHCP konfiguriert sein.

Managen einer Domainsuchliste

Verwenden Sie die Domainsuchliste zum Definieren, welche Domains das System suchen kann.

Vorgehensweise

1. Wählen Sie **Hardware** > **Ethernet** > **Settings**.
2. Klicken Sie auf **Edit** im Bereich „Search Domain List“.
3. So fügen Sie eine Suchdomain mithilfe des Dialogfelds „Configure Search Domains“ hinzu:
   a. Klicken Sie auf „Add“ (**+**).
   b. Geben Sie im Dialogfeld „Add Search Domain“ einen Namen in das Feld **Search Domain** ein.

      Beispiel: `id##.yourcompany.com`

   c. Klicken Sie auf **OK**.

      Das System fügt die neue Domain zur Liste der durchsuchbaren Domains hinzu.

   d. Klicken Sie auf **OK**, um die Änderungen zu übernehmen und zur Ansicht „Settings“ zurückzukehren.
4. So entfernen Sie eine Suchdomain mithilfe des Dialogfelds „Configure Search Domains“:
   a. Wählen Sie die Suchdomain aus, der gelöscht werden soll.
   b. Klicken Sie auf „Delete“ (**X**).

      Das System entfernt die neue Domain aus der Liste der durchsuchbaren Domains.

   c. Klicken Sie auf **OK**, um die Änderungen zu übernehmen und zur Ansicht „Settings“ zurückzukehren.

Hinzufügen und Löschen von Hostzuordnungen

Eine Hostzuordnung verknüpft eine IP-Adresse mit einem Hostnamen, sodass entweder die IP-Adresse oder der Hostname zum Angeben des Hosts verwendet werden kann.

Vorgehensweise

1. Wählen Sie **Hardware** > **Ethernet** > **Settings**.
2. Um eine Hostzuordnung hinzuzufügen, führen Sie die folgenden Schritte aus:
   a. Klicken Sie im Bereich „Host Mapping“ auf **Add**.
   b. Geben Sie im Dialogfeld „Add Hosts“ die IP-Adresse des Hosts im Feld **IP Address** ein.
   c. Klicken Sie auf „Add“ (**+**).
   d. Geben Sie im Dialogfeld „Add Host“ im Feld `Host Name` einen Hostnamen ein, wie **id##.yourcompany.com**.
   e. Klicken Sie auf **OK**, um den neuen Hostnamen zur Liste „Host Name“ hinzuzufügen.

f. Klicken Sie auf **OK**, um zur Registerkarte „Settings“ zurückzukehren.

3. Um eine Hostzuordnung zu löschen, führen Sie die folgenden Schritte aus:
   a. Wählen Sie im Bereich „Host Mapping“ die Hostzuordnung aus, die gelöscht werden soll.
   b. Klicken Sie auf „Delete“ (**X**).

Konfigurieren von DNS-IP-Adressen

DNS-IP-Adressen geben die DNS-Server an, die das System verwenden kann, um IP-Adressen für Hostnamen abzurufen, die sich nicht in der Tabelle mit Hostzuordnungen befinden.

Sie können die DNS-IP-Adressen manuell konfigurieren oder DD OS konfigurieren, um IP-Adressen automatisch von einem DHCP-Server zu erhalten. Ein Vorteil der manuellen Konfiguration von DNS-Adressen besteht darin, dass Sie die Abhängigkeit von dem DHCP-Server und der Schnittstelle entfernen, die zu dem DHCP-Server führt. Um das Risiko einer Betriebsunterbrechung zu minimieren, empfiehlt EMC, dass Sie die DNS-IP-Adressen manuell konfigurieren.

Vorgehensweise

1. Wählen Sie **Hardware** > **Ethernet** > **Settings**.
2. Klicken Sie auf **Edit** im Bereich „DNS List“.
3. So fügen Sie manuell eine DNS-IP-Adresse hinzu:
   a. Wählen Sie **Manually configure DNS list** aus.

      Die Kontrollkästchen für DNS-IP-Adressen werden aktiviert.

   b. Klicken Sie auf „Add“ (**+**).
   c. Geben Sie im Dialogfeld „Add DNS“ die hinzuzufügende DNS-IP-Adresse ein.
   d. Klicken Sie auf **OK**.

      Das System fügt die neue IP-Adresse der Liste der DNS-IP-Adressen hinzu.

   e. Klicken Sie auf **OK**, um die Änderungen zu übernehmen.
4. So löschen Sie eine DNS-IP-Adresse aus der Liste:
   a. Wählen Sie **Manually configure DNS list** aus.

      Die Kontrollkästchen für DNS-IP-Adressen werden aktiviert.

   b. Wählen Sie die zu löschende DNS-IP-Adresse aus und klicken Sie auf „Delete“ (**X**).

      Das System entfernt die IP-Adresse aus der Liste der DNS-IP-Adressen.

   c. Klicken Sie auf **OK**, um die Änderungen zu übernehmen.
5. Um DNS-Adressen von einem DHCP-Server abzurufen, wählen Sie **Obtain DNS using DHCP** und klicken Sie auf **OK**.

   Mindestens eine Schnittstelle muss zur Verwendung von DHCP konfiguriert sein.

Management von Netzwerkrouten

Routen bestimmen den Pfad für die Datenübertragung vom lokalen Host (dem Data Domain-System) zu einem anderen Netzwerk oder Host und umgekehrt.

Data Domain-Systeme erzeugen keine Protokolle zur Verwaltung des Netzwerkroutings (RIP, EGRP/EIGRP und BGP) und antworten nicht auf diese. Das einzige auf einem Data Domain-System implementierte Routing ist Policy-basiertes IPv4-Routing, wodurch nur eine Route zu einem Standardgateway pro Routingtabelle ermöglicht wird. Es können mehrere Routingtabellen und mehrere Standardgateways vorhanden sein. Eine Routingtabelle wird für jede Adresse erstellt, die dasselbe Subnetz wie ein Standardgateway hat. Die Routingregeln senden die Pakete mit der Quell-IP-Adresse, die der zum Erstellen der Tabelle zu dieser Routingtabelle verwendete IP-Adresse entspricht. Alle Pakete, die nicht über Quell-IP-Adressen verfügen, die einer Routingtabelle entsprechen, werden an die Routinghaupttabelle gesendet.

Innerhalb jeder Routingtabelle können statische Routen hinzugefügt werden; aber da Quellrouting zum Senden der Pakete an die Tabelle verwendet wird, funktionieren nur statische Routen, die die Schnittstelle der Quelladresse jeder Tabelle verwenden. Andernfalls müssen sie in die Haupttabelle eingefügt werden.

Data Domain-Systeme verwenden – anders als das an diesen anderen Routingtabellen durchgeführte IPv4-Quellrouting – quellbasiertes Routing für die IPv4- und IPv6-Hauptroutingtabellen, d. h., ausgehende Netzwerkpakete, die dem Subnetz verschiedener Schnittstellen entsprechen, werden nur über die physische Schnittstelle geroutet, von der sie stammen und deren IP-Adresse mit der Quell-IP-Adresse der Pakete übereinstimmt.

Für IPv6 enthalten mehrere festgelegte Schnittstellen für statische Routen dieselben IPv6-Subnetze und Verbindungen zu IPv6-Adressen werden mit diesem Subnetz hergestellt. Normalerweise werden statische Routen für IPv4-Adressen mit demselben Subnetz, z. B. für Backups, nicht benötigt. In einigen Fällen können statische IP-Adressen erforderlich sein, damit Verbindungen funktionieren, z. B. bei Verbindungen vom Data Domain-System zu Remotesystemen.

Durch das Hinzufügen oder Löschen einer Tabelle in bzw. aus den Routenspezifikationen werden statische Routen einzelnen Routingtabellen hinzugefügt oder aus ihnen gelöscht. Dadurch werden die Regeln für direkte Pakete mit bestimmten Quelladressen über bestimmte Routingtabellen weitergeleitet. Wenn eine statische Route für Pakete mit diesen Quelladressen erforderlich ist, müssen den Routen die spezifischen Tabellen hinzugefügt werden, an die die IP-Adresse weitergeleitet wird.

Hinweis

Routing für Verbindungen, die vom Data Domain-System initiiert werden, z. B. für die Replikation, hängt von der Quelladresse ab, die für Schnittstellen im selben Subnetz verwendet wird. Um Datenverkehr für eine bestimmte Schnittstelle zu einem bestimmten Ziel zu erzwingen (selbst wenn diese Schnittstelle sich im selben Subnetz wie andere Schnittstellen befindet), konfigurieren Sie einen statischen Routingeintrag zwischen den beiden Systemen. Dieses statische Routing setzt dass Quellrouting außer Kraft. Dies ist nicht erforderlich, wenn die Quelladresse IPv4 und ein Standardgateway zugeordnet ist. In diesem Fall wird das Quellrouting bereits über eine eigene Routingtabelle verarbeitet.

Anzeigen von Routeninformationen

Auf der Registerkarte „Routes“ werden Standardgateways sowie statische und dynamische Routen angezeigt.

Vorgehensweise

1. Wählen Sie **Hardware** > **Ethernet** > **Routes**.

Ergebnisse

Im Bereich „Static Routes“ sind die Routenspezifikationen aufgeführt, die zum Konfigurieren jeder statischen Route verwendet werden. In der Tabelle „Dynamic Routes“ sind die Informationen zu den einzelnen dynamisch zugewiesenen Routen aufgeführt.

Tabelle 32 Beschreibung der Spaltenbeschriftungen für dynamische Routen

Element	Beschreibung
Ziel	Zielhost/-netzwerk, an den/das der Netzwerkdatenverkehr (Daten) gesendet wird
Gateway	IP-Adresse des Routers im DD-Netzwerk oder 0.0.0.0, wenn kein Gateway festgelegt ist
Genmask	Netzmaske für das Zielnetzwerk. Legen Sie 255.255.255.255 für ein Hostziel und 0.0.0.0 für die Standardroute fest.
Flags	Mögliche Flags sind: U (Route ist aktiv), H (Ziel ist ein Host), G (Gateway verwenden), R (Route für dynamisches Routing erneut einsetzen), D (dynamische Installation durch Daemon oder Umleitung), M (geändert durch Routing-Daemon oder Umleitung), A (installiert von addrconf), C (Cacheeintrag) und ! (Route ablehnen)
Kennzahl	Die Entfernung zum Ziel (in der Regel gezählt in Hops). Nicht vom DD OS verwendet, wird aber möglicherweise von Routing-Daemons benötigt.
MTU	Größe der MTU (Maximum Transmission Unit) für die physische Schnittstelle (Ethernet).
Fenster	Standardfenstergröße für TCP-Verbindungen über diese Route
IRTT	Anfangs-RTT (Round Trip Time), die vom Kernel verwendet wird, um die besten TCP-Protokollparameter zu schätzen, ohne auf möglicherweise langsame Antworten zu warten
Schnittstelle	Mit der Routingschnittstelle verbundener Schnittstellenname

Festlegen des Standardgateway

Sie können das Standardgateway manuell konfigurieren oder DD OS so konfigurieren, dass Sie die standardmäßigen Gateway IP-Adressen von einem DHCP-Server automatisch erhalten.

Ein Vorteil dafür, das Standardgateway manuell zu konfigurieren, liegt darin, dass Sie die Abhängigkeit von dem DHCP-Server und der Schnittstelle eliminieren, die zu dem DHCP-Server führt. Um das Risiko einer Betriebsunterbrechung zu minimieren, empfiehlt es sich, dass Sie die Standardgateway-IP-Adresse manuell konfigurieren.

Vorgehensweise

1. Wählen Sie **Hardware** > **Ethernet** > **Routes**.
2. Klicken Sie auf **Edit** neben dem Standardgatewaytyp (IPv4 oder IPv6), den Sie konfigurieren möchten.
3. So konfigurieren Sie die Standardgatewayadresse manuell:
   a. Wählen Sie **Manually Configure**.
   b. Geben Sie im Feld **Gateway** die Gatewayadresse ein.

c. Klicken Sie auf **OK**.

4. Um die Standardgatewayadresse von einem DHCP-Server zu erhalten, wählen Sie **Use DHCP value** aus und klicken Sie auf **OK**.

   Mindestens eine Schnittstelle muss zur Verwendung von DHCP konfiguriert sein.

Erstellen von statischen Routen

Statische Routen definieren Zielhosts oder -netzwerke, mit denen das System kommunizieren kann.

Vorgehensweise

1. Wählen Sie **Hardware** > **Ethernet** > **Routes**.
2. Klicken Sie auf **Create** im Bereich „Static Routes“.
3. Wählen Sie im Dialogfeld **Create Routes** die Schnittstelle aus, die die statische Route hosten soll und klicken Sie auf **Next**.
4. Geben Sie das Ziel an.
   - Um ein Zielnetzwerk anzugeben, wählen Sie **Network** aus und geben Sie die Netzwerkadresse und die Netzmaske für das Zielnetzwerk ein.
   - Um einen Zielhost anzugeben, wählen Sie **Host** aus und geben Sie den Hostnamen oder die IP-Adresse des Zielhosts ein.
5. Optional geben Sie das Gateway an, das verwendet werden soll, um eine Verbindung zum Zielnetzwerk oder zum Host herzustellen.
   a. Wählen Sie **Specify a gateway for this route** aus.
   b. Geben Sie im Feld **Gateway** die Gatewayadresse ein.
6. Überprüfen Sie die Konfiguration und klicken Sie auf **Next**.

   Die Seite „Create Routes Summary“ wird angezeigt.
7. Klicken Sie auf **Finish**.
8. Wenn der Vorgang abgeschlossen ist, klicken Sie auf **OK**.

   Die neue Routenspezifikation wird in der Liste „Route Spec“ aufgelistet.

Löschen von statischen Routen

Löschen Sie eine statische Route, wenn Sie nicht mehr möchten, dass das System mit einem Zielhost oder einem Zielnetzwerk kommuniziert.

Vorgehensweise

1. Wählen Sie**Hardware** > **Ethernet** > **Routes**.
2. Wählen Sie die Option „Route Spec“ für die Routenspezifikation aus, die Sie löschen möchten.
3. Klicken Sie auf **Delete**.
4. Klicken Sie auf **Delete**, um den Vorgang zu bestätigen, und anschließend auf **Close**.

   Die ausgewählte Routenspezifikation wird aus der Liste „Route Spec“ entfernt.

System-Passphrasen-Management

Die System-Passphrase ist ein Schlüssel, mit dessen Hilfe ein Data Domain-System mit Chiffrierschlüsseln im System transportiert werden kann. Die Chiffrierschlüssel schützen die Daten und die System-Passphrase schützt die Chiffrierschlüssel.

Die System-Passphrase ist ein visuell lesbarer (verständlicher) Schlüssel (z. B. eine Smartcard) der verwendet wird, um einen von einem Rechner vewendbaren AES256-Chiffrierschlüssel zu erzeugen. Wenn das System während der Übertragung gestohlen wird, kann ein Angreifer die Daten nicht einfach wiederherstellen: Er kann höchstens die verschlüsselten Benutzerdaten und die verschlüsselten Schlüssel wiederherstellen.

Die Passphrase wird intern auf einem versteckten Teil des Data Domain-Speichersubsystem gespeichert. Auf diese Weise kann das Data Domain-System ohne Eingriff durch den Administrator gestartet werden und den Datenzugriff weiterhin bedienen.

Festlegen der System-Passphrase

Die System-Passphrase muss zuerst festgelegt werden, erst dann kann das System die Datenverschlüsselung unterstützen oder digitale Zertifikate anfordern.

Bevor Sie beginnen

Bei der Installation von DD OS wird für die System-Passphrase keine Mindestlänge festgelegt. Die Befehlszeilenoberfläche stellt jedoch einen Befehl zum Festlegen einer Mindestlänge bereit. Wenn Sie ermitteln möchten, ob für die Passphrase eine Mindestlänge konfiguriert wurde, geben Sie den CLI-Befehl `system passphrase option show` ein.

Vorgehensweise

1. Wählen Sie **Administration** > **Access** > **Administrator Access**.

   Wenn keine System-Passphrase festgelegt wurde, wird im Bereich Passphrase die Schaltfläche **Set Passphrase** angezeigt. Wenn eine System-Passphrase konfiguriert wurde, wird die Schaltfläche **Change Passphrase** angezeigt, und Sie haben nur die Möglichkeit, die Passphrase zu ändern.

2. Klicken Sie auf die Schaltfläche **Set Passphrase**.

   Das Dialogfeld „Set Passphrase“ wird angezeigt.

3. Geben Sie die System-Passphrase in die Felder ein und klicken Sie auf **Next.**

   Wenn für die System-Passphrase eine Mindestlänge konfiguriert wurde, muss die eingegebene Passphrase mindestens die angegebene Anzahl Zeichen enthalten.

Ergebnisse

Die System-Passphrase wird festgelegt und die Schaltfläche **Change Passphrase** wird anstelle der Schaltfläche **Set Passphrase** angezeigt.

Ändern der System-Passphrase

Der Administrator kann die Passphrase ändern, ohne die eigentlichen Chiffrierschlüssel bearbeiten zu müssen. Durch Ändern der Passphrase wird indirekt die Verschlüsselung

der Schlüssel geändert. Dies hat jedoch keine Auswirkungen auf die Benutzerdaten oder den zugrunde liegenden Chiffrierschlüssel.

Beim Ändern der Passphrase ist eine Authentifizierung durch zwei Benutzer erforderlich, um sich gegen die Möglichkeit zu schützen, dass Daten zerstört werden.

Vorgehensweise

1. Wählen Sie **Administration** > **Access** > **Administrator Access**.
2. Um die System-Passphrase zu ändern, klicken Sie auf **Change Passphrase**.

   Das Dialogfeld „Change Passphrase“ wird angezeigt.

   Hinweis

   Das Dateisystem muss deaktiviert werden, um die Passphrase zu ändern. Wenn das Dateisystem ausgeführt wird, werden Sie aufgefordert, es zu deaktivieren.

3. Geben Sie in den Textfeldern Folgendes an:
   - Den Benutzernamen und das Passwort eines Security Officer-Kontos (eines autorisierten Benutzers in der Sicherheitsbenutzergruppe auf diesem Data Domain-System)
   - Die aktuelle Passphrase, wenn die Passphrase geändert wird
   - Die neue Passphrase, die mindestens die Anzahl Zeichen enthalten muss, die mit dem Befehl `system passphrase option set min-length` konfiguriert wurde.
4. Klicken Sie auf das Kontrollkästchen für **Enable file system now**.
5. Klicken Sie auf **OK**.

   HINWEIS

   Notieren Sie sich die Passphrase. Wenn Sie die Passphrase verlieren, können Sie das Dateisystem nicht entsperren und auf die Daten zugreifen. Die Daten sind unwiderruflich verloren.

Systemzugriffsmanagement

Mithilfe der Funktionen für das Systemzugriffsmanagement können Sie den Systemzugriff auf Benutzer in einer lokalen Datenbank oder in einem Netzwerkverzeichnis steuern. Mit weiteren Steuerelementen können Sie unterschiedliche Zugriffsebenen definieren und festlegen, welche Protokolle auf das System zugreifen können.

Rollenbasierten Zugriffskontrolle

Die rollenbasierte Zugriffskontrolle ist eine Authentifizierungsrichtlinie, mit der gesteuert wird, welche Steuerelemente und CLI-Befehle von DD System Manager ein Benutzer auf einem System verwenden kann.

Beispielsweise können Benutzer mit der Rolle *admin* das gesamte System konfigurieren und überwachen, während Benutzer mit der Rolle *user* ein System nur überwachen können. Wenn sich Benutzer bei DD System Manager anmelden, sehen sie nur die Programmfunktionen, die sie basierend auf der ihnen zugewiesenen Rolle

verwenden können. Die folgenden Rollen sind für die Administration und das Management des DD OS verfügbar.

admin

Ein Benutzer mit der Rolle *admin* kann das gesamte Data Domain-System konfigurieren und überwachen. Die meisten Konfigurationsfunktionen und -befehle sind nur für Benutzer mit der Rolle *admin* verfügbar. Für einige Funktionen und Befehle ist jedoch die Genehmigung eines Benutzers mit der Rolle *security* erforderlich, bevor eine Aufgabe abgeschlossen wird.

limited-admin

Die Rolle *limited-admin* kann das Data Domain-System mit einigen Einschränkungen konfigurieren und überwachen. Benutzer mit dieser Rolle können Datenlöschvorgänge durchführen, das Verzeichnis bearbeiten oder den Bash- oder SE-Modus verwenden.

user

Benutzer mit der Rolle *user* können Systeme überwachen und das eigene Passwort ändern. Benutzer mit der Rolle *user* können den Systemstatus anzeigen, jedoch nicht die Systemkonfiguration ändern.

security (security officer)

Ein Benutzer mit der Rolle *security*, manchmal auch als Security Officer bezeichnet, kann andere Security Officer verwalten, Verfahren autorisieren, für die eine Security Officer-Genehmigung erforderlich ist, und alle Aufgaben durchführen, die für Benutzer mit der Rolle „user“ unterstützt werden.

Die Rolle *security* dient der Einhaltung der WORM-Vorschrift (Write Once Read Many). Diese Vorschrift verlangt, dass elektronisch gespeicherte Unternehmensdaten in einem unveränderten, ursprünglichen Zustand gespeichert werden, z. B. für Zwecke wie eDiscovery. Data Domain hat Audit- und Protokollierungsfunktionen hinzugefügt, um diese Funktion zu verbessern. Als Folge der Compliancevorschriften ist für die meisten Befehlsoptionen zur Verwaltung sensibler Vorgänge wie DD Encryption, DD Retention Lock Compliance und Archivierung eine Security Officer-Genehmigung erforderlich.

In einem typischen Szenario gibt ein Benutzer mit der Rolle *admin* einen Befehl aus und wenn eine Security Officer-Genehmigung erforderlich ist, wird vom System eine Aufforderung zur Genehmigung angezeigt. Um mit der ursprünglichen Aufgabe fortzufahren, muss der Security Officer seinen Benutzernamen und sein Passwort auf derselben Konsole eingeben, auf der der Befehl ausgeführt wurde. Wenn die Anmeldedaten des Security Officer vom System erkannt werden, wird das Verfahren autorisiert. Falls nicht, wird eine Sicherheitswarnmeldung erzeugt.

Im Folgenden finden Sie einige Richtlinien, die für Benutzer mit der Rolle „security“ gelten:

- Nur der *sysadmin*-Benutzer (der Standardbenutzer, der während der Installation des DD-Betriebssystems erstellt wurde) kann den ersten Security Officer erstellen. Anschließend wird dem *sysadmin*-Benutzer die Berechtigung zur Erstellung von Security Officers entzogen.
- Nachdem der erste Security Officer erstellt wurde, können nur noch Security Officers andere Security Officers erstellen.
- Durch Erstellung eines Security Officer wird die Autorisierungs-Policy nicht aktiviert. Um die Autorisierungs-Policy zu aktivieren, muss sich ein Security Officer anmelden und die Autorisierungs-Policy aktivieren.

- Es gilt eine Trennung von Rechten und Aufgaben. Benutzer mit der Rolle *admin* können keine Security Officer-Aufgaben durchführen und Security Officers können keine Systemkonfigurationsaufgaben durchführen.
- Wenn die Systemkonfiguration Security Officers enthält, wird während eines Upgrades eine Security Officer-Standardberechtigung erstellt, die eine Liste aller aktuellen Security Officers umfasst.

backup-operator

Ein Benutzer mit der Rolle *backup-operator* kann alle für Benutzer mit der Rolle *user* zulässigen Aufgaben durchführen, Snapshots für MTrees erstellen, Bänder zwischen Elementen in einer virtuellen Bandbibliothek importieren, exportieren und verschieben und Bänder zwischen Pools kopieren.

Ein Benutzer mit der Rolle *backup-operator* kann außerdem öffentliche SSH-Schlüssel für Anmeldungen hinzufügen und löschen, bei denen kein Passwort erforderlich ist. (Diese Funktion wird hauptsächlich für die automatisierte Skripterstellung verwendet.) Der Benutzer kann CLI-Befehlsaliase hinzufügen, löschen, zurücksetzen und anzeigen, geänderte Dateien synchronisieren und auf den Abschluss einer Replikation auf dem Zielsystem warten.

none

Die Rolle *none* ist nur für Benutzer der DD Boost-Authentifizierung und Benutzer mit der Rolle „tenant-unit“. Ein Benutzer mit der Rolle *none* kann sich bei einem Data Domain-System anmelden und sein Passwort ändern, er kann das primäre System jedoch nicht überwachen, verwalten oder konfigurieren. Wenn das primäre System in Mandanteneinheiten aufgeteilt wird, wird entweder die Rolle *tenant-admin* oder die Rolle *tenant-user* verwendet, um die Rolle eines Benutzers in Bezug auf eine bestimmte Mandanteneinheit zu definieren. Dem Mandantenbenutzer wird zuerst die Rolle *none* zugewiesen, um den Zugriff auf das primäre System zu minimieren, und anschließend wird entweder die Rolle *tenant-admin* oder *tenant-user* hinzugefügt.

tenant-admin

Die Rolle *tenant-admin* kann zu anderen Rollen (nicht-tenant-Rollen) hinzugefügt werden, wenn die Secure Multi-Tenancy-Funktion (SMT) aktiviert ist. Ein Benutzer mit der Rolle *tenant-admin* kann eine bestimmte Mandanteneinheit konfigurieren und überwachen.

tenant-user

Die Rolle *tenant-user* kann zu anderen Rollen (nicht-tenant-Rollen) hinzugefügt werden, wenn die SMT-Funktion aktiviert ist. Mit der Rolle *tenant-user* kann ein Benutzer eine bestimmte Mandanteneinheit überwachen und das Benutzerpasswort ändern. Benutzer mit der Rolle *tenant-user* können den Status der Mandanteneinheit anzeigen, jedoch nicht die Konfiguration der Mandanteneinheit ändern.

Zugriffsmanagement für IP-Protokolle

Diese Funktion managt den Systemzugriff für die Protokolle FTP, FTPS, HTTP, HTTPS, SSH, SCP und Telnet.

Anzeigen der Konfiguration von IP-Services

Auf der Registerkarte „Administrator Access“ wird der Konfigurationsstatus für die IP-Protokolle angezeigt, die für den Zugriff auf das System verwendet werden können.

FTP und FTPS sind die einzigen Protokolle, die nur von Administratoren verwendet werden dürfen.

Vorgehensweise

1. Wählen Sie **Administration** > **Access** > **Administrator Access**.

Ergebnisse

Auf der Seite „Access Management“ werden die Registerkarten „Administrator Access“, „Local Users“, „Authentication“ und „Active Users“ angezeigt.

Tabelle 33 Informationen der Registerkarte „Administrator Access“

Element	Beschreibung
Passphrase	Wenn keine Passphrase festgelegt wurde, wird die Schaltfläche **Set Passphrase** angezeigt. Wenn eine Passphrase festgelegt wurde, wird die Schaltfläche **Change Passphrase** angezeigt.
Services	Der Name eines Services/des Protokolls, der oder das auf das System zugreifen kann.
Enabled (Yes/No)	Der Status des Services. Wenn der Service deaktiviert ist, aktivieren Sie ihn, indem Sie den Service aus der Liste auswählen und auf **Configure** klicken. Füllen Sie die Registerkarte „General“ des Dialogfelds aus. Wenn der Service aktiviert ist, ändern Sie die Einstellungen, indem Sie den Service aus der Liste auswählen und auf **Configure** klicken. Bearbeiten Sie die Einstellungen auf der Registerkarte „General“ des Dialogfelds.
Allowed Hosts	Die Hosts, die auf den Service zugreifen können.
Serviceoptionen	Der Wert für den Port oder das Sitzungs-Timeout für den in der Liste ausgewählten Service.
FTP/FTPS	Es kann nur das Sitzungs-Timeout festgelegt werden.
HTTP port	Die Portnummer für das HTTP-Protokoll (standardmäßig Port 80).
HTTPS port	Die Portnummer für das HTTPS-Protokoll (standardmäßig Port 443).
SSH/SCP port	Die Portnummer für das SSH-/SCP-Protokoll (standardmäßig Port 22).
Telnet	Es kann keine Portnummer festgelegt werden.
Sitzungs-Timeout	Die Menge der zulässigen inaktiven Zeit, bevor eine Verbindung getrennt wird. Die Standardeinstellung ist „Infinite“, d. h. die Verbindung wird nicht getrennt. Legen Sie ein maximales Sitzungstimeout von 5 Minuten fest. Verwenden Sie die Registerkarte **Advanced** im Dialogfeld, um ein Timeout in Sekunden festzulegen.

Managen des FTP-Zugriffs

FTP (File Transfer Protocol) ermöglicht Administratoren den Zugriff auf Dateien im Data Domain-System.

Sie können den FTP- oder FTPS-Zugriff für Benutzer mit der Managementrolle „admin“ aktivieren. Der FTP-Zugriff ist eine nicht sichere Zugriffsmethode, bei der Administratorbenutzernamen und -passwörter als Klartext über das Netzwerk

gesendet werden. Als sichere Zugriffsmethode wird FTPS empfohlen. Wenn Sie FTP- oder FTPS-Zugriff aktivieren, wird die jeweils andere Zugriffsmethode deaktiviert.

Hinweis

Nur Benutzer mit Administratorrolle sind berechtigt, über FTP auf das System zuzugreifen.

Hinweis

LFTP-Clients, die sich über FTPS oder FTP mit dem Data Domain-System verbinden, werden nach einer festgelegten Timeout-Grenze getrennt. Der LFTP-Client verwendet jedoch den zwischengespeicherten Benutzernamen und das zwischengespeicherte Passwort, um nach dem Timeout eine neue Verbindung herzustellen, während Sie einen beliebigen Befehl ausführen.

Vorgehensweise

1. Wählen Sie **Administration** > **Access** > **Administrator Access**.
2. Wählen Sie **FTP** aus und klicken Sie auf **Configure**.
3. Um den FTP-Zugriff und die Hosts zu verwalten, die Verbindungen herstellen können, wählen Sie die Registerkarte „General“ aus und gehen Sie folgendermaßen vor:
   a. Um den FTP-Zugriff zu aktivieren, wählen Sie **Allow FTP Access** aus.
   b. Um allen Hosts die Verbindung zu gestatten, wählen Sie **Allow all hosts to connect**.
   c. Um den Zugriff auf ausgewählte Hosts zu beschränken, wählen Sie **Limit Access to the following systems** und ändern Sie die Liste „Allowed Hosts“.

      Hinweis

      Sie können einen Host anhand des vollständig qualifizierten Hostnamens, einer IPv4-Adresse oder einer IPv6-Adresse erkennen.

      - Klicken Sie zum Hinzufügen eines Hosts auf „Add“ (**+**). Geben Sie die Host-Identifizierung ein und klicken Sie auf **OK**.
      - Um eine Host-ID zu ändern, wählen Sie den Host in der Liste **Hosts** aus und klicken Sie auf „Edit“ (Bleistift). Ändern Sie die Host-ID und klicken Sie auf **OK**.
      - Um eine Host-ID zu entfernen, wählen Sie den Host in der Liste **Hosts** aus und klicken Sie auf „Delete“ (**X**).
4. Um ein Sitzungs-Timeout festzulegen, wählen Sie die Registerkarte **Advanced** aus und geben Sie den Timeout-Wert in Sekunden ein.

   Hinweis

   Der Standardwert für das Sitzungs-Timeout ist „Infinite“, d. h. die Verbindung wird nicht geschlossen.
5. Klicken Sie auf **OK**.

Wenn FTPS aktiviert ist, wird eine Warnmeldung mit der Aufforderung angezeigt, auf **OK** zu klicken, um fortzufahren.

Managen des FTPS-Zugriffs

Das Protokoll FTP Secure (FTPS) ermöglicht Administratoren den Zugriff auf Dateien im Data Domain-System.

FTPS bietet im Vergleich zu FTP zusätzliche Sicherheit, z. B. Unterstützung für die kryptografischen Protokolle Transport Layer Security (TLS) und Secure Sockets Layer (SSL). Beachten Sie bei der Verwendung von FTPS die folgenden Richtlinien:

- Nur Benutzer mit Administratormanagementrolle können über FTPS auf das System zugreifen.
- Wenn Sie den FTPS-Zugriff aktivieren, wird der FTP-Zugriff deaktiviert.
- Für DD-Systeme, auf denen DD OS 5.2 ausgeführt wird und die von einem DD-System mit DD OS 5.3 oder höher verwaltet werden, wird FTPS nicht als Service angezeigt.
- Wenn Sie den Befehl `get` ausgeben, wird der schwerwiegende Fehler `SSL_read: wrong version number lftp` angezeigt, wenn keine passenden Versionen von SSL auf dem Data Domain-System installiert und auf dem LFTP-Client kompiliert sind. Workaround: Versuchen Sie, den Befehl `get` für dieselbe Datei neu auszuführen.

Vorgehensweise

1. Wählen Sie **Administration** > **Access** > **Administrator Access**.
2. Wählen Sie **FTPS** aus und klicken Sie auf **Configure**.
3. Um den FTPS-Zugriff und die Hosts zu verwalten, die Verbindungen herstellen können, wählen Sie die Registerkarte General aus und gehen Sie folgendermaßen vor:
   a. Um den FTPS-Zugriff zu aktivieren, wählen Sie **Allow FTPS Access** aus.
   b. Um allen Hosts die Verbindung zu gestatten, wählen Sie **Allow all hosts to connect**.
   c. Um den Zugriff auf ausgewählte Hosts zu beschränken, wählen Sie **Limit Access to the following systems** und ändern Sie die Hostliste.

   Hinweis

   Sie können einen Host anhand des vollständig qualifizierten Hostnamens, einer IPv4-Adresse oder einer IPv6-Adresse erkennen.

   - Klicken Sie zum Hinzufügen eines Hosts auf „Add“ (**+**). Geben Sie die Host-Identifizierung ein und klicken Sie auf **OK**.
   - Um eine Host-ID zu ändern, wählen Sie den Host in der Liste **Hosts** aus und klicken Sie auf „Edit“ (Bleistift). Ändern Sie die Host-ID und klicken Sie auf **OK**.
   - Um eine Host-ID zu entfernen, wählen Sie den Host in der Liste **Hosts** aus und klicken Sie auf „Delete“ (**X**).
4. Um ein Sitzungs-Timeout festzulegen, wählen Sie die Registerkarte **Advanced** aus und geben Sie den Timeout-Wert in Sekunden ein.

Hinweis

Der Standardwert für das Sitzungs-Timeout ist „Infinite“, d. h. die Verbindung wird nicht geschlossen.

5. Klicken Sie auf **OK**. Wenn FTP aktiviert ist, wird eine Warnmeldung mit der Aufforderung angezeigt, auf **OK** zu klicken, um fortzufahren.

Managen des HTTP- und HTTPS-Zugriffs

HTTP- bzw. HTTPS-Zugriff ist zur Unterstützung des Zugriffs auf DD System Manager über einen Browser erforderlich.

Vorgehensweise

1. Wählen Sie **Administration** > **Access** > **Administrator Access**.
2. Wählen Sie **HTTP** oder **HTTPS** und klicken Sie auf **Configure**.

   Das Dialogfeld „Configure HTTP/HTTPS Access“ wird angezeigt. Darin werden Registerkarten für die allgemeine Konfiguration, erweiterte Konfiguration und das Zertifikatsmanagement angezeigt.
3. Um die Zugriffsmethode zu verwalten und zu bestimmen, welche Hosts sich verbinden können, wählen Sie die Registerkarte „General“ und gehen Sie wie folgt vor:
   a. Aktivieren Sie die Kontrollkästchen der Zugriffsmethoden, die Sie zulassen möchten.
   b. Um allen Hosts die Verbindung zu gestatten, wählen Sie **Allow all hosts to connect**.
   c. Um den Zugriff auf ausgewählte Hosts zu beschränken, wählen Sie **Limit Access to the following systems** und ändern Sie die Hostliste.

   Hinweis

   Sie können einen Host anhand des vollständig qualifizierten Hostnamens, einer IPv4-Adresse oder einer IPv6-Adresse erkennen.

   - Klicken Sie zum Hinzufügen eines Hosts auf „Add“ (**+**). Geben Sie die Host-Identifizierung ein und klicken Sie auf **OK**.
   - Um eine Host-ID zu ändern, wählen Sie den Host in der Liste **Hosts** aus und klicken Sie auf „Edit“ (Bleistift). Ändern Sie die Host-ID und klicken Sie auf **OK**.
   - Um eine Host-ID zu entfernen, wählen Sie den Host in der Liste **Hosts** aus und klicken Sie auf „Delete“ (**X**).
4. Um Systemports und Werte für das Sitzungs-Timeout zu konfigurieren, wählen Sie die Registerkarte **Advanced** und füllen Sie das Formular aus.
   - Geben Sie im Feld **HTTP Port** die Portnummer ein. Port 80 ist standardmäßig zugewiesen.
   - Geben Sie im Feld **HTTPS Port** die Nummer ein. Port 443 ist standardmäßig zugewiesen.
   - Geben Sie im Textfeld **Session Timeout** das Intervall in Sekunden ein, das verstreichen soll, bevor eine Verbindung getrennt wird. Der Mindestwert beträgt 60 Sekunden und der Höchstwert beträgt 31.536.000 Sekunden (ein Jahr).

Hinweis

Der Standardwert für das Sitzungs-Timeout ist „Infinite“, d. h. die Verbindung wird nicht geschlossen.

5. Klicken Sie auf **OK**.

Managen von Hostzertifikaten für HTTP und HTTPS

Ein Hostzertifikat ermöglicht es Browsern, die Identität des Systems zu überprüfen, wenn Managementsitzungen erstellt werden.

Anfordern eines Hostzertifikats für HTTP und HTTPS

Sie können DD System Manager verwenden, um eine Hostzertifikatanforderung zu erzeugen, die Sie dann an eine Zertifizierungsstelle weiterleiten können.

Hinweis

Sie müssen eine Systempassphrase (ein Systempassphrasen-Set) konfigurieren, bevor Sie eine Zertifikatsignieranforderung erzeugen können.

Vorgehensweise

1. Wählen Sie **Administration** > **Access** > **Administrator Access**.
2. Wählen Sie im Bereich „Services“ **HTTP** oder **HTTPS** und klicken Sie auf **Configure**.
3. Wählen Sie die Registerkarte **Certificate**.
4. Klicken Sie auf Hinzufügen.

   Es wird ein Dialogfeld für das Protokoll angezeigt, das Sie zuvor in diesem Verfahren ausgewählt haben.

5. Klicken Sie auf **Generate the CSR for this Data Domain system**.

   Das Dialogfeld wird erweitert, um ein CSR-Formular anzuzeigen.

   Hinweis

   DD OS unterstützt eine aktive CSR gleichzeitig. Nachdem eine CSR erzeugt wurde, wird der Link **Generate the CSR for this Data Domain system** durch den Link **Download the CSR for this Data Domain system** ersetzt. Um eine Zertifikatsignieranforderung zu löschen, verwenden Sie den Befehl `adminaccess certificate cert-signing-request delete` der Befehlszeilenoberfläche.

6. Füllen Sie das CSR-Formular aus und klicken Sie auf **Generate and download a CSR**.

   Die CSR-Datei wird unter folgendem Pfad gespeichert: `/ddvar/certificates/CertificateSigningRequest.csr`. Verwenden Sie SCP, FTP oder FTPS, um die CSR-Datei vom System auf einen Computer zu übertragen, von dem aus Sie die Zertifikatsignieranforderung an eine Zertifizierungsstelle senden können.

Hinzufügen eines Hostzertifikats für HTTP und HTTPS

Sie können DD System Manager verwenden, um ein Hostzertifikat zum System hinzuzufügen.

Vorgehensweise

1. Wenn Sie noch kein Hostzertifikat angefordert haben, fordern Sie ein Hostzertifikat von einer Zertifizierungsstelle an.
2. Wenn Sie ein Hostzertifikat erhalten, kopieren oder verschieben Sie es auf den Computer, von dem Sie DD Service Manager ausführen.
3. Wählen Sie **Administration** > **Access** > **Administrator Access**.
4. Wählen Sie im Bereich „Services“ **HTTP** oder **HTTPS** aus und klicken Sie auf **Configure**.
5. Wählen Sie die Registerkarte **Certificate**.
6. Klicken Sie auf **Hinzufügen**.

   Es wird ein Dialogfeld für das Protokoll angezeigt, das Sie zuvor in diesem Verfahren ausgewählt haben.

7. Gehen Sie wie folgt vor, um ein Hostzertifikat hinzuzufügen, das in eine .p12-Datei eingeschlossen ist:
   a. Wählen Sie **I want to upload the certificate as a .p12 file**.
   b. Geben Sie das Passwort in das Feld **Password** ein.
   c. Klicken Sie auf **Browse** und wählen Sie die Hostzertifikatdatei aus, die an das System hochgeladen werden soll.
   d. Klicken Sie auf **Add**.
8. Gehen Sie wie folgt vor, um ein Hostzertifikat hinzuzufügen, das in eine .pem-Datei eingeschlossen ist:
   a. Wählen Sie **I want to upload the public key as a .pem file and use a generated private key**.
   b. Klicken Sie auf **Browse** und wählen Sie die Hostzertifikatdatei aus, die an das System hochgeladen werden soll.
   c. Klicken Sie auf **Add**.

Löschen eines Hostzertifikats für HTTP und HTTPS

DD OS unterstützt ein Hostzertifikat für HTTP und HTTPS. Wenn das System derzeit ein Hostzertifikat verwendet und Sie ein anderes Hostzertifikat verwenden möchten, müssen Sie vor dem Hinzufügen des neuen Zertifikats zuerst das aktuelle Zertifikat löschen.

Vorgehensweise

1. Wählen Sie **Administration** > **Access** > **Administrator Access**.
2. Wählen Sie im Bereich „Services“ **HTTP** oder **HTTPS** aus und klicken Sie auf **Configure**.
3. Wählen Sie die Registerkarte **Certificate**.
4. Wählen Sie das Zertifikat aus, das Sie löschen möchten.
5. Klicken Sie auf **Delete** und dann auf **OK**.

Managen des SSH- und SCP-Zugriffs

SSH ist ein sicheres Protokoll, das den Netzwerkzugriff auf die Befehlszeilenoberfläche des Systems mit oder ohne SCP (Secure Copy) ermöglicht. Sie können DD System Manager verwenden, um den Systemzugriff mithilfe des SSH-Protokolls zu ermöglichen. Für SCP ist SSH erforderlich. Wenn SSH deaktiviert ist, wird SCP automatisch deaktiviert.

Vorgehensweise

1. Wählen Sie **Administration** > **Access** > **Administrator Access**.
2. Wählen Sie**SSH** or **SCP** und klicken Sie auf **Configure**.
3. Um die Zugriffsmethode zu managen und zu bestimmen, welche Hosts sich verbinden können, wählen Sie die Registerkarte **General**.
   a. Aktivieren Sie die Kontrollkästchen der Zugriffsmethoden, die Sie zulassen möchten.
   b. Um allen Hosts die Verbindung zu gestatten, wählen Sie **Allow all hosts to connect**.
   c. Um den Zugriff auf ausgewählte Hosts zu beschränken, wählen Sie **Limit Access to the following systems** und ändern Sie die Hostliste.

   Hinweis

   Sie können einen Host anhand des vollständig qualifizierten Hostnamens, einer IPv4-Adresse oder einer IPv6-Adresse erkennen.

   - Klicken Sie zum Hinzufügen eines Hosts auf „Add“ (**+**). Geben Sie die Host-Identifizierung ein und klicken Sie auf **OK**.
   - Um eine Host-ID zu ändern, wählen Sie den Host in der Liste **Hosts** aus und klicken Sie auf „Edit“ (Bleistift). Ändern Sie die Host-ID und klicken Sie auf **OK**.
   - Um eine Host-ID zu entfernen, wählen Sie den Host in der Liste **Hosts** aus und klicken Sie auf „Delete“ (**X**).
4. Um Systemports und Werte für das Sitzungs-Timeout zu konfigurieren, klicken Sie auf die Registerkarte **Advanced**.
   - Geben Sie in das Texteingabefeld für den Port **SSH/SCP**die Portnummer ein. Standardmäßig ist Port 22 zugewiesen.
   - Geben Sie im Feld **Session Timeout** das Intervall in Sekunden ein, das verstreichen soll, bevor die Verbindung getrennt wird.

   Hinweis

   Der Standardwert für das Sitzungs-Timeout ist „Infinite“, d. h. die Verbindung wird nicht geschlossen.

   Hinweis

   Klicken Sie auf **Default**, um zum Standardwert zurückzukehren.
5. Klicken Sie auf **OK**.

Managen des Telnet-Zugriffs

Telnet ist ein nicht sicheres Protokoll, das den Netzwerkzugriff auf die Benutzeroberfläche des Systems ermöglicht.

Hinweis

Mit dem Telnet-Zugriff können Benutzernamen und Passwörter im Klartext über das Netzwerk übertragen werden, was Telnet zu einem nicht sicheren Zugriffsverfahren macht.

Vorgehensweise

1. Wählen Sie **Administration** > **Access** > **Administrator Access**.
2. Wählen Sie **Telnet** und klicken Sie auf **Configure**.
3. Um den Telnet-Zugriff zu verwalten und zu bestimmen, welche Hosts sich verbinden können, wählen Sie die Registerkarte **General**.
   a. Um den Telnet-Zugriff zu aktivieren, wählen Sie **Allow Telnet Access**.
   b. Um allen Hosts die Verbindung zu gestatten, wählen Sie **Allow all hosts to connect**.
   c. Um den Zugriff auf ausgewählte Hosts zu beschränken, wählen Sie **Limit Access to the following systems** und ändern Sie die Hostliste.

      Hinweis

      Sie können einen Host anhand des vollständig qualifizierten Hostnamens, einer IPv4-Adresse oder einer IPv6-Adresse erkennen.

      - Klicken Sie zum Hinzufügen eines Hosts auf „Add“ (**+**). Geben Sie die Host-Identifizierung ein und klicken Sie auf **OK**.
      - Um eine Host-ID zu ändern, wählen Sie den Host in der Liste **Hosts** aus und klicken Sie auf „Edit“ (Bleistift). Ändern Sie die Host-ID und klicken Sie auf **OK**.
      - Um eine Host-ID zu entfernen, wählen Sie den Host in der Liste **Hosts** aus und klicken Sie auf „Delete“ (**X**).
4. Um ein Sitzungs-Timeout festzulegen, wählen Sie die Registerkarte „Advanced“ aus und geben Sie den Timeout-Wert in Sekunden ein.

   Hinweis

   Der Standardwert für das Sitzungs-Timeout ist „Infinite“, d. h. die Verbindung wird nicht geschlossen.
5. Klicken Sie auf **OK**.

Management von lokalen Benutzerkonten

Bei einem lokalen Benutzer handelt es sich um ein Benutzerkonto (Benutzername und Passwort), das auf dem Data Domain-System und nicht in einem Windows Active Directory, in einer Windows-Arbeitsgruppe oder in einem NIS-Verzeichnis definiert wird.

UID-Konflikte: Lokale Benutzer- und NIS-Benutzerkonten

Wenn Sie ein Data Domain-System in einer NIS-Umgebung konfigurieren, berücksichtigen Sie potenzielle UID-Konflikte zwischen lokalen und NIS-Benutzerkonten.

Lokale Benutzerkonten auf einem Data Domain-System beginnen mit einer UID von 500. Um Konflikte zu vermeiden, berücksichtigen Sie bei der Definition zulässiger UID-Bereiche für NIS-Benutzer die Größe potenzieller lokaler Konten.

Anzeigen der lokalen Benutzerinformationen

Lokale Benutzer sind Benutzerkonten, die nicht in Active Directory, in einer Arbeitsgruppe oder UNIX, sondern auf dem System definiert sind. Sie können Benutzername, Managementrolle, Anmeldestatus und Zieldeaktivierungsdatum des lokalen Benutzers anzeigen. Zudem können Sie die Passwort-Steuerelemente des Benutzers und die Mandanteneinheiten anzeigen, auf die der Benutzer zugreifen kann, anzeigen.

Hinweis

Das Benutzerauthentifizierungsmodul verwendet GMT (Greenwich Mean Time). Um dafür zu sorgen, dass Benutzerkonten und Passwörter ordnungsgemäß ablaufen, konfigurieren Sie die entsprechenden Einstellungen so, dass die GMT verwendet wird, die der Ortszeit des Ziels entspricht.

Vorgehensweise

1. Wählen Sie **Administration** > **Access** > **Local Users** .

   Die Ansicht „Local Users“ wird mit der Tabelle „Local Users“ und dem Bereich „Detailed Information“ angezeigt.

Tabelle 34 Liste lokaler Benutzer, Beschreibungen der Spaltenbezeichnungen

Element	Beschreibung
Name	Die Benutzer-ID, die dem System hinzugefügt wurde.
Management Role	Mögliche Werte sind „admin“, „user“, „security“, „backup-operator“ oder „none“. In dieser Tabelle werden Mandantenbenutzerrollen als *none* angezeigt. Wählen Sie zum Anzeigen einer zugewiesenen Mandantenrolle den Benutzer aus und zeigen Sie die Rolle im Bereich mit den detaillierten Informationen an.
Status	• Active: Benutzerzugriff das Konto ist zulässig. • Disabled: Der Benutzerzugriff auf das Konto wird verweigert, da das Konto vom Administrator deaktiviert wurde, das aktuelle Datum das Ablaufdatum für das Konto überschritten hat oder das Passwort eines gesperrten Kontos verlängert werden muss. • Locked: Der Benutzerzugriff wird verweigert, weil das Passwort abgelaufen ist.
Disable Date	Das Datum, an dem das Konto als deaktiviert festgelegt wird.
Last Login From	Der Ort, an dem der Benutzer das letzte Mal angemeldet war.

Tabelle 34 Liste lokaler Benutzer, Beschreibungen der Spaltenbezeichnungen (Fortsetzung)

Element	Beschreibung
Last Login Time	Der Zeitpunkt, zu dem der Benutzer sich das letzte Mal angemeldet hat.

Hinweis

Mit der Administrator- oder Security Officer-Rolle konfigurierte Benutzerkonten können alle Benutzer anzeigen. Benutzer mit anderen Rollen können nur ihre eigenen Benutzerkonten anzeigen.

2. Wählen Sie den Benutzer, den Sie anzeigen möchten, aus der Liste der Benutzer aus.

   Informationen über den ausgewählten Benutzer werden im Bereich „Detailed Information“ angezeigt.

Tabelle 35 Detaillierte Benutzerinformationen, Beschreibungen der Reihenbezeichnungen

Element	Beschreibung
Tenant-User	Die Liste der Mandanteneinheiten, auf die der Benutzer als Benutzer mit der Rolle „tenant-user“ zugreifen kann.
Tenant-Admin	Die Liste der Mandanteneinheiten, auf die der Benutzer als Benutzer mit der Rolle „tenant-admin“ zugreifen kann.
Password Last Changed	Das Datum, an dem das Passwort zuletzt geändert wurde.
Minimum Days Between Change	Die Mindestanzahl an Tagen zwischen Passwortänderungen, die Sie für einen Benutzer festlegen. Der Standardwert ist 0.
Maximum Days Between Change	Die Höchstanzahl an Tagen zwischen Passwortänderungen, die Sie für einen Benutzer festlegen. Der Standardwert lautet 90.
Warn Days Before Expire	Die Anzahl der Tage, die der Benutzer eine Warnmeldung erhält, bevor sein Passwort abläuft. Der Standardwert ist 7.
Disable Days After Expire	Die Anzahl der Tage, nach der ein Passwort abläuft, um das Benutzerkonto zu deaktivieren. Der Standardwert ist „Never“.

Hinweis

Die Standardwerte sind die ursprünglichen Werte für die standardmäßige Passwort-Policy. Ein Systemadministrator (Administratorrolle) kann sie durch Auswahl von **More Tasks** > **Change Login Options** ändern.

Erstellen von lokalen Benutzern

Erstellen Sie lokale Benutzer, wenn Sie den Zugriff auf das lokale System statt über ein externes Verzeichnis managen möchten. Data Domain-Systeme unterstützen maximal 500 lokale Benutzerkonten.

Vorgehensweise

1. Wählen Sie **Administration** > **Access** > **Local Users**.

   Die Ansicht „Local Users“ wird geöffnet.

2. Um einen neuen Benutzer zu erstellen, klicken Sie auf **Create**.

   Das Dialogfeld „Create User“ wird angezeigt.

3. Geben Sie die Benutzerinformationen auf der Registerkarte „General“ ein.

Tabelle 36 Dialogfeld „Create User“, Steuerelemente unter „General“

Element	Beschreibung
Benutzer	Die Benutzer-ID oder der Name.
Passwort	Das Benutzerpasswort. Erstellen Sie ein Standardpasswort, das der Benutzer später ändern kann.
Verify Password	Das Benutzerpasswort, erneut.
Management Role	Die Rolle, die dem Benutzer zugewiesen wurde. Mögliche Werte sind „admin“, „user“, „security“, „backup-operator“ oder keiner. **Hinweis** Nur der sysadmin-Benutzer (der Standardbenutzer, der während der DD OS-Installation erstellt wurde), kann den ersten Sicherheitsrollenbenutzer erstellen. Nachdem der erste Sicherheitsrollenbenutzer erstellt wurde, können nur Sicherheitsrollenbenutzer andere Sicherheitsrollenbenutzer erstellen.
Passwortänderung erzwingen	Aktivieren Sie dieses Kontrollkästchen, um zu erzwingen, dass der Benutzer das Passwort während der ersten Anmeldung bei DD System Manager oder der CLI mit SSH oder Telnet ändert.

Der Standardwert für die Mindestlänge eines Passworts beträgt 6 Zeichen. Der Standardwert für die Mindestanzahl von Zeichenklassen, die für ein Benutzerpasswort erforderlich sind, ist 1. Zulässige Zeichenklassen umfassen:

- Kleinbuchstaben (a-z)
- Großbuchstaben (A-Z)
- Zahlen (0-9)
- Sonderzeichen ($, %, #, + usw.)

Hinweis

Sysadmin ist der standardmäßige Administratorrollenbenutzer, der weder gelöscht noch geändert werden kann.

4. Wählen Sie zur Verwaltung des Passwort- und Kennwortablaufs die Registerkarte „Advanced“ und verwenden Sie die in der folgenden Tabelle beschriebenen Steuerelemente.

Tabelle 37 Dialogfeld „Create User“, Steuerelemente unter „Advanced“

Element	Beschreibung
Minimum Days Between Change	Die Mindestanzahl an Tagen zwischen Passwortänderungen, die Sie für einen Benutzer festlegen. Der Standardwert ist 0.

Tabelle 37 Dialogfeld „Create User“, Steuerelemente unter „Advanced“ (Fortsetzung)

Element	Beschreibung
Maximum Days Between Change	Die Höchstanzahl an Tagen zwischen Passwortänderungen, die Sie für einen Benutzer festlegen. Der Standardwert lautet 90.
Warn Days Before Expire	Die Anzahl der Tage, die der Benutzer eine Warnmeldung erhält, bevor sein Passwort abläuft. Der Standardwert ist 7.
Disable Days After Expire	Die Anzahl der Tage, nach der ein Passwort abläuft, um das Benutzerkonto zu deaktivieren. Der Standardwert ist „Never“.
Disable account on the following date	Aktivieren Sie dieses Kontrollkästchen und geben Sie ein Datum (tt.mm.jjjj) ein, zu dem Sie dieses Konto deaktivieren möchten. Sie können auf den Kalender klicken und ein Datum auswählen.

5. Klicken Sie auf **OK**.

Hinweis

Hinweis: Die standardmäßige Passwort-Policy kann sich ändern, wenn ein Administrator diese ändert (**More Tasks** > **Change Login Options**). Die Standardwerte sind die ursprünglichen Werte für die standardmäßige Passwort-Policy.

Ändern eines lokalen Benutzerprofils

Nach dem Erstellen eines Benutzers können Sie DD System Manager verwenden, um die Konfiguration des Benutzers zu ändern.

Vorgehensweise

1. Wählen Sie **Administration** > **Access** > **Local Users**.

   Die Ansicht „Local Users“ wird geöffnet.

2. Klicken Sie auf einen Benutzernamen in der Liste.
3. Klicken Sie auf **Modify**, um Änderungen an einem Benutzerkonto vorzunehmen.

   Das Dialogfeld „Modify User“ wird angezeigt.
4. Aktualisieren Sie die Informationen auf der Registerkarte „General“.

Hinweis

Wenn SMT aktiviert ist und eine Rollenänderung von "none" zu einer anderen Rolle angefordert wird, wird die Änderung nur übernommen, wenn Folgendes gilt: Der Benutzer ist keiner Mandanteneinheit als Managementbenutzer zugewiesen, er ist kein DD Boost-Benutzer mit festgelegter Standardmandanteneinheit und er ist nicht der Eigentümer einer Speichereinheit, die einer Mandanteneinheit zugewiesen wurde.

Hinweis

Um die Rolle für einen DD Boost-Benutzer zu ändern, der keine Speichereinheiten besitzt, heben Sie die Zuweisung als DD Boost-Benutzer auf, ändern Sie die Benutzerrolle und weisen Sie sie erneut als DD Boost-Benutzer zu.

Tabelle 38 Dialogfeld „Modify User“, Steuerelemente unter „General“

Element	Beschreibung
Benutzer	Die Benutzer-ID oder der Name.
Rolle	Wählen Sie die Rolle in der Liste aus.

5. Aktualisieren Sie die Informationen auf der Registerkarte „Advanced“.

Tabelle 39 Dialogfeld „Modify User“, Steuerelemente unter „Advanced“

Element	Beschreibung
Minimum Days Between Change	Die Mindestanzahl an Tagen zwischen Passwortänderungen, die Sie für einen Benutzer festlegen. Der Standardwert ist 0.
Maximum Days Between Change	Die Höchstanzahl an Tagen zwischen Passwortänderungen, die Sie für einen Benutzer festlegen. Der Standardwert lautet 90.
Warn Days Before Expire	Die Anzahl der Tage, die der Benutzer eine Warnmeldung erhält, bevor sein Passwort abläuft. Der Standardwert ist 7.
Disable Days After Expire	Die Anzahl der Tage, nach der ein Passwort abläuft, um das Benutzerkonto zu deaktivieren. Der Standardwert ist „Never“.

6. Klicken Sie auf **OK**.

Löschen lokaler Benutzer

Sie können bestimmte Benutzer auf der Basis Ihrer Benutzerrolle löschen. Wenn einer der ausgewählten Benutzer nicht gelöscht werden kann, ist die Schaltfläche „Delete“ deaktiviert.

Der sysadmin-Benutzer kann nicht gelöscht werden. Administratorbenutzer können keine Security Officers löschen. Nur Security Officers können andere Security Officers löschen, aktivieren und deaktivieren.

Vorgehensweise

1. Wählen Sie **Administration** > **Access** > **Local Users**.

   Die Ansicht „Local Users“ wird geöffnet.

2. Klicken Sie auf einen oder mehrere Benutzernamen aus der Liste.
3. Klicken Sie auf **Delete**, um die Benutzerkonten zu löschen.

   Das Dialogfeld „Delete User“ wird angezeigt.

4. Klicken Sie auf **OK** und **Close**.

Aktivieren und Deaktivieren lokaler Benutzer

Administratorbenutzer können außer dem sysadmin-Benutzer und Benutzern mit der Sicherheitsrolle alle Benutzer aktivieren oder deaktivieren. Der sysadmin-Benutzer

kann nicht deaktiviert werden. Nur Security Officer können andere Security Officers aktivieren oder deaktivieren.

Vorgehensweise

1. Wählen Sie**Administration** > **Access** > **Local Users**.

   Die Ansicht „Local Users“ wird geöffnet.

2. Klicken Sie auf einen oder mehrere Benutzernamen aus der Liste.
3. Klicken Sie entweder auf **Enable** oder **Disable**, um Benutzerkonten zu aktivieren oder zu deaktivieren.

   Das Dialogfeld „Enable or Disable User“ wird angezeigt.

4. Klicken Sie auf **OK** und **Close**.

Aktivieren der Sicherheitsautorisierung

Sie können die Befehlszeilenoberfläche (CLI) des Data Domain-Systems verwenden, um die Sicherheitsautorisierungs-Policy zu aktivieren und zu deaktivieren.

Informationen zu den Befehlen, die in diesem Verfahren verwendet werden, finden Sie im *Data Domain Operating System Command Reference Guide*.

Hinweis

Die DD Retention Lock Compliance-Lizenz muss installiert sein. Sie sind nicht berechtigt, die Autorisierungs-Policy auf DD Retention Lock Compliance-Systemen zu deaktivieren.

Vorgehensweise

1. Melden Sie sich mit einem Security Officer-Benutzernamen und -Passwort bei der CLI an.
2. Geben Sie Folgendes ein, um die Security Officer-Autorisierungs-Policy zu aktivieren: `# authorization policy set security-officer enabled`

Ändern von Benutzerpasswörtern

Nach dem Erstellen eines Benutzers können Sie DD System Manager verwenden, um das Passwort des Benutzers zu ändern. Auch einzelne Benutzer können ihre eigenen Passwörter ändern.

Vorgehensweise

1. Klicken Sie auf **Administration** > **Access** > **Local Users**.

   Die Ansicht „Local Users“ wird geöffnet.

2. Klicken Sie auf einen Benutzernamen in der Liste.
3. Klicken Sie auf **Change Password**, um das Benutzerpasswort zu ändern.

   Das Dialogfeld „Change Password“ wird angezeigt.

   Geben Sie nach Aufforderung das alte Passwort ein.

4. Geben Sie im Feld **New Passwort** das neue Passwort ein.
5. Geben Sie im Feld **Verify New Password** das neue Passwort erneut ein.
6. Klicken Sie auf **OK**.

Ändern von Passwortrichtlinie und Anmeldungskontrolle

Passwortrichtlinie und Anmeldungskontrolle definieren Anmeldeanforderungen für alle Benutzer. Administratoren können festlegen, wie häufig ein Passwort geändert werden muss, was zum Erstellen eines gültigen Passworts erforderlich ist und wie das System auf ungültige Anmeldeversuche reagiert.

Vorgehensweise

1. Wählen Sie **Administration** > **Access**.
2. Wählen Sie **More Tasks** > **Change Login Options**.

   Das Dialogfeld „Change Login Options“ wird angezeigt.

3. Legen Sie die neue Konfiguration in den Feldern für die jeweilige Option fest. Klicken Sie zum Auswählen des Standardwerts neben der jeweiligen Option auf **Default**.
4. Klicken Sie auf **OK**, um die Passworteinstellungen zu speichern.

Dialogfeld „Change Login Options“

Verwenden Sie dieses Dialogfeld, um die Passwortrichtlinie festzulegen und die maximal zulässige Anzahl Anmeldeversuche und die Sperrdauer anzugeben.

Tabelle 40 Steuerelemente im Dialogfeld „Change Login Options“

Element	Beschreibung
Minimum Days Between Change	Die Mindestanzahl an Tagen zwischen Passwortänderungen, die Sie für einen Benutzer festlegen. Dieser Wert muss kleiner als der Wert **Maximum Days Between Change** minus dem Wert **Warn Days Before Expire** sein. Die Standardeinstellung lautet 0.
Maximum Days Between Change	Die Höchstanzahl an Tagen zwischen Passwortänderungen, die Sie für einen Benutzer festlegen. Der Mindestwert ist 1. Der Standardwert ist 90.
Warn Days Before Expire	Die Anzahl der Tage, die der Benutzer eine Warnmeldung erhält, bevor sein Passwort abläuft. Der Wert muss kleiner als der Wert **Maximum Days Between Change** minus dem Wert **Minimum Days Between Change** sein. Die Standardeinstellung lautet 7.
Disable Days After Expire	Das System deaktiviert ein Benutzerkonto nach Ablauf des Passworts gemäß der in dieser Option festgelegten Anzahl von Tagen. Gültige Einträge sind *never* oder eine Zahl größer als oder gleich 0. Die Standardeinstellung ist „never“.
Minimum Length of Password	Die erforderliche Passwort-Mindestlänge. Der Standardwert lautet 6.
Minimum Number of Character Classes	Die Mindestanzahl der Zeichenklassen, die für ein Benutzerpasswort erforderlich sind. Der Standardwert lautet 1. Zeichenklassen beinhalten die folgenden: • Kleinbuchstaben (a-z) • Großbuchstaben (A-Z) • Zahlen (0-9) • Sonderzeichen ($, %, #, + usw.)

Tabelle 40 Steuerelemente im Dialogfeld „Change Login Options“ (Fortsetzung)

Element	Beschreibung
Lowercase Character Requirement	Aktivieren oder deaktivieren Sie die Anforderung für mindestens ein Zeichen in Kleinschreibung. Die Einstellung ist standardmäßig deaktiviert.
Uppercase Character Requirement	Aktivieren oder deaktivieren Sie die Anforderung für mindestens ein Zeichen in Großschreibung. Die Einstellung ist standardmäßig deaktiviert.
One Digit Requirement	Aktivieren oder deaktivieren Sie die Anforderung für mindestens ein numerisches Zeichen. Die Einstellung ist standardmäßig deaktiviert.
Special Character Requirement	Aktivieren oder deaktivieren Sie die Anforderung für mindestens ein Sonderzeichen. Die Einstellung ist standardmäßig deaktiviert.
Max Consecutive Character Requirement	Aktivieren oder deaktivieren Sie die Anforderung für maximal drei wiederholte Zeichen. Die Einstellung ist standardmäßig deaktiviert.
Prevent use of Last N Passwords	Geben Sie die Anzahl der gespeicherten Passwörter an. Der Bereich liegt zwischen 0 und 24. Die Standardeinstellung lautet 1. **Hinweis** Wird dieser Wert verkleinert, bleibt die Liste der gespeicherten Passwörter bis zur nächsten Änderung des Passworts unverändert. Wenn dieser Wert beispielsweise von 4 in 3 geändert wird, bleiben die letzten vier Passwörter bis zur nächsten Änderung des Passworts gespeichert.
Maximum login attempts	Gibt die maximale Anzahl an Anmeldeversuchen an, bevor eine obligatorische Sperre auf das Benutzerkonto angewendet wird. Diese Begrenzung gilt für alle Benutzerkonten, auch für das sysadmin-Konto. Ein gesperrter Benutzer kann sich nicht anmelden, solange das Konto gesperrt ist. Der Bereich liegt zwischen 4 und 10. Die Standardeinstellung lautet 4.
Unlock timeout (seconds)	Gibt an, wie lange ein Benutzerkonto nach Überschreiten der maximalen Anzahl an Anmeldeversuchen gesperrt bleibt. Wenn das konfigurierte Timeout für das Entsperren erreicht ist, kann sich ein Benutzer wieder anmelden. Der Bereich liegt zwischen 120 bis 600 Sekunden. Die Dauer beträgt standardmäßig 120 Sekunden.

Verzeichnisbenutzer- und Verzeichnisgruppenmanagement

Sie können DD System Manager verwenden, um den Zugriff auf das System für Benutzer und Gruppen in Windows Active Directory, Windows-Arbeitsgruppen und NIS zu managen. Dabei ist die Kerberos-Authentifizierung eine Option für CIFS- und NFS-Clients.

Anzeigen von Active Directory- und Kerberos-Informationen

Die Active Directory-/Kerberos-Konfiguration bestimmt die Authentifizierungsmethoden für CIFS- und NFS-Clients. Diese Konfiguration wird im Bereich „Active Directory/Kerberos Authentication“ angezeigt.

Vorgehensweise

1. Wählen Sie **Administration** > **Access** > **Authentication**.
2. Blenden Sie den Bereich „Active Directory/Kerberos Authentication“ ein.

Tabelle 41 Beschreibungen der Bezeichnungen für die Active Directory-/Kerberos-Authentifizierung

Element	Beschreibung
Mode	Typ des Authentifizierungsmodus. Im Windows/Active Directory-Modus verwenden CIFS-Clients die Active Directory- und Kerberos-Authentifizierung und NFS-Clients verwenden die Kerberos-Authentifizierung. Im Unix-Modus verwenden CIFS-Clients die Arbeitsgruppenauthentifizierung (ohne Kerberos) und NFS-Clients verwenden die Kerberos-Authentifizierung. Im deaktivierten Modus ist die Kerberos-Authentifizierung deaktiviert und CIFS-Clients verwenden die Arbeitsgruppenauthentifizierung.
Bereich	Der Bereichsname der Arbeitsgruppe oder von Active Directory
DDNS	Aktivierungsstatus von Dynamic Domain Name System
Domain Controllers	Der Name des Domaincontrollers für die Arbeitsgruppe oder Active Directory
Organisationseinheit	Der Name der Organisationseinheit für die Arbeitsgruppe oder Active Directory
CIFS Server Name	Der Name des verwendeten CIFS-Servers (nur Windows-Modus)
WINS Server	Der Name des verwendeten WINS-Servers (nur Windows-Modus)
Short Domain Name	Ein abgekürzter Name für die Domain
NTP	„Enabled“/„Disabled“ (nur UNIX-Modus)
NIS	„Enabled“/„Disabled“ (nur UNIX-Modus)
Key Distribution Centers	Hostnamen oder IP-Adressen des verwendeten KDC (nur UNIX-Modus)
Active Directory Administrative Access	Aktiviert/deaktiviert: Klicken Sie auf dieses Element, um den Administratorzugriff für Active Directory-Gruppen (Windows) zu aktivieren bzw. zu deaktivieren.

Tabelle 42 Administratorgruppen und -rollen bei Active Directory

Element	Beschreibung
Windows Group	Der Name der Windows-Gruppe.
Management Role	Die Rolle der Gruppe (admin, user usw.)

Konfigurieren der Active Directory-/Kerberos-Authentifizierung

Durch Konfigurieren der Active Directory-Authentifizierung wird das Data Domain-System zu einem Teil eines Windows Active Directory-Bereichs. CIFS-Clients und NFS-Clients verwenden die Kerberos-Authentifizierung.

Vorgehensweise

1. Wählen Sie **Administration** > **Access** > **Authentication**.
   Die Authentifizierungsansicht wird angezeigt.

2. Blenden Sie den Bereich „Active Directory/Kerberos Authentication“ ein.
3. Klicken Sie auf **Configure...** neben dem Modus, um den Konfigurationsassistenten zu starten.

   Das Dialogfeld „Active Directory/Kerberos Authentication“ wird angezeigt.
4. Wählen Sie **Windows/Active Directory** aus und klicken Sie auf **Next**.
5. Geben Sie den vollständigen Namen des Bereichs für das System ein (z. B. „domain1.local“) sowie den Benutzernamen und das Passwort für das Data Domain-System. Klicken Sie dann auf **Weiter**.

   Hinweis

   Verwenden Sie den vollständigen Namen des Bereichs. Stellen Sie sicher, dass dem Benutzer ausreichende Berechtigungen zugewiesen sind, um das System mit der Domain zu verbinden. Der Benutzername und das Passwort müssen mit Microsoft-Anforderungen für die Active Directory-Domain kompatibel sein. Diesem Benutzer muss auch die Berechtigung zum Erstellen von Konten in dieser Domain zugewiesen sein.
6. Wählen Sie den Standard-CIFS-Servernamen aus. Wählen Sie alternativ **Manual** aus und geben Sie einen CIFS-Servernamen ein.
7. Um Domaincontroller auszuwählen, wählen Sie **Automatically assign** aus. Wählen Sie alternativ **Manual** aus und geben Sie bis zu drei Domaincontrollernamen ein.

   Sie können vollständig qualifizierte Domainnamen, Hostnamen oder IP-Adressen (IPv4 oder IPv6) eingeben.
8. Um eine Organisationseinheit auszuwählen, wählen Sie **Use default Computers** aus. Wählen Sie alternativ **Manual** aus und geben Sie einen Organisationseinheitsnamen ein.

   Hinweis

   Das Konto wird in die neue Organisationseinheit verschoben.
9. Klicken Sie auf **Next**.

   Die Seite „Summary“ für die Konfiguration wird angezeigt.
10. Klicken Sie auf **Finish**.

    Das System zeigt die Konfigurationsinformationen in der Authentifizierungsansicht an.
11. Um den Administratorzugriff zu aktivieren, klicken Sie rechts neben **Active Directory Administrative Access** auf **Enable**.

Auswahl des Authentifizierungsmodus

Der ausgewählte Authentifizierungsmodus bestimmt, wie sich CIFS- und NFS-Clients anhand unterstützter Kombinationen von Active Directory, Arbeitsgruppen und Kerberos authentifizieren.

DD OS unterstützt folgende Authentifizierungsoptionen.

- Disabled: Die Kerberos-Authentifizierung ist für CIFS- und NFS-Clients deaktiviert. CIFS-Clients verwenden die Arbeitsgruppenauthentifizierung.

- Windows/Active Directory: Die Kerberos-Authentifizierung ist für CIFS- und NFS-Clients aktiviert. CIFS-Clients verwenden die Active Directory-Authentifizierung.
- Unix: Die Kerberos-Authentifizierung ist für nur für NFS-Clients aktiviert. CIFS-Clients verwenden die Arbeitsgruppenauthentifizierung.

Managen von Administratorgruppen für Active Directory

Im Bereich „Active Directory/Kerberos Authentication“ können Sie Active Directory-Gruppen (Windows) erstellen, ändern und löschen und diesen Gruppen Managementrollen (admin, backup-operator usw.) zuweisen.

Um das Managen von Gruppen vorzubereiten, wählen Sie **Administration** > **Access** > **Authentication** aus, blenden Sie den Bereich „Active Directory/Kerberos Authentication“ ein und klicken Sie neben „Active Directory Administrative Access“ auf die Schaltfläche **Enable**.

Erstellen von Administratorgruppen für Active Directory

Erstellen Sie eine Administratorgruppe, wenn Sie allen in einer Active Directory-Gruppe konfigurierten Benutzern eine Managementrolle zuweisen möchten.

Bevor Sie beginnen

Aktivieren Sie "Active Directory Administrative Access" im Bereich "Active Directory/Kerberos Authentication" auf der Seite **Administration** > **Access** > **Authentication** .

Vorgehensweise

1. Klicken Sie auf **Create...**.
2. Geben Sie den Domainnamen und den Gruppennamen getrennt durch einen umgekehrten Schrägstrich ein. Beispiel: domainname\groupname
3. Wählen Sie aus dem Drop-down-Menü die Managementrolle für die Gruppe aus.
4. Klicken Sie auf **OK**.

Ändern von Administratorgruppen für Active Directory

Ändern Sie eine Administratorgruppe, wenn Sie den Namen der Administratorgruppe oder die für eine Active Directory-Gruppe konfigurierte Managementrolle ändern möchten.

Bevor Sie beginnen

Aktivieren Sie "Active Directory Administrative Access" im Bereich "Active Directory/Kerberos Authentication" auf der Seite **Administration** > **Access** > **Authentication** .

Vorgehensweise

1. Wählen Sie eine zu ändernde Gruppe unter der Überschrift **Active Directory Administrative Access**.
2. Klicken Sie auf **Modify...**.
3. Ändern Sie den Domain- und Gruppennamen. Diese Namen werden durch einen umgekehrten Schrägstrich getrennt. Beispiel: domainname\groupname
4. Ändern Sie die Managementrolle für die Gruppe, indem Sie eine andere Rolle im Drop-down-Menü auswählen.

Löschen von Administratorgruppen für Active Directory

Löschen Sie eine Administratorgruppe, wenn Sie allen in einer Active Directory-Gruppe konfigurierten Benutzern den Systemzugriff entziehen möchten.

Bevor Sie beginnen

Aktivieren Sie "Active Directory Administrative Access" im Bereich "Active Directory/ Kerberos Authentication" auf der Seite **Administration** > **Access** > **Authentication** .

Vorgehensweise

1. Wählen Sie unter der Überschrift **Active Directory Administrative Access** die zu löschende Gruppe aus.
2. Klicken Sie auf **Delete**.

Konfigurieren der UNIX-Kerberos-Authentifizierung

Durch Konfigurieren der UNIX-Kerberos-Authentifizierung können NFS-Clients die Kerberos-Authentifizierung verwenden. CIFS-Clients verwenden die Arbeitsgruppenauthentifizierung.

Bevor Sie beginnen

NIS muss ausgeführt werden, damit die Kerberos-Authentifizierung im UNIX-Modus funktioniert. Anweisungen zum Aktivieren von Kerberos finden Sie im Abschnitt zum Aktivieren von NIS-Services.

Das Konfigurieren von Kerberos für UNIX ermöglicht es NFS-Clients, die Kerberos-Authentifizierung zu verwenden. CIFS-Clients verwenden die Arbeitsgruppenauthentifizierung.

Vorgehensweise

1. Wählen Sie **Administration** > **Access** > **Authentication**.

   Die Authentifizierungsansicht wird angezeigt.

2. Blenden Sie den Bereich „Active Directory/Kerberos Authentication“ ein.
3. Klicken Sie auf **Configure...** neben dem Modus, um den Konfigurationsassistenten zu starten.

   Das Dialogfeld „Active Directory/Kerberos Authentication“ wird angezeigt.
4. Wählen Sie **Unix** aus und klicken Sie auf **Next**.
5. Geben Sie den Namen des Bereichs (z. B. domain1.local) und bis zu drei Hostnamen oder IP-Adressen (IPv4 oder IPv6) für Key Distribution Centers (KDCs) ein.
6. Klicken Sie optional auf **Browse**, um eine Keytab-Datei hochzuladen und klicken Sie auf **Next**.

   Die Seite „Summary“ für die Konfiguration wird angezeigt.

   Hinweis

   Keytab-Dateien werden auf den Authentifizierungsservern (KDCs) erzeugt und enthalten einen gemeinsamen geheimen Schlüssel zwischen dem KDC-Server und dem DDR.

   HINWEIS

   Eine Keytab-Datei muss hochgeladen und importiert werden, damit die Kerberos-Authentifizierung korrekt funktioniert.
7. Klicken Sie auf **Finish**.

Das System zeigt die Konfigurationsinformationen im Bereich „Active Directory/Kerberos Authentication“ an.

Deaktivieren der Kerberos-Authentifizierung

Durch Deaktivieren der Kerberos-Authentifizierung können CIFS- und NFS-Clients die Kerberos-Authentifizierung nicht verwenden. CIFS-Clients verwenden die Arbeitsgruppenauthentifizierung.

Vorgehensweise

1. Wählen Sie **Administration** > **Access Management** > **Authentication**.

   Die Authentifizierungsansicht wird angezeigt.

2. Blenden Sie den Bereich „Active Directory/Kerberos Authentication“ ein.
3. Klicken Sie auf **Configure...** neben dem Modus, um den Konfigurationsassistenten zu starten.

   Das Dialogfeld „Active Directory/Kerberos Authentication“ wird angezeigt.
4. Wählen Sie **Disabled** aus und klicken Sie auf **Next**.

   Es wird eine Seite mit einer Zusammenfassung angezeigt, auf der die Änderungen fett formatiert sind.
5. Klicken Sie auf **Finish**.

   Das System zeigt „Disabled“ neben „Mode“ im Bereich „Active Directory/Kerberos Authentication“ an.

Anzeigen von Informationen zur Arbeitsgruppenauthentifizierung

Über den Bereich „Workgroup Authentication“ können Sie Informationen zur Arbeitsgruppenkonfiguration anzeigen.

Vorgehensweise

1. Wählen Sie**Administration** > **Access** > **Authentication**.
2. Erweitern Sie den Bereich „Workgroup Authentication“.

Tabelle 43 Beschreibungen der Bezeichnungen der Arbeitsgruppenauthentifizierung

Element	Beschreibung
Mode	Der Typ des Authentifizierungsmodus (Arbeitsgruppe oder Active Directory).
Workgroup-Name	Die angegebene Arbeitsgruppe
CIFS Server Name	Name des verwendeten CIFS-Servers
WINS Server	Name des verwendeten WINS-Servers

Konfigurieren von Authentifizierungsparametern für Arbeitsgruppen

Mithilfe von Authentifizierungsparametern für Arbeitsgruppen können Sie einen Arbeitsgruppennamen und einen CIFS-Servernamen konfigurieren.

Vorgehensweise

1. Wählen Sie**Administration** > **Access** > **Authentication**.

   Die Authentifizierungsansicht wird angezeigt.

2. Erweitern Sie den Bereich „Workgroup Authentication“.
3. Klicken Sie auf **Konfigurieren**.

   Das Dialogfeld „Workgroup Authentication“ wird angezeigt.

4. Für den Arbeitsgruppennamen wählen Sie **Manual** und geben einen Arbeitsgruppennamen zum Beitreten ein oder verwenden Sie den Standardnamen.

   Der Arbeitsgruppenmodus verbindet ein Data Domain-System mit einer Arbeitsgruppendomain.

5. Für CIFS-Servernamen wählen Sie **Manual** und geben einen Servernamen (den DDR) ein oder verwenden die Standardeinstellung.
6. Klicken Sie auf **OK**.

Anzeigen von NIS-Authentifizierungsinformationen

Im Bereich „NIS Authentication“ werden die NIS-Konfigurationsparameter sowie Informationen dazu angezeigt, ob die NIS-Authentifizierung aktiviert ist.

Vorgehensweise

1. Wählen Sie**Administration** > **Access** > **Authentication**.

   Die Authentifizierungsansicht wird angezeigt.

2. Erweitern Sie den Bereich „NIS Authentication“.

Ergebnisse

Tabelle 44 Elemente des Bereichs „NIS Authentication“

Element	Beschreibung
NIS Status	„Enabled“ oder „Disabled“.
Domain-Name	Der Name der Domain für diesen Service.
Server	Authentifizierungsserver.
NIS Group	Der Namen der NIS-Gruppe.
Management Role	Die Rolle der Gruppe (admin, user usw.).

Aktivieren und Deaktivieren der NIS-Authentifizierung

Verwenden Sie zum Aktivieren und Deaktivieren der NIS-Authentifizierung den Bereich „NIS Authentication“.

Vorgehensweise

1. Wählen Sie **Maintenance** > **Access** > **Authentication**.

   Die Authentifizierungsansicht wird angezeigt.

2. Erweitern Sie den Bereich „NIS Authentication“.
3. Klicken Sie neben „NIS Status“ auf **Enable** zum Aktivieren oder auf **Disable** zum Deaktivieren der NIS-Authentifizierung.

   Das Dialogfeld „Enable NIS“ oder „Disable NIS“ wird angezeigt.

4. Klicken Sie auf **OK**.

Konfigurieren des NIS-Domainnamens

Verwenden Sie zum Konfigurieren des NIS-Domainnamens den Bereich „NIS Authentication“.

Vorgehensweise

1. Wählen Sie **Administration** > **Access** > **Authentication**.

   Die Authentifizierungsansicht wird angezeigt.

2. Erweitern Sie den Bereich „NIS Authentication“.
3. Klicken Sie neben „Domain Name“ auf **Edit**, um den NIS-Domainnamen zu bearbeiten.

   Das Dialogfeld „Configure NIS Domain Name“ wird angezeigt.

4. Geben Sie den Domainnamen in das Feld **Domain Name** ein.
5. Klicken Sie auf **OK**.

Festlegen von NIS-Authentifizierungsservern

Verwenden Sie den Bereich „NIS Authentication“ zum Angeben von NIS-Authentifizierungsservern.

Vorgehensweise

1. Wählen Sie **Administration** > **Access** > **Authentication**.

   Die Authentifizierungsansicht wird angezeigt.

2. Erweitern Sie den Bereich „NIS Authentication“.
3. Wählen Sie unter „Domain Name“ eine der folgenden Optionen aus:
   - **Obtain NIS Servers from DHCP**: Das System ruft NIS-Server automatisch mithilfe von DHCP ab.
   - **Manually Configure**: Verwenden Sie die folgenden Verfahren, um NIS-Server manuell zu konfigurieren.

   - Um einen Authentifizierungsserver hinzuzufügen, klicken Sie in der Servertabelle auf „Add“ (**+**), geben Sie den Servernamen ein und klicken Sie auf **OK**.
   - Um einen Authentifizierungsserver zu ändern, wählen Sie den Authentifizierungsservernamen aus und klicken Sie auf das Bearbeitungssymbol (Bleistift). Ändern Sie den Servernamen und klicken Sie auf **OK**.
   - Um einen Authentifizierungsservernamen zu entfernen, wählen Sie den Server aus, klicken Sie auf das Symbol „X“ und klicken Sie auf **OK**.
4. Klicken Sie auf **OK**.

Konfigurieren von NIS-Gruppen

Im Bereich „NIS Authentication“ können Sie NIS-Gruppen konfigurieren.

Vorgehensweise

1. Wählen Sie **Administration** > **Access** > **Authentication**.

   Die Authentifizierungsansicht wird angezeigt.

2. Erweitern Sie den Bereich „NIS Authentication“.
3. Konfigurieren Sie die NIS-Gruppen in der Tabelle.
   - Um eine NIS-Gruppe hinzuzufügen, klicken Sie auf „Add“ (**+**), geben Sie den Namen und die Rolle der NIS-Gruppe ein und klicken Sie auf **Validate**. Klicken Sie auf **OK**, um das Dialogfeld zum Hinzufügen einer NIS-Gruppe zu schließen. Klicken Sie erneut auf **OK**, um das Dialogfeld **Configure Allowed NIS Groups** zu schließen.
   - Zum Ändern einer NIS-Gruppe aktivieren Sie das Kontrollkästchen für den NIS-Gruppennamen in der NIS-Gruppenliste und klicken Sie auf die Schaltfläche zum Bearbeiten (Bleistift). Ändern Sie den NIS-Gruppennamen und klicken Sie auf **OK**.
   - Zum Entfernen eines NIS-Gruppennamens wählen Sie die NIS-Gruppe in der Liste aus und klicken Sie auf **X**.
4. Klicken Sie auf **OK**.

Ändern der Systemauthentifizierungsmethode

Das Data Domain-System unterstützt passwortbasierte Authentifizierung oder zertifikatbasierte Authentifizierung. Passwortbasierte Authentifizierung ist die Standardmethode.

Bevor Sie beginnen

Die zertifikatbasierte Authentifizierung erfordert, dass SSH-Schlüssel und CA-Zertifikate importiert werden, um Benutzern die Authentifizierung beim System zu ermöglichen, wenn die passwortbasierte Authentifizierung deaktiviert ist.

Führen Sie die folgenden Schritte aus, um die Systemauthentifizierungsmethode von passwortbasierter Authentifizierung in zertifikatbasierte Authentifizierung zu ändern.

Vorgehensweise

1. Wählen Sie **Administration** > **Access**.

   Die Ansicht „Access Management“ wird angezeigt.
2. Klicken Sie auf **Manage CA Certificates**.
3. Klicken Sie auf **Add**, um ein neues Zertifikat zu erstellen.
4. Fügen Sie das Zertifikat hinzu.
   - Wählen Sie **I want to upload the certificate as a .pem file** und klicken Sie auf **Choose File**, um die Zertifikatdatei auszuwählen und sie in das System hochzuladen.
   - Wählen Sie **I want to copy and paste the certificate text**, um den Zertifikattext zu kopieren und in das Textfeld einzufügen.
5. Klicken Sie auf **Add**.
6. Wählen Sie **More Tasks** > **Change Login Options**.
7. Wählen Sie im Drop-Down-Menü **Password Based Login** die Option **Disable**.

Hinweis

Das Drop-Down-Menü ist deaktiviert, wenn die erforderlichen SSH-Schlüssel und CA-Zertifikate nicht auf dem System konfiguriert sind.

8. Klicken Sie auf **OK**.

   Wenn eine Sicherheits-Policy konfiguriert ist, fordert das System Security Officer-Anmeldedaten an. Geben Sie die Anmeldedaten ein und klicken Sie auf **OK**.

Setzen Sie die Systemauthentifizierungsmethode auf die passwortbasierte Authentifizierung zurück.

Führen Sie die folgenden Schritte aus, um die Systemauthentifizierungsmethode von zertifikatbasierter Authentifizierung in passwortbasierte Authentifizierung zu ändern.

Vorgehensweise

1. Wählen Sie **Administration** > **Access**.

   Die Ansicht „Access Management“ wird angezeigt.

2. Wählen Sie **More Tasks** > **Change Login Options**.
3. Wählen Sie im Drop-Down-Menü **Password Based Login** die Option **Enable**.
4. Klicken Sie auf **OK**.

   Wenn eine Sicherheits-Policy konfiguriert ist, fordert das System Security Officer-Anmeldedaten an. Geben Sie die Anmeldedaten ein und klicken Sie auf **OK**.

Konfigurieren von Mailservereinstellungen

Über die Registerkarte „Mail Server“ können Sie den Mailserver angeben, an den DD OS E-Mail-Berichte senden soll.

Vorgehensweise

1. Wählen Sie **Administration** > **Settings** > **Mail Server**.
2. Wählen Sie **More Tasks** > **Set Mail Server** aus.

   Das Dialogfeld „Set Mail Server“ wird angezeigt.

3. Geben Sie den Namen des Mailservers in das Feld **Mail Server** ein.
4. Klicken Sie auf **OK**.

Managen von Zeit- und Datumseinstellungen

Über die Registerkarte „Time and Date Settings“ können Sie Uhrzeit und Datum des Systems anzeigen und konfigurieren oder festlegen, dass Uhrzeit und Datum vom Network Time Protocol bestimmt werden.

Vorgehensweise

1. Um die aktuelle Uhrzeit- und Datumskonfiguration anzuzeigen, wählen Sie **Administration** > **Settings** > **Time and Date Settings**.

   Auf der Seite „Time and Date“ werden das aktuelle Systemdatum und die Uhrzeit, ob NTP aktiviert ist oder nicht und die IP-Adressen oder Hostnamen der konfigurierten NTP-Server angezeigt.

2. Wählen Sie zum Ändern der Konfiguration **More Tasks** > **Configure Time Settings**.

   Das Dialogfeld „Configure Time Settings“ wird angezeigt.

3. Wählen Sie in der Drop-down-Liste **Time Zone** die Zeitzone aus, in der sich das Data Domain-System befindet.
4. Um das Datum und die Uhrzeit manuell festzulegen, wählen Sie **None** aus, geben Sie das Datum im Feld **Date** ein und legen Sie die Uhrzeit in den Drop-down-Listen **Time** fest.
5. Wenn Sie die Uhrzeit mittels NTP synchronisieren möchten, wählen Sie „NTP“ und legen Sie den Zugriff auf den NTP-Server fest.
   - Um DHCP zum automatischen Auswählen eines Servers zu verwenden, wählen Sie **Obtain NTP Servers using DHCP**.
   - Wählen Sie zum Konfigurieren eine NTP-Server-IP-Adresse **Manually Configure** aus, fügen Sie die IP-Adresse des Servers hinzu und klicken Sie auf **OK**.

   Hinweis

   Die Verwendung der Zeitsynchronisierung von einem Active Directory-Domaincontroller verursacht möglicherweise übermäßige Zeitänderungen auf dem System, wenn NTP und der Domain Controller die Zeit ändern.
6. Klicken Sie auf **OK**.
7. Wenn Sie die Zeitzone geändert haben, müssen Sie das System neu starten.
   a. Wählen Sie **Maintenance** > **System**.
   b. Wählen Sie im Menü "More Tasks" die Option "Reboot System".
   c. Klicken Sie zur Bestätigung auf "OK".

Managen von Systemeigenschaften

Über die Registerkarte „System Properties“ können Sie Systemeigenschaften anzeigen und konfigurieren, mit denen Speicherort, Administrator und Hostname des gemanagten Systems festgelegt werden.

Vorgehensweise

1. Um die aktuelle Konfiguration anzuzeigen, wählen Sie **Administration** > **Settings** > **System Properties**.

   Auf der Registerkarte „System Properties“ werden der Systemstandort, die E-Mail-Adresse des Administrators und der Hostname des Administrators angezeigt.
2. Wählen Sie zum Ändern der Konfiguration **More Tasks** > **Set System Properties**.

   Das Dialogfeld „System Properties“ wird angezeigt.
3. Geben Sie im Feld **Location** Informationen dazu ein, wo sich das Data Domain-System befindet.
4. Geben Sie im Feld **Admin Email** die E-Mail-Adresse des Systemadministrators ein.
5. Geben Sie im Feld **Admin Host** den Namen des Administrationsservers ein.
6. Klicken Sie auf **OK**.

SNMP-Management

Das Simple Network Management Protocol (SNMP) ist ein Standardprotokoll zum Austauschen von Netzwerkmanagementinformationen und Teil der TCP/IP-Protokollsuite (Transmission Control Protocol/Internet Protocol). SNMP stellt ein Tool für Netzwerkadministratoren zum Managen und Monitoring von an das Netzwerk angebundenen Geräten (z. B. Data Domain-Systeme) für Umstände bereit, die die Aufmerksamkeit des Administrators erfordern.

Für das Monitoring von Data Domain-Systemen mit SNMP müssen Sie die Data Domain-MIB in Ihrem SNMP-Managementsystem installieren. DD OS unterstützt außerdem die Standard-MIB-II, sodass Sie auch MIB-II-Statistiken für allgemeine Daten wie Netzwerkstatistiken abfragen können. Für eine vollständige Abdeckung der verfügbaren Daten sollten Sie sowohl die Data Domain-MIB als auch die Standard MIB-II verwenden.

Der SNMP-Agent des Data Domain-Systems akzeptiert Abfragen für Data Domain-spezifische Informationen von Managementsystemen mit SNMP v1, v2c und v3. SNMP V3 bietet ein höheres Maß an Sicherheit als v2C und v1 durch Ersetzen der Communityzeichenfolgen in Klartext (verwendet zur Authentifizierung) durch eine benutzerbasierte Authentifizierung mithilfe von MD5 oder SHA1. Außerdem können SNMP v3-Benutzerauthentifizierungspakete verschlüsselt und ihre Integrität mit DES oder AES überprüft werden.

Data Domain-Systeme können SNMP-Traps (Warnmeldungen) mit SNMP v2c und SNMP v3 senden. Da SNMP v1-Traps nicht unterstützt werden, verwenden Sie SNMP v2c oder v3 (wenn möglich).

Der Standardport, der geöffnet ist, wenn SNMP aktiviert ist, ist Port 161. Traps werden über Port 162 gesendet.

- Im *Data Domain Operating System Initial Configuration Guide* wird beschrieben, wie Sie das Data Domain-System konfigurieren, um das SNMP-Monitoring zu verwenden.
- In der *Data Domain Operating System MIB Quick Reference* werden alle MIB-Parameter beschrieben, die in der Data Domain-MIB-Version enthalten sind.

Anzeigen des SNMP-Status und der SNMP-Konfiguration

Auf der Registerkarte „SNMP“ werden der aktuelle SNMP-Status und die SNMP-Konfiguration angezeigt.

Vorgehensweise

1. Wählen Sie **Administration** > **Settings** > **SNMP**.

   In der SNMP-Ansicht werden der SNMP-Status, SNMP-Eigenschaften, die SNMP V3-Konfiguration und die SNMP V2C-Konfiguration angezeigt.

Bezeichnungen der Registerkarte „SNMP“

Die Bezeichnungen der Registerkarte „SNMP“ geben SNMP-Gesamtstatus, SNMP-Eigenschaftswerte und die Konfigurationen für SNMPv3 und SNMPv2 an.

Status
Im Bereich „Status“ wird der Betriebsstatus des SNMP-Agent auf dem System angezeigt: entweder „Enabled“ oder „Disabled“.

SNMP-Eigenschaften

Tabelle 45 Beschreibung von SNMP-Eigenschaften

Element	Beschreibung
SNMP System Location	Der Speicherort des überwachten Data Domain-Systems
SNMP System Contact	Die Person, die als Ansprechpartner für die Data Domain-Systemadministration angegeben ist
SNMP System Notes	(Optional) Zusätzliche SNMP-Konfigurationsdaten.
SNMP Engine ID	Eine hexadezimale eindeutige Kennung für das Data Domain-System.

SNMP V3-Konfiguration

Tabelle 46 Beschreibung der Spalte „SNMP Users“

Element	Beschreibung
Name	Name des Benutzers auf dem SNMP-Manager mit Zugriff auf den Agent für das Data Domain-System
Access	Zugriffsberechtigungen für den SNMP-Benutzer, die schreibgeschützt oder Lesen/Schreiben sein können
Authentication Protocols	Das Authentifizierungsprotokoll, das für die Überprüfung des SNMP-Benutzers verwendet wird und MD5, SHA1 oder „None“ (kein Protokoll) sein kann
Privacy Protocol	Das während der SNMP-Benutzerauthentifizierung verwendete Verschlüsselungsprotokoll, das AES, DES oder „None“ (kein Protokoll) sein kann

Tabelle 47 Beschreibung der Spalte „Trap Hosts“

Element	Beschreibung
Host	Die IP-Adresse oder der Domainname des SNMP-Managementhosts.
Port	Der für die SNMP-Trap-Kommunikation mit dem Host verwendete Port. 162 ist beispielsweise der Standardwert.
User	Der auf dem Trap-Host dafür authentifizierte Benutzer, auf die Data Domain SNMP-Informationen zuzugreifen.

SNMP V2C-Konfiguration

Tabelle 48 Beschreibung der Spalte „Communities“

Element	Beschreibung
Community	Der Name der Community, beispielsweise public, private oder localCommunity.
Access	Die zugewiesene Zugriffsberechtigung, die schreibgeschützt oder Lesen/Schreiben sein kann

Tabelle 48 Beschreibung der Spalte „Communities“ (Fortsetzung)

Element	Beschreibung
Hosts	Die Hosts in dieser Community.

Tabelle 49 Beschreibung der Spalte „Trap Hosts“

Element	Beschreibung
Host	Die Systeme, die darauf ausgelegt sind, die vom Data Domain-System erzeugten SNMP-Traps zu empfangen. Wenn dieser Parameter festgelegt ist, erhalten Systeme selbst dann Warnmeldungen, wenn der SNMP-Agent deaktiviert ist.
Port	Der für die SNMP-Trap-Kommunikation mit dem Host verwendete Port. 162 ist beispielsweise der Standardwert.
Community	Der Name der Community, beispielsweise public, private oder localCommunity.

Aktivieren und Deaktivieren von SNMP

Verwenden Sie die Registerkarte „SNMP“, um SNMP zu aktivieren oder zu deaktivieren.

Vorgehensweise

1. Wählen Sie **Administration** > **Settings** > **SNMP**.
2. Klicken Sie im Bereich „Status“ auf **Enable** oder **Disable**.

Herunterladen der SNMP-MIB

Verwenden Sie die Registerkarte „SNMP“, um die SNMP-MIB herunterzuladen.

Vorgehensweise

1. Wählen Sie**Administration** > **Settings** > **SNMP**.
2. Klicken Sie auf **Download MIB file**.
3. Wählen Sie im Dialogfeld „Opening DATA_DOMAIN.mib“ **Open** aus.
4. Klicken Sie auf **Browse** und wählen Sie einen Browser aus, um die MIB in einem Browserfenster anzuzeigen.

   Hinweis

   Wenn Sie den Microsoft Internet Explorer-Browser verwenden, aktivieren Sie das automatische Auffordern zum Herunterladen von Dateien.

5. Speichern Sie die MIB oder beenden Sie den Browser.

Konfigurieren von SNMP-Eigenschaften

Auf der Registerkarte „SNMP“ können Sie die Texteinträge für Systemstandort und Systemkontakt konfigurieren.

Vorgehensweise

1. Wählen Sie**Administration** > **Settings** > **SNMP**.
2. Klicken Sie im Bereich „Configure SNMP Properties“ auf**Configure**.

   Das Dialogfeld „SNMP Configuration“ wird angezeigt.

3. Geben Sie in den Textfeldern die folgenden Informationen ein: und/oder
   - SNMP System Location: Eine Beschreibung des Speicherorts des Data Domain-Systems.
   - SNMP System Contact: Die E-Mail-Adresse des Systemadministrators für das Data Domain-System.
   - SNMP System Notes: (Optional) Zusätzliche SNMP-Konfigurationsinformationen.
   - SNMP Engine ID: Eine eindeutige Kennung für die SNMP-Einheit. Die Engine-ID muss 5–34 Hexadezimalzeichen lang sein (nur SNMPv3).

     Hinweis

     Das System zeigt eine Fehlermeldung an, wenn die SNMP-Engine-ID die Längenanforderungen nicht erfüllt oder ungültige Zeichen verwendet.

4. Klicken Sie auf **OK**.

SNMP-V3-Benutzer-Management

Verwenden Sie die Registerkarte „SNMP“, um SNMPv3-Benutzer und -Trap-Hosts zu erstellen, zu ändern und zu löschen.

Erstellen von SNMP-V3-Benutzern

Beim Erstellen von Erstellen von SNMP-V3-Benutzern definieren Sie einen Benutzernamen, legen entweder schreibgeschützten oder Lese-/Schreibzugriff fest und wählen ein Authentifizierungsprotokoll aus.

Vorgehensweise

1. Wählen Sie **Administration** > **Settings** > **SNMP**.
2. Klicken Sie im Bereich „SNMP Users“ auf**Create**.

   Das Dialogfeld „Create SNMP User“ wird angezeigt.

3. Geben Sie im Textfeld **Name** den Namen des Benutzers ein, der Zugriff auf den Agent für das Data Domain-System haben soll. Der Name muss mindestens acht Zeichen lang sein.
4. Wählen Sie entweder schreibgeschützten oder Lese-/Schreibzugriff für diesen Benutzer.
5. Um den Benutzer zu authentifizieren, wählen Sie **Authentication** aus.
   a. Wählen Sie entweder das MD5- oder das SHA1-Protokoll aus.
   b. Geben Sie den Authentifizierungsschlüssel im Textfeld **Key** ein.
   c. Um Verschlüsselung für die Authentifizierungssitzung bereitzustellen, wählen Sie **Privacy**.
   d. Wählen Sie entweder das AES- oder das DES-Protokoll aus.

e. Geben Sie den Chiffrierschlüssel im Textfeld **Key** ein.

6. Klicken Sie auf **OK**.

   Das neu hinzugefügte Benutzerkonto wird in der Tabelle „SNMP Users“ angezeigt.

Ändern von SNMP-V3-Benutzern

Für vorhandene SNMPv3-Benutzer können die Zugriffsebene (Nur Lesezugriff oder Lese-/Schreibzugriff) und das Authentifizierungsprotokoll geändert werden.

Vorgehensweise

1. Wählen Sie**Administration** > **Settings** > **SNMP**.
2. Aktivieren Sie im Bereich **SNMP Users** ein Kontrollkästchen für den Benutzer und klicken Sie auf **Modify**.

   Das Dialogfeld „Modify SNMP User“ wird angezeigt. Sie können alle der folgenden Einstellungen hinzufügen oder ändern.

3. Wählen Sie entweder schreibgeschützten oder Lese-/Schreibzugriff für diesen Benutzer.
4. Um den Benutzer zu authentifizieren, wählen Sie **Authentication** aus.
   a. Wählen Sie entweder das MD5- oder das SHA1-Protokoll aus.
   b. Geben Sie den Authentifizierungsschlüssel im Textfeld "Key" ein.
   c. Um Verschlüsselung für die Authentifizierungssitzung bereitzustellen, wählen Sie **Privacy**.
   d. Wählen Sie entweder das AES- oder das DES-Protokoll aus.
   e. Geben Sie den Chiffrierschlüssel im Textfeld **Key** ein.
5. Klicken Sie auf **OK**.

   Die neuen Einstellungen für dieses Benutzerkonto werden in der Tabelle „SNMP Users“ angezeigt.

Entfernen von SNMP-V3-Benutzern

Verwenden Sie die Registerkarte „SNMP“, um vorhandene SNMP-V3-Benutzer zu löschen.

Vorgehensweise

1. Wählen Sie**Administration** > **Settings** > **SNMP**.
2. Wählen Sie im Bereich „SNMP Users“ ein Kontrollkästchen für den Benutzer aus und klicken Sie auf **Delete**.

   Das Dialogfeld „Delete SNMP User“ wird angezeigt.

   Hinweis

   Wenn die Schaltfläche **Delete** deaktiviert ist, wird der ausgewählte Benutzer von einem oder mehreren Trap-Hosts verwendet. Löschen Sie die Trap-Hosts und anschließend den Benutzer.

3. Überprüfen Sie den zu entfernenden Benutzernamen und klicken Sie auf **OK**.

4. Klicken Sie im Dialogfeld „Delete SNMP User Status“ auf **Close**.

   Das Benutzerkonto wird aus der Tabelle „SNMP Users“ entfernt.

SNMP-V3C-Community-Management

Definieren Sie SNMP-V2C-Communitys (die als Passwörter dienen), um den Zugriff des Managementsystems auf das Data Domain-System zu steuern. Wenn Sie den Zugriff auf bestimmte Hosts begrenzen möchten, die die angegebene Community verwenden, weisen Sie die Hosts der Community zu.

Hinweis

Die Zeichenfolge für SNMP V2c-Communitys wird als Klartext gesendet und kann sehr leicht abgefangen werden. In diesem Fall kann die abfangende Person Informationen von Geräten in Ihrem Netzwerk abrufen, deren Konfiguration ändern und sie möglicherweise herunterfahren. SNMP V3 bietet Authentifizierungs- und Verschlüsselungsfunktionen, um das Abfangen zu verhindern.

Hinweis

Definitionen der SNMP-Community ermöglichen nicht die Übertragung von SNMP-Traps an eine Managementstation. Sie müssen Trap-Hosts definieren, um die Trap-Übertragung an Managementstationen zu ermöglichen.

Erstellen von SNMP-V2C-Communitys

Erstellen Sie Communitys, um den Zugriff auf das DDR-System einzuschränken oder Traps an einen Trap-Host zu senden. Sie müssen eine Community erstellen und einem Host zuweisen, bevor Sie diese Community für die Verwendung mit dem Trap-Host auswählen können.

Vorgehensweise

1. Wählen Sie **Administration** > **Settings** > **SNMP**.
2. Klicken Sie im Bereich „Communities“ auf **Create**.

   Das Dialogfeld „Create SNMP V2C Community“ wird angezeigt.

3. Geben Sie in das Feld **Community** den Namen einer Community ein, der Sie Zugriff auf den Agent auf dem Data Domain-System erteilen möchten.
4. Wählen Sie entweder schreibgeschützten oder Lese-/Schreibzugriff für diese Community aus.
5. Wenn Sie die Community einem oder mehreren Hosts zuordnen möchten, fügen Sie die Hosts wie folgt hinzu:
   a. Klicken Sie auf **+**, um einen Host hinzuzufügen.

      Das Dialogfeld „Host“ wird angezeigt.

   b. Geben Sie im Textfeld **Host** die IP-Adresse oder den Domainnamen des Hosts ein.

   c. Klicken Sie auf **OK**.

      Der Host wird der Hostliste hinzugefügt.
6. Klicken Sie auf **OK**.

Der neue Communityeintrag wird zusammen mit den ausgewählten Hosts in der Tabelle **Communities** angezeigt.

Ändern von SNMP-V2P-Communitys

Vorgehensweise

1. Wählen Sie **Administration** > **Settings** > **SNMP**.
2. Aktivieren Sie im Bereich „Communities“ das Kontrollkästchen für die Community und klicken Sie auf **Modify**.

   Das Dialogfeld „Modify SNMP V2C Community“ wird angezeigt.

3. Zum Ändern des Zugriffsmodus für diese Community wählen Sie **read-only** oder **read-write** aus.

   Hinweis

   Die „Access“-Schaltflächen für die ausgewählte Community sind deaktiviert, wenn ein Trap-Host auf demselben System als Teil dieser Community konfiguriert ist. Wenn Sie die Zugriffseinstellung ändern möchten, löschen Sie den Trap-Host und fügen Sie ihn nach dem Ändern der Community wieder hinzu.

4. Gehen Sie wie folgt vor, um einen oder mehrere Hosts zu dieser Community hinzuzufügen:
   a. Klicken Sie auf **+**, um einen Host hinzuzufügen.

      Das Dialogfeld „Host“ wird angezeigt.

   b. Geben Sie im Textfeld **Host** die IP-Adresse oder den Domainnamen des Hosts ein.
   c. Klicken Sie auf **OK**.

      Der Host wird der Hostliste hinzugefügt.
5. Gehen Sie wie folgt vor, um einen oder mehrere Hosts in der Hostliste zu entfernen:

   Hinweis

   DD System Manager lässt das Löschen eines Hosts nicht zu, wenn ein Trap-Host im selben System als Teil der Community konfiguriert wurde. Um einen Trap-Host in einer Community zu löschen, löschen Sie den Trap-Host und fügen Sie ihn nach dem Ändern der Community wieder hinzu.

   Hinweis

   Die „Access“-Schaltflächen für die ausgewählte Community sind nicht deaktiviert, wenn der Trap-Host eine IPv6-Adresse verwendet und das System von einer früheren DD OS-Version verwaltet wird, die IPv6 nicht unterstützt. Wählen Sie stets ein Managementsystem aus, das dieselbe oder eine neuere DD OS-Version verwendet als die Systeme, die von ihm verwaltet werden (falls möglich).

a. Aktivieren Sie die Kontrollkästchen für alle Hosts oder klicken Sie auf das Kontrollkästchen „Host“ im Tabellenkopf, um alle aufgeführten Hosts auszuwählen.

b. Klicken Sie auf die Schaltfläche zum Löschen (X).

6. Gehen Sie wie folgt vor, um einen Hostnamen zu bearbeiten:

a. Aktivieren Sie das Kontrollkästchen für den Host.

b. Klicken Sie auf die Schaltfläche zum Bearbeiten (Bleistiftsymbol).

c. Bearbeiten Sie den Hostnamen.

d. Klicken Sie auf **OK**.

7. Klicken Sie auf **OK**.

Der geänderte Communityeintrag wird in der Communitytabelle angezeigt.

Löschen von SNMP-V2C-Communitys

Verwenden Sie die Registerkarte „SNMP“, um vorhandene SNMP-V2-Communitys zu löschen.

Vorgehensweise

1. Wählen Sie **Administration** > **Settings** > **SNMP**.
2. Aktivieren Sie im Bereich **Communities** ein Kontrollkästchen für die Community aus und klicken Sie auf **Delete**.

   Das Dialogfeld „Delete SNMP V2C Communities“ wird angezeigt.

   Hinweis

   Wenn die Schaltfläche **Delete** deaktiviert ist, wird die ausgewählte Community von einem oder mehreren Trap-Hosts verwendet. Löschen Sie die Trap-Hosts und anschließend die Community.

3. Überprüfen Sie den zu entfernenden Community-Namen und klicken Sie auf **OK**.
4. Klicken Sie im Dialogfeld „Delete SNMP V2C Communities Status“ auf **Close**. Der Community-Eintrag wird aus der Tabelle „Communities“ gelöscht.

SNMP-Trap-Host-Management

Mit Trap-Host-Definitionen können Data Domain-Systeme Warnmeldungen in SNMP-Trap-Meldungen an eine SNMP-Managementstation senden.

Erstellen von SNMP-V3- und V2C-Trap-Hosts

Trap-Host-Definitionen geben Remotehosts an, die SNMP-Trap-Meldungen vom System empfangen.

Bevor Sie beginnen

Wenn Sie einem Trap-Host eine vorhandene SNMP-V2C-Community zuweisen möchten, müssen Sie den Trap-Host zunächst über den Bereich „Communities“ der Community zuweisen.

Vorgehensweise

1. Wählen Sie **Administration** > **Settings** > **SNMP**.
2. Klicken Sie im Bereich „SNMP V3 Trap Hosts“ oder „SNMP V2C Trap Hosts“ auf **Create**.

   Das Dialogfeld „Create SNMP [V3 oder V2C] Trap Hosts“ wird angezeigt.
3. Geben im Feld **Host** die IP-Adresse oder den Domainnamen des SNMP-Hosts ein, an den Traps gesendet werden sollen.
4. Geben Sie im Feld **Port** die Portnummer für das Senden von Traps ein (Port 162 ist ein gängiger Port).
5. Wählen Sie den Benutzer (SNMP V3) oder die Community (SNMP V2C) aus dem Dropdown-Menü aus.

   Hinweis

   Die Community-Liste zeigt ausschließlich die Communitys an, denen der Trap-Host bereits zugewiesen wurde.
6. Um eine neue Community zu erstellen, führen Sie die folgenden Schritte aus:
   a. Wählen Sie im Kontextmenü „Community“ den Eintrag **Create New Community** aus.
   b. Geben Sie den Namen für die neue Community im Feld **Community** ein.
   c. Wählen Sie den Zugriffstyp aus.
   d. Klicken Sie auf die Schaltfläche „Add“ (+).
   e. Geben Sie den Namen des Trap-Hosts ein.
   f. Klicken Sie auf **OK**.
   g. Klicken Sie auf **OK**.
7. Klicken Sie auf **OK**.

Ändern von SNMP-V3- und V2C-Trap-Hosts

Für vorhandene Trap-Host-Konfigurationen können die Portnummer und die Community-Auswahl geändert werden.

Vorgehensweise

1. Wählen Sie **Administration** > **Settings** > **SNMP**.
2. Wählen Sie im Bereich **SNMP V3 Trap Hosts** oder **SNMP V2C Trap Hosts** einen Trap Host-Eintrag aus und klicken Sie auf **Modify**.

   Das Dialogfeld „Modify SNMP [V3 oder V2C] Trap Hosts“ wird angezeigt.
3. Um die Portnummer zu ändern, geben Sie im Feld **Port** eine neue Portnummer ein (Port 162 wird häufig verwendet).
4. Wählen Sie den Benutzer (SNMP V3) oder die Community (SNMP V2C) aus dem Dropdown-Menü aus.

Hinweis

Die Community-Liste zeigt ausschließlich die Communitys an, denen der Trap-Host bereits zugewiesen wurde.

5. Um eine neue Community zu erstellen, führen Sie die folgenden Schritte aus:
   a. Wählen Sie im Kontextmenü „Community“ den Eintrag **Create New Community** aus.
   b. Geben Sie den Namen für die neue Community im Feld **Community** ein.
   c. Wählen Sie den Zugriffstyp aus.
   d. Klicken Sie auf die Schaltfläche „Add“ (+).
   e. Geben Sie den Namen des Trap-Hosts ein.
   f. Klicken Sie auf **OK**.
   g. Klicken Sie auf **OK**.
6. Klicken Sie auf **OK**.

Entfernen von SNMP-V3- und V2C-Trap-Hosts

Verwenden Sie die Registerkarte „SNMP“, um vorhandene Trap-Host-Konfigurationen zu löschen.

Vorgehensweise

1. Wählen Sie **Administration** > **Settings** > **SNMP**.
2. Aktivieren Sie im Bereich **Trap Hosts** (entweder für V3 oder V2C) das Kontrollkästchen für den Trap-Host und klicken Sie auf **Delete**.

   Das Dialogfeld „Delete SNMP [V3 oder V2C] Trap Hosts“ wird angezeigt.
3. Überprüfen Sie den zu entfernenden Hostnamen und klicken Sie auf **OK**.
4. Klicken Sie im Dialogfeld „Delete SNMP [V3 oder V2C] Trap Hosts“ auf **Close**.

   Der Eintrag für den Trap-Host wird aus der Tabelle **Trap Hosts** gelöscht.

Autosupport-Berichtsmanagement

Die Autosupport-Funktion erzeugt einen Bericht mit der Bezeichnung ASUP. Der ASUP-Bericht enthält Informationen zur Identifizierung des Systems, die zusammengefasste Ausgabe einer Anzahl von Data Domain-Systembefehlen sowie Einträge verschiedener Protokolldateien. Umfassende und detaillierte interne Statistiken und Informationen sind am Ende des Berichts enthalten. Dieser Bericht wurde entwickelt, um den Data Domain-Support beim Debugging von Systemproblemen zu unterstützen.

Ein ASUP-Bericht wird jedes Mal erzeugt, wenn das Dateisystem gestartet wird, also in der Regel einmal am Tag. Das Dateisystem kann jedoch mehrmals am Tag gestartet werden.

Sie können E-Mail-Adressen für den Empfang dieser täglichen ASUP-Berichte konfigurieren und den Versand dieser Berichte an Data Domain aktivieren oder deaktivieren. Für den täglichen Versand des ASUP-Berichts ist standardmäßig 6:00 Uhr festgelegt. Sie können diese Uhrzeit jedoch ändern. Für den Versand von ASUP-Berichten an Data Domain können Sie die alte, unsichere Methode oder die

ConnectEMC-Methode wählen, bei der die Informationen vor der Übertragung verschlüsselt werden.

Management von Autosupport und Supportbündel für HA-System

Die Konfiguration erfolgt auf dem aktiven Node und wird zum Stand-by-Node gespiegelt; daher befindet sich dieselbe Konfiguration auf beiden Nodes, ASUP und Supportbündel sind jedoch nicht konsolidiert.

Autosupport und Supportbündel auf dem aktiven Node umfassen auch Informationen zu Dateisystem, Replikation, Protokoll und HA zusätzlich zu Informationen zum lokalen Node. Autosupport und Supportbündel auf dem Stand-by-Node umfassen nur Informationen zum lokalen Node sowie einige Informationen zu HA (Konfiguration und Status), jedoch keine Informationen zu Dateisystem/Replikation/Protokoll. Autosupports und Supportbündel von beiden Nodes sind erforderlich, um Probleme mit dem HA-Systemstatus zu beheben (Dateisystem, Replikation, Protokolle und HA-Konfiguration).

Aktivieren und Deaktivieren des Autosupport-Reporting an Data Domain

Sie können das Autosupport-Reporting an Data Domain aktivieren oder deaktivieren. Auf das Senden von Warnmeldungen an Data Domain hat dies keine Auswirkungen.

Vorgehensweise

1. Um den Autosupport-Reportingstatus anzuzeigen, wählen Sie **Maintenance** > **Support** > **Autosupport** aus.

   Der Autosupport-Reportingstatus wird neben der Autosupport-Beschriftung „Scheduled“ im Bereich „Support“ hervorgehoben. Abhängig von der aktuellen Konfiguration wird entweder die Schaltfläche **Enable** oder **Disable** in der Autosupport-Zeile „Scheduled“ angezeigt.
2. Um Autosupport-Reporting an Data Domain zu aktivieren, klicken Sie auf **Enable** in der Autosupport-Zeile „Scheduled“.
3. Um Autosupport-Reporting an Data Domain zu deaktivieren, klicken Sie auf **Disable** in der Autosupport-Zeile „Scheduled“.

Überprüfen der erzeugten Autosupport-Berichte

Überprüfen Sie Autosupport-Berichte, um in der Vergangenheit erfasste Systemstatistiken und Konfigurationsinformationen anzuzeigen. Das System speichert maximal 14 Autosupport-Berichte.

Vorgehensweise

1. Wählen Sie **Maintenance** > **Support** > **Autosupport** aus.

   Auf der Seite „Autosupport Reports“ werden der Dateiname und die Dateigröße des Autosupport-Berichts angezeigt sowie das Datum, wann der Bericht erzeugt wurde. Berichte werden automatisch benannt. Der Name des aktuellsten Autosupport-Berichts ist „autosupport“, der Name des Autosupport-Berichts vom Vortag ist „autosupport.1“. Je älter der Bericht ist, desto höher wird die Zahl.

   CLI-Entsprechung

   ```
   # autosupport show history
   ```

2. Klicken Sie auf den Link des Dateinamens, um den Bericht mithilfe eines Texteditors anzuzeigen. Laden Sie die Datei zunächst herunter, wenn dies bei Ihrem Browser erforderlich ist.

Konfigurieren der Autosupport-Mailingliste

Abonnenten der Autosupport-Mailingliste erhalten Autosupport-Meldungen per E-Mail. Verwenden Sie die Registerkarte „Autosupport“, um Abonnenten hinzuzufügen, zu ändern oder zu löschen.

Autosupport-E-Mails werden über den konfigurierten Mailserver an alle Abonnenten in der Autosupport-E-Mail-Liste gesendet. Nachdem Sie den Mailserver und die Autosupport-E-Mail-Liste konfiguriert haben, ist es sinnvoll, die Einrichtung zu testen, um sicherzustellen, dass Autosupport-Meldungen die gewünschten Ziele erreichen.

Vorgehensweise

1. Wählen Sie **Maintenance** > **Support** > **Autosupport** aus.
2. Klicken Sie auf **Konfigurieren**.

   Das Dialogfeld „Configure Autosupport Subscribers“ wird angezeigt.

3. Gehen Sie folgendermaßen vor, um einen Abonnenten hinzuzufügen:
   a. Klicken Sie auf „Add“ (**+**).

      Das Dialogfeld „Email“ wird angezeigt.

   b. Geben Sie die E-Mail-Adresse des Empfängers in das Feld „Email“ ein.

   c. Klicken Sie auf OK.

   CLI-Entsprechung

   ```
    # autosupport add asup-detailed emails djones@company.com # autosupport add alert-summary emails djones@company.com
   ```

4. Um einen Abonnenten zu löschen, gehen Sie folgendermaßen vor.
   a. Wählen Sie im Dialogfeld „Configure Autosupport Subscribers“ den Abonnenten aus, den Sie löschen möchten.

   b. Klicken Sie auf **Delete (X)**.

   CLI-Entsprechung

   ```
    # autosupport del asup-detailed emails djones@company.com # autosupport del alert-summary emails djones@company.com
   ```

5. Um eine Abonnenten-E-Mail-Adresse zu ändern, gehen Sie wie folgt vor.
   a. Wählen Sie im Dialogfeld „Configure Autosupport Subscribers“ den Namen des Abonnenten aus, den Sie bearbeiten möchten.

   b. Klicken Sie auf das Symbol zum Ändern (Bleistiftsymbol).

      Das Dialogfeld „Email“ wird angezeigt.

   c. Ändern Sie die E-Mail-Adresse nach Bedarf.

   d. Klicken Sie auf OK.
6. Klicken Sie auf **OK**, um das Dialogfeld „Configure Autosupport Subscribers“ zu schließen.

Die überarbeitete Autosupport E-Mail-Liste wird im Bereich „Autosupport Mailing List“ angezeigt.

Supportbündelmanagement

Ein Supportbündel ist eine Datei, die Informationen zu Systemkonfiguration und Betrieb enthält. Es wird empfohlen, ein Supportbündel zu erzeugen, bevor Sie ein Softwareupgrade oder eine Änderung an der Systemtopologie (beispielsweise ein Controllerupgrade) durchführen.

Der Data Domain-Support fordert oft ein Supportbündel an, wenn Hilfe bereitgestellt wird.

Erzeugen eines Supportbündels

Beim Troubleshooting von Problemen fragt der Data Domain-Support womöglich nach einem Supportbündel. Dabei handelt es sich um eine als tar.gz-Datei komprimierte Auswahl von Protokolldateien mit einer README-Datei, die ID-Autosupport-Header enthält.

Vorgehensweise

1. Wählen Sie **Maintenance** > **Support** > **Support Bundles** aus.
2. Klicken Sie auf **Generate Support Bundle**.

   Hinweis

   Das System unterstützt maximal fünf Supportbündel. Wenn Sie versuchen, ein sechstes Supportbündel zu erzeugen, löscht das System automatisch das älteste Supportbündel. Sie können Supportbündel auch über die Befehlszeilenoberfläche mit dem Befehl `support bundle delete` löschen.

   Wenn Sie ein Supportbündel auf einem System erzeugen, für das ein Upgrade durchgeführt wurde und das über ein Supportbündel verfügt, das nach dem alten Format, `support-bundle.tar.gz`, benannt ist, wird diese Datei in das neuere Namensformat umbenannt.

3. Senden Sie die Datei per E-Mail zum Customer Service unter support@emc.com.

   Hinweis

   Wenn das Bündel zum Versenden per E-Mail zu groß ist, laden Sie es über die Onlinesupport-Website hoch. (Wechseln Sie zu https://support.emc.com.)

Anzeigen der Liste „Support Bundles“

Verwenden Sie die Registerkarte „Support Bundles“, um die Supportbündeldateien im System anzuzeigen.

Vorgehensweise

1. Wählen Sie **Maintenance** > **Support** > **Support Bundles** aus.

   Die Liste „Support Bundles“ wird angezeigt.

   Es werden der Dateiname und die Dateigröße des Supportbündels aufgelistet sowie das Datum, wann das Bündel erzeugt wurde. Bündel werden automatisch folgendermaßen benannt: *hostname*`-support-bundle-`

datestamp.tar.gz. Ein Beispiel für einen Dateinamen ist localhost-support-bundle-1127103633.tar.gz, was bedeutet, dass das Supportbündel am 27. November um 10:36:33 Uhr auf dem localhost-System erstellt wurde.

2. Klicken Sie auf den Link des Dateinamens und wählen Sie ein gz-/tar-Komprimierungstool aus, um die ASCII-Inhalte des Bündels anzuzeigen.

Coredump-Management

Wenn DD OS aufgrund eines Coredump abstürzt, wird eine Core-Datei mit einer Beschreibung des Problems im Verzeichnis /ddvar/coreerstellt. Diese Datei ist möglicherweise groß und lässt sich schwer aus dem Data Domain-System kopieren.

Wenn die Core-Datei nicht aus dem Data Domain-System kopiert werden kann, da sie zu groß ist, führen Sie den Befehl **support coredump split *<filename>* by *<n>* {MiB|GiB}** aus, wobei:

- *<filename>* der Name der Core-Datei im Verzeichnis /ddvar/core ist.
- *<n>* die Anzahl kleinerer Blöcke ist, um die Core-Datei aufzuteilen.

Hinweis

Eine einzelne Core-Datei kann in maximal 20 Blöcke aufgeteilt werden. Der Befehl schlägt mit einem Fehler fehl, wenn die angegebene Größe zu mehr als 20 Blöcken führen würde.

Das Aufteilen einer 42,1-MB-Core-Datei namebs cpmdb.core.19297.1517443767 in 10-MB-Blöcke würde in 5 Blöcken resultieren.

```
# support coredump split cpmdb.core.19297.1517443767 10 MiB
cpmdb.core.19297.1517443767 will be split into 5 chunks.
Splitting...

The md5 and split chunks of cpmdb.core.19297.1517443767:
File                              Size       Time Created
--------------------------------  --------   ------------------------
cpmdb.core.19297.1517443767_5_01  10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_02  10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_03  10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_04  10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_05  2.1 MiB    Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767.md5   0 MiB      Mon Feb  5 11:50:58 2018
--------------------------------  --------   ------------------------
Download the files as soon as possible. Otherwise they will be automatically delete in 48
hours.
```

Management von Warnmeldungsbenachrichtigungen

Die Warnmeldungsfunktion erzeugt Event- und Zusammenfassungsberichte, die an konfigurierbare E-Mail-Listen und an Data Domain gesendet werden können.

Eventberichte werden sofort gesendet und bieten detaillierte Informationen zu einem Systemevent. Die Verteilerlisten für Eventwarnmeldungen werden als *Benachrichtigungsgruppen* bezeichnet. Sie können eine Benachrichtigungsgruppe konfigurieren, die eine oder mehrere E-Mail-Adressen enthält und Sie können die Typen und den Schweregrad der Eventberichte konfigurieren, die an diese Adressen gesendet werden. Beispielsweise können Sie eine Benachrichtigungsgruppe für Personen konfigurieren, die über kritische Events informiert werden müssen, und eine andere Gruppe für Personen, die weniger kritische Events überwachen. Eine weitere

Möglichkeit besteht darin, Gruppen für verschiedene Technologien zu konfigurieren. Beispielsweise können Sie eine Benachrichtigungsgruppe konfigurieren, um E-Mails über sämtliche Netzwerkevents zu erhalten, und eine andere Gruppe, um Meldungen über Speicherprobleme zu erhalten.

Zusammenfassungsberichte werden täglich gesendet und enthalten eine Zusammenfassung der in den letzten 24 Stunden aufgetretenen Events. Zusammenfassungsberichte enthalten nicht alle Informationen, die in Eventberichten enthalten sind. Die Standarderzeugungszeit für den täglichen Bericht ist 08:00 Uhr und sie kann geändert werden. Zusammenfassungsberichte werden an eine dedizierte E-Mail-Liste gesendet, die von den Eventbenachrichtigungsgruppen getrennt ist.

Sie können das Warnmeldungsreporting an Data Domain aktivieren oder deaktivieren. Wenn Sie Berichte an Data Domain senden, haben Sie die Möglichkeit, die herkömmliche unsichere Methode oder Secure Remote Services für die sichere Übertragung auszuwählen.

Management von Warnmeldungsbenachrichtigungen für HA-System

Die Warnmeldungsfunktion in einem HA-System erzeugt einen Ereignis- und Zusammenfassungsbericht wie ein Nicht-HA-System, aber das Management dieser Warnmeldungen durch das HA-System unterscheidet sich aufgrund der Einrichtung des Systems mit zwei Nodes.

Die Erstkonfiguration von Warnmeldungen wird auf dem aktiven Node durchgeführt und auf den Stand-by-Node gespiegelt (d. h. dieselbe Konfiguration auf beiden Nodes). Lokale und AM-Warnmeldungen werden gemäß den Benachrichtigungseinstellungen per E-Mail versendet und enthalten Informationen, die angeben, dass sie von einem HA-System und von welchem Node sie stammen (aktiver Node oder Stand-by-Node, der die Warnmeldungen erzeugt hat).

Wenn aktive Warnmeldungen zu Dateisystem, Replikation oder Protokollen vorhanden sind, wenn ein Failover erfolgt, werden diese aktiven Warnmeldungen nach dem Failover weiterhin auf dem neuen aktiven Node angezeigt, wenn die Warnmeldungsbedingungen nicht aufgehoben wurden.

Historische Warnmeldungen zu Dateisystem, Replikation und Protokollen werden mit dem Node gespeichert, auf dem sie ausgegeben wurden, und nicht zusammen mit dem Dateisystem bei einem Failover verschoben. Das bedeutet, dass die CLIs auf dem aktiven Node keine komplette/fortlaufende Ansicht historischer Warnmeldungen für Dateisystem, Replikation und Protokolle bereitstellen

Während eines Failover werden lokale historische Warnmeldungen mit dem Node gespeichert, auf dem sie erzeugt wurden; die historischen Warnmeldungen für Dateisystem, Replikation und Protokolle (im Allgemeinen „logische Warnmeldungen“ genannt) werden jedoch bei einem Failover zusammen mit dem Dateisystem verschoben.

Hinweis

Der Bereich **Health** > **High Availability** zeigt nur Warnmeldungen an, die HA-bezogen sind. Diese Warnmeldungen können nach HA-Hauptkomponente gefiltert werden, wie HA Manager, Node, Interconnect, Speicher und SAS-Verbindung.

Anzeigen der Benachrichtigungsgruppenliste

Eine Benachrichtigungsgruppe definiert eine Gruppe von Warnmeldungstypen (Klassen) und eine Gruppe von E-Mail-Adressen (für Abonnenten). Wenn das System

einen in einer Benachrichtigungsliste ausgewählten Warnmeldungstyp generiert, wird diese Warnmeldung an die Listenabonnenten gesendet.

Vorgehensweise

1. Wählen Sie **Health** > **Alerts** > **Notification**.

   CLI-Entsprechung

   ```
   # alerts notify-list show
   ```

2. Um die Einträge in der Liste „Group Name“ zu filtern, geben Sie in das Feld „Group Name“ einen Gruppennamen ein oder geben Sie in das Feld „Alert Email“ eine Abonnenten-E-Mail-Adresse ein. Klicken Sie anschließend auf **Update**.

   Hinweis

   Klicken Sie auf **Reset**, um alle konfigurierten Gruppen anzuzeigen.

3. Um detaillierte Informationen für eine Gruppe anzuzeigen, wählen Sie die Gruppe in der Liste „Group Name“ aus.

Registerkarte „Notification“

Über die Registerkarte „Notification“ können Sie E-Mail-Adressgruppen konfigurieren, die Systemwarnmeldungen für die ausgewählten Warnmeldungstypen und Schweregrade erhalten.

Tabelle 50 Liste „Group Name“, Beschreibung der Spaltenbezeichnungen

Element	Beschreibung
Gruppenname	Der konfigurierte Name für die Gruppe.
Klassen	Die Anzahl der Warnmeldungsklassen, die der Gruppe gemeldet werden.
Abonnenten	Die Anzahl der Abonnenten, die für den Empfang von Benachrichtigungen per E-Mail konfiguriert wurden.

Tabelle 51 Detailed Information, Beschreibung der Bezeichnungen

Element	Beschreibung
Klasse	Ein Service oder ein Subsystem, der bzw. das Warnmeldungen weiterleiten kann. Es werden die Klassen aufgelistet, für die die Benachrichtigungsgruppe Warnmeldungen empfängt.
Severity	Schweregrad, der den Versand einer E-Mail an die Benachrichtigungsgruppe auslöst. Alle Warnmeldungen ab einem bestimmten Schweregrad werden an die Benachrichtigungsgruppe gesendet.
Abonnenten	Im Bereich „Subscribers“ wird eine Liste mit allen für die Benachrichtigungsgruppe konfigurierten E-Mail-Adressen angezeigt.

Tabelle 52 Steuerelemente auf der Registerkarte „Notification“

Steuerelement	Beschreibung
Schaltfläche „Add“	Klicken Sie auf die Schaltfläche **Add**, um mit dem Erstellen einer Benachrichtigungsgruppe zu beginnen.
Bereich „Class Attributes“, Schaltfläche „Configure“	Klicken Sie auf diese Schaltfläche „Configure“, um die Klassen und Schweregrade zu ändern, die Warnmeldungen für die ausgewählte Benachrichtigungsgruppe generieren.
Schaltfläche „Löschen“	Klicken Sie auf die Schaltfläche **Delete**, um die ausgewählte Benachrichtigungsgruppe zu löschen.
Filter By: Feld „Alert Email“	Geben Sie in diesem Feld Text ein, um die Einträge in der Liste mit Gruppennamen auf Gruppen zu begrenzen, die über eine E-Mail-Adresse mit dem eingegebenen Text verfügen.
Filter By: Feld „Group Name“	Geben Sie in diesem Feld Text ein, um die Einträge in der Liste mit Gruppennamen auf Gruppennamen zu begrenzen, die den eingegebenen Text enthalten.
Schaltfläche „Modify“	Klicken Sie auf die Schaltfläche **Modify**, um die Konfiguration für die ausgewählte Benachrichtigungsgruppe zu ändern.
Schaltfläche zum Zurücksetzen	Klicken Sie auf diese Schaltfläche, um Einträge in den Feldern „Filter By“ zu entfernen und alle Gruppennamen anzuzeigen.
Bereich „Subscribers“, Schaltfläche „Configure“	Klicken Sie auf diese Schaltfläche „Configure“, um die Liste mit E-Mail-Adressen für die ausgewählte Benachrichtigungsgruppe zu ändern.
Schaltfläche „Update“	Klicken Sie auf diese Schaltfläche, um die Liste mit Gruppennamen nach der Eingabe von Text in einem Filterfeld zu aktualisieren.

Erstellen einer Benachrichtigungsgruppe

Verwenden Sie die Registerkarte „Notification“, um Benachrichtigungsgruppen hinzuzufügen und den Schweregrad für die einzelnen Gruppen auszuwählen.

Vorgehensweise

1. Wählen Sie **Health** > **Alerts** > **Notification**.
2. Klicken Sie auf **Add**.

   Das Dialogfeld „Add Group“ wird angezeigt.

3. Geben Sie den Namen für die Gruppe in das Feld **Group Name** ein.
4. Aktivieren Sie das Kontrollkästchen für eine oder mehrere Warnmeldungsklassen, über die Sie benachrichtigt werden möchten.
5. Zum Ändern des Standardschweregrads (Warnung) für eine Klasse wählen Sie ein anderes Level im entsprechenden Listenfeld aus.

   Die Schweregrade werden in aufsteigend aufgeführt. *Emergency* ist der höchste Schweregrad.
6. Klicken Sie auf **OK**.

   CLI-Entsprechung

   ```
   # alerts notify-list create eng_grp class hardwareFailure
   ```

Managen der Abonnentenliste für eine Gruppe

Auf der Registerkarte „Notification“ können Sie E-Mail-Adressen in Abonnentenlisten für Benachrichtigungsgruppen hinzufügen, ändern oder löschen.

Vorgehensweise

1. Wählen Sie **Health** > **Alerts** > **Notification**.
2. Aktivieren Sie das Kontrollkästchen einer Gruppe in der Liste der Benachrichtigungsgruppen und führen Sie einen der folgenden Schritte aus.
   - Klicken Sie auf **Modify** und wählen Sie **Subscribers**.
   - Klicken Sie in der Liste „Subscribers“ auf **Configure**.
3. Gehen Sie wie folgt vor, um der Gruppe einen Abonnenten hinzuzufügen.
   a. Klicken Sie auf das Symbol **+**.

      Das Dialogfeld „Email Address“ wird angezeigt.

   b. Geben Sie die E-Mail-Adresse eines Abonnenten ein.

   c. Klicken Sie auf **OK**.

      CLI-Entsprechung

      ```
      # alerts notify-list add eng_lab emails
      mlee@urcompany.com,bob@urcompany.com
      ```
4. Gehen Sie wie folgt vor, um eine E-Mail-Adresse zu ändern.
   a. Klicken Sie auf das Kontrollkästchen der E-Mail-Adresse in der Liste **Subscriber Email**.

   b. Klicken Sie auf das Bleistiftsymbol.

   c. Bearbeiten Sie die E-Mail-Adresse im Dialogfeld „Email Address“.

   d. Klicken Sie auf **OK**.
5. Klicken Sie zum Löschen einer E-Mail-Adresse auf das Kontrollkästchen der E-Mail-Adresse in der Liste **Subscriber Email** und klicken Sie dann auf das Symbol **X**.

   CLI-Entsprechung

   ```
   # alerts notify-list del eng_lab emails bob@urcompany.com
   ```
6. Klicken Sie auf **Finish** oder **OK**.

Ändern einer Benachrichtigungsgruppe

Verwenden Sie die Benachrichtigungstabelle, um die Attributklassen in einer bestehenden Gruppe zu ändern.

Vorgehensweise

1. Wählen Sie **Health** > **Alerts** > **Notification**.
2. Aktivieren Sie in der Gruppenliste das Kontrollkästchen für die Gruppe, die Sie ändern möchten.
3. Um die Klassenattribute für eine Gruppe zu ändern, gehen Sie wie folgt vor.
   a. Klicken Sie im Bereich „Class Attributes“ auf **Configure**.

      Das Dialogfeld "Edit Group" wird angezeigt.

   b. Aktivieren (oder deaktivieren) Sie das Kontrollkästchen für ein oder mehrere Attribute.

   c. Um den Schweregrad für ein Klassenattribut zu ändern, wählen Sie ein Level aus dem entsprechenden Listenfeld aus.

   d. Klicken Sie auf **OK**.

      CLI-Entsprechung

      ```
      # alerts notify-list add eng_lab class cloud severity warning
      # alerts notify-list del eng_lab class cloud severity notice
      ```

4. Um die Abonnentenliste für eine Gruppe zu ändern, gehen Sie wie folgt vor.
   a. Klicken Sie im Bereich „Subscribers“ auf **Configure**.

      Das Dialogfeld „Edit Subscribers“ wird geöffnet.

   b. Um Abonnenten aus der Gruppenliste zu löschen, aktivieren Sie die Kontrollkästchen der zu löschenden Abonnenten und klicken Sie auf das Symbol zum Löschen (X).

   c. Um einen Abonnenten hinzuzufügen, klicken Sie auf das Symbol zum Hinzufügen (+), geben Sie eine Abonnenten-E-Mail-Adresse ein und klicken Sie auf „OK“.

   d. Klicken Sie auf **OK**.

      CLI-Entsprechung

      ```
      # alerts notify-list add eng_lab emails
      mlee@urcompany.com,bob@urcompany.com
      # alerts notify-list del eng_lab emails bob@urcompany.com
      ```

5. Klicken Sie auf **OK**.

Löschen einer Benachrichtigungsgruppe

Verwenden Sie die Registerkarte „Notification“, um eine oder mehrere vorhandene Benachrichtigungsgruppen zu löschen.

Vorgehensweise

1. Wählen Sie **Health** > **Alerts** > **Notification**.
2. Aktivieren Sie ein oder mehrere Kontrollkästchen für Gruppen in der Liste der Benachrichtigungsgruppen aus und klicken Sie auf **Delete**.

Das Dialogfeld „Delete Group“ wird angezeigt.

3. Bestätigen Sie den Löschvorgang und klicken Sie auf **OK**.

   CLI-Entsprechung

   ```
   # alerts notify-list destroy eng_grp
   ```

Zurücksetzen der Benachrichtigungsgruppenkonfiguration

Verwenden Sie die Registerkarte „Notification“, um alle hinzugefügten Benachrichtigungsgruppen zu entfernen und alle an der Standardgruppe vorgenommen Änderungen zurückzusetzen.

Vorgehensweise

1. Wählen Sie **Health** > **Alerts** > **Notification**.
2. Wählen Sie **More Tasks** > **Reset Notification Groups**.
3. Klicken Sie im Dialogfeld „Reset Notification Groups“ im Überprüfungsdialogfeld auf **Yes**.

   CLI-Entsprechung

   ```
   # alerts notify-list reset
   ```

Konfigurieren der täglichen zusammenfassenden Planungs- und Verteilerliste

Jeden Tag sendet jedes gemanagte System den Abonnenten eine tägliche Zusammenfassung der Warnmeldungen per E-Mail, die für die E-Mail-Gruppe alertssummary.list konfiguriert ist. Die E-Mail mit der täglichen Zusammenfassung von Warnmeldungen enthält aktuelle und frühere Warnmeldungen mit Meldungen zu nicht kritischen Hardwaresituationen und Zahlen zur Speicherplatznutzung, für die Sie bald entsprechende Maßnahmen ergreifen sollten.

Ein Lüfterausfall ist ein Beispiel für ein nicht kritisches Problem, das Sie innerhalb angemessener Zeit beheben sollten. Wenn der Support eine Fehlerbenachrichtigung erhält, werden Sie wegen eines Komponentenaustauschs vom Support kontaktiert.

Vorgehensweise

1. Wählen Sie **Health** > **Alerts** > **Daily Alert Summary**.
2. Wenn der Standard für die Bereitstellungszeit von 8 Uhr nicht akzeptabel ist, gehen Sie wie folgt vor.
   a. Klicken Sie auf **Schedule**.

      Das Dialogfeld „Schedule Alert Summary“ wird angezeigt.

   b. Verwenden Sie die Listenfelder, um die Stunde, die Minute und AM oder PM für den zusammenfassenden Bericht auszuwählen.
   c. Klicken Sie auf **OK**.

      CLI-Entsprechung

      ```
      # autosupport set schedule alert-summary daily 1400
      ```

3. Gehen Sie zum Konfigurieren der Abonnentenliste für die tägliche Zusammenfassung wie folgt vor.
   a. Klicken Sie auf **Konfigurieren**.

      Das Dialogfeld „Daily Alert Summary Mailing List“ wird angezeigt.

b. Ändern Sie die Abonnentenliste für die tägliche Zusammenfassung von Warnmeldungen wie folgt.

- Klicken Sie zum Hinzufügen eines Abonnenten auf das **+**-Symbol, geben Sie die E-Mail-Adresse ein und klicken Sie auf **OK**.
  CLI-Entsprechung
  ```
  # autosupport add alert-summary emails djones@company.com
  ```
- Zum Ändern einer E-Mail-Adresse aktivieren Sie das Kontrollkästchen für den Abonnenten, klicken Sie auf das Bleistiftsymbol, bearbeiten Sie die E-Mail-Adresse und klicken Sie auf**OK**.
- Sie können eine E-Mail-Adresse löschen, indem Sie das Kontrollkästchen für den Abonnenten aktivieren und auf **X** klicken.
  CLI-Entsprechung
  ```
  # autosupport del alert-summary emails djones@company.com
  ```

c. Klicken Sie auf **Finish**.

Registerkarte „Daily Alert Summary“

Über die Registerkarte „Daily Alert Summary“ können Sie eine Liste mit E-Mail-Adressen der Personen konfigurieren, die einmal am Tag eine Zusammenfassung aller Systemwarnmeldungen erhalten möchten. Die Personen in dieser Liste erhalten keine einzelnen Warnmeldungen, es sei denn, sie werden auch zu einer Benachrichtigungsgruppe hinzugefügt.

Tabelle 53 Beschreibung der Bezeichnungen auf der Registerkarte „Daily Alert Summary“

Element	Beschreibung
Bereitstellungszeit	Die Bereitstellungszeit gibt die konfigurierte Zeit für tägliche E-Mails an.
E-Mail-Liste	Diese Liste enthält die E-Mail-Adressen der Personen, die die täglichen E-Mails erhalten.

Tabelle 54 Steuerelemente auf der Registerkarte „Daily Alert Summary“

Steuerelement	Beschreibung
Schaltfläche „Configure“	Klicken Sie zum Bearbeiten der Liste „Subscriber Email“ auf die Schaltfläche **Configure**.
Schaltfläche „Schedule“	Klicken Sie zum Konfigurieren der Uhrzeit, zu der der tägliche Bericht gesendet wird, auf die Schaltfläche **Schedule**.

Aktivieren und Deaktivieren der Warnmeldungsbenachrichtigung an Data Domain

Sie können die Warnmeldungsbenachrichtigung an Data Domain aktivieren oder deaktivieren. Auf das Senden von Autosupport-Berichten an Data Domain hat dies keine Auswirkungen.

Vorgehensweise

1. Um den Warnmeldungsreportingstatus anzuzeigen, wählen Sie **Maintenance** > **Support** > **Autosupport** aus.

Der Status der Warnmeldungsbenachrichtigung wird in Grün neben der Bezeichnung „Real-time alert“ im Bereich „Support“ hervorgehoben. Abhängig von der aktuellen Konfiguration wird entweder die Schaltfläche **Enable** oder **Disable** in der Zeile "Real-time alert" angezeigt.

2. Um Warnmeldungsreporting an Data Domain zu aktivieren, klicken Sie auf **Enable** in der Zeile „Real-time alert“.
3. Um Warnmeldungsreporting an Data Domain zu deaktivieren, klicken Sie auf **Disable** in der Zeile „Real-time alert“.

Testen der E-Mail-Funktion für Warnmeldungen

Verwenden Sie die Registerkarte „Notification“, um eine Test-E-Mail an ausgewählte Benachrichtigungsgruppen oder E-Mail-Adressen zu senden. Mit dieser Funktion können Sie feststellen, ob das System ordnungsgemäß konfiguriert ist, um Warnmeldungen zu senden.

Vorgehensweise

1. Gehen Sie folgendermaßen vor, um zu steuern, ob eine Testwarnmeldung an Data Domain gesendet wird:
   a. Wählen Sie **Maintenance** > **Support** > **Autosupport** aus.
   b. Klicken Sie im Bereich **Alert Support** auf **Enable** oder **Disable**, um zu steuern, ob die Test-E-Mail gesendet wird oder nicht.

      Sie können die E-Mail-Adresse nicht ändern.
2. Wählen Sie **Health** > **Alerts** > **Notification**.
3. Wählen Sie **More Tasks** > **Send Test Alert** aus.

   Das Dialogfeld „Send Test Alert“ wird angezeigt.
4. Wählen Sie aus der Liste **Notification Groups** die Gruppen aus, die die Test-E-Mail empfangen sollen, und klicken Sie auf **Next**.
5. Optional können Sie zusätzliche E-Mail-Adressen hinzufügen, an die die E-Mail gesendet werden soll.
6. Klicken Sie auf **Send now** und auf **OK**.

   CLI-Entsprechung

   ```
   # alerts notify-list test jsmith@yourcompany.com
   ```
7. Wenn Sie das Senden der Testwarnmeldung an Data Domain deaktiviert haben und diese Funktion jetzt aktivieren möchten, gehen Sie folgendermaßen vor:
   a. Wählen Sie **Maintenance** > **Support** > **Autosupport** aus.
   b. Klicken Sie im Bereich **Alert Support** auf **Enable**.

Ergebnisse

Um neu hinzugefügte Warnmeldungs-E-Mails auf Mailerprobleme zu testen, geben Sie Folgendes ein: `autosupport test email`*email-addr*.

Nachdem Sie beispielsweise die E-Mail-Adresse djones@yourcompany.com zur Liste hinzugefügt haben, prüfen Sie die Adresse mit dem Befehl: `autosupport test email`*djones@yourcompany.com*.

Support-Zustellungsmanagement

Das Zustellungsmanagement definiert, wie Warnmeldungen und Autosupport-Berichte an Data Domain gesendet werden. Standardmäßig werden Warnmeldungen und Autosupport-Berichte per E-Mail (nicht sicher) an den Data Domain-Kundensupport gesendet. Bei der ConnectEMC-Methode werden Meldungen sicher über das Secure Remote Services Virtual Edition(VE)-Gateway gesendet.

Wenn die ConnectEMC-Methode mit einem Secure Remote Services-Gateway verwendet wird, ist ein Vorteil, dass ein Gateway ausreicht, um Meldungen von mehreren Systemen weiterzuleiten. So müssen Sie die Netzwerksicherheit nur für das Secure Remote Services-Gateway und nicht für mehrere Systeme konfigurieren. Darüber hinaus wird ein Bericht mit Nutzungsinformationen generiert und gesendet, wenn elektronische Lizenzen zum Einsatz kommen.

Wenn Sie ein Secure Remote Services-Gateway konfigurieren, unterstützt das Data Domain-System das Registrieren von mehreren Gateways, um Redundanz zu ermöglichen.

Auswählen der standardmäßigen E-Mail-Zustellung an Data Domain

Wenn Sie die standardmäßige (nicht sichere) E-Mail-Zustellungsmethode wählen, gilt diese Methode für Warnmeldungs- und Autosupportberichte.

Vorgehensweise

1. Wählen Sie **Maintenance** > **Support** > **Autosupport** aus.
2. Klicken Sie auf **Configure** in der Zeile „Channel“ im Bereich „Support“.

   Das Dialogfeld "Configure EMC Support Delivery" wird angezeigt. Die Zustellungsmethode wird nach der Bezeichnung „Channel“ im Bereich „Support“ angezeigt.
3. Wählen Sie im Listenfeld **Channel** die Option **Email to datadomain.com**.
4. Klicken Sie auf **OK**.

   CLI-Entsprechung

   ```
   # support notification method set email
   ```

Auswählen und Konfigurieren der Bereitstellung von Secure Remote Services

Das Secure Remote Services Virtual Edition(VE)-Gateway bietet automatisierte Connect Home- und Remotesupportaktivitäten über eine IP-basierte Lösung, die durch ein umfassendes Sicherheitssystem erweitert wurde.

Ein lokales Gateway mit Secure Remote Services Version 3 bietet die Möglichkeit, Data Domain-Systeme und DD VE-Instanzen und cloudbasierte DD VE-Instanzen zu überwachen.

Vorgehensweise

1. Wählen Sie **Maintenance** > **Support** > **Autosupport** aus.
2. Klicken Sie auf **Configure** in der Zeile „Channel“ im Bereich „Support“.

   Das Dialogfeld „Configure EMC Support Delivery“ wird angezeigt. Die Zustellungsmethode wird nach der Bezeichnung „Channel“ im Bereich „Support“ angezeigt.

3. Wählen Sie im Listenfeld **Channel** die Option **EMC Secure Remote Support Services** aus.
4. Geben Sie den Gatewayhostnamen ein und wählen Sie die lokale IP-Adresse für das Data Domain-System aus.
5. Klicken Sie auf **OK**.
6. Geben Sie den Benutzernamen und das Passwort für den Servicelink ein.
7. Klicken Sie auf **Register**.

   Secure Remote Services-Details werden im Fensterbereich „Autosupport“ angezeigt.

CLI-Entsprechung

```
# support connectemc device register ipaddr esrs-gateway [host-list] [ha-peer ipaddr]
```

Hinweis

Der Parameter `ha-peer` ist bei der Konfiguration von Secure Remote Services für Data Domain-HA-Paare erforderlich, um beide Nodes zu registrieren.

Testen des ConnectEMC-Betriebs

Ein CLI-Befehl ermöglicht es Ihnen, den ConnectEMC-Betrieb zu testen, indem Sie eine Testmeldung an den Support über das Secure Remote Services-Gateway senden.

Vorgehensweise

1. Verwenden Sie zum Testen des ConnectEMC-Betriebs die CLI.

```
#support connectemc test
Sending test message through ConnectEMC...
Test message successfully sent through ConnectEMC.
```

Protokolldateimanagement

Das Data Domain-System unterhält einen Satz Protokolldateien, die gebündelt und an den Support gesendet werden können, damit er Unterstützung beim Troubleshooting von Systemproblemen bietet, die auftreten können. Protokolldateien können nicht von jedem Benutzer mit DD System Manager geändert oder gelöscht werden, aber Sie können sie aus dem Protokollverzeichnis kopieren und außerhalb des Systems managen.

Hinweis

Protokollmeldungen in einem HA-System werden auf dem Node gespeichert, von dem die Protokolldatei stammt.

Protokolldateien werden wöchentlich rotiert. Jeden Sonntag um 0:45 Uhr öffnet das System automatisch neue Protokolldateien für die vorhandenen Protokolle und benennt die vorherigen Dateien mit angehängten Zahlen um. Beispielsweise wird nach der ersten Woche des Betriebs die Datei der vorherigen Woche `messages` in `messages.1` umbenannt und neue Meldungen werden in einer neuen Datei namens „messages“ gespeichert. Jede nummerierte Datei wechselt wöchentlich zur nächsten Zahl. Beispielsweise wird nach der zweiten Woche die Datei `messages.1` zur Datei `messages.2`. Wenn bereits eine Datei `messages.2` vorhanden war, wird diese zu `messages.3`. Nach Ablauf der Aufbewahrungsfrist (siehe die Tabelle unten) wird das

abgelaufene Protokoll gelöscht. Beispielsweise wird eine vorhandene Datei `messages.9` gelöscht, wenn `messages.8` in `messages.9` geändert wird.

Sofern in diesem Thema nicht anders erwähnt, werden die Protokolldateien in `/ddvar/log` gespeichert.

Hinweis

Dateien im Verzeichnis `/ddvar` können mithilfe von Linux-Befehlen gelöscht werden, wenn dem Linux-Benutzer *Schreibberechtigungen* für dieses Verzeichnis zugewiesen wurden.

Der Satz von Protokolldateien auf jedem System wird durch die Funktionen festgelegt, die auf dem System konfiguriert sind, und durch die Events, die auftreten. In der folgenden Tabelle werden die Protokolldateien beschrieben, die das System erzeugen kann:

Tabelle 55 Systemprotokolldateien

Protokolldatei	Beschreibung	Retention Period
audit.log	Meldungen über Benutzeranmeldungsevents	15 Wochen
cifs.log	Protokollmeldungen des CIFS-Subsystems werden nur in `debug/cifs/cifs.log` protokolliert. Die maximale Größe beträgt 50 MiB.	10 Wochen
Meldungen	Meldungen über allgemeine Systemevents, einschließlich der ausgeführten Befehle.	9 Wochen
secure.log	Meldungen zu Benutzerevents wie erfolgreiche und fehlgeschlagene Anmeldungen, Hinzufügen und Löschen von Benutzern sowie Passwortänderungen. Nur Benutzer mit Administratorrolle können diese Datei anzeigen.	9 Wochen
space.log	Meldungen über die Festplattenspeicherplatznutzung durch Systemkomponenten und Meldungen von der Bereinigung. Jede Stunde wird eine Meldung zur Speicherplatznutzung erzeugt. Jedes Mal bei einer Bereinigung werden ca. 100 Meldungen erstellt. Alle Meldungen sind durch Kommas getrennt. Ferner sind Tags vorhanden, mit denen Meldungen zum Festplattenspeicherplatz und zur Bereinigung getrennt werden können. Sie können Software von Drittanbietern verwenden, um jeden dieser Meldungssätze zu analysieren. Die Protokolldatei verwendet die folgenden Tags. • CLEAN für Datenzeilen aus Bereinigungsvorgängen. • CLEAN_HEADER für Zeilen, die Kopfzeilen für die Datenzeilen der Bereinigungsvorgänge enthalten. • SPACE für Datenzeilen zum Speicherplatz. • SPACE_HEADER für Zeilen, die Kopfzeilen für die Datenzeilen zum Speicherplatz enthalten.	Eine einzige Datei wird dauerhaft aufbewahrt. Es gibt keine Protokolldateirotation für dieses Protokoll.

Anzeigen von Protokolldateien in DD System Manager

Auf der Registerkarte „Logs“ können Sie die Systemprotokolldateien in DD System Manager anzeigen und öffnen.

Vorgehensweise

1. Wählen Sie **Maintenance** > **Logs** aus.

   In der Liste „Logs“ werden Dateiprotollnamen sowie die Größe und das Erstellungsdatum für jede Protokolldatei angezeigt.

2. Klicken Sie auf den Namen einer Protokolldatei, um ihren Inhalt anzuzeigen. Sie werden möglicherweise aufgefordert, eine Anwendung wie Notepad.exe auszuwählen, um die Datei zu öffnen.

Anzeigen einer Protokolldatei in der Befehlszeilenoberfläche

Mit dem Befehl `log view` können Sie eine Protokolldatei in der CLI anzeigen.

Vorgehensweise

1. Verwenden Sie den Befehl `log view` , um eine Protokolldatei in der CLI anzuzeigen.

   Ohne Argument zeigt der Befehl die aktuelle Meldungsdatei an.

2. Wenn Sie das Protokoll anzeigen, können Sie mit den Pfeiltasten nach oben und unten durch die Datei blättern, mit der Taste Q beenden und durch Eingeben eines Schrägstrichs (/) und eines Suchmusters die Datei durchsuchen.

Die Anzeige der Meldungsdatei ähnelt der folgenden. Die neueste Meldung im Beispiel ist eine stündliche Systemstatusmeldung, die das Data Domain-System automatisch erzeugt. Die Meldung meldet die Systemverfügbarkeit, die Menge der gespeicherten Daten, NFS-Vorgänge und die Menge des Speicherplatzes, der für das Speichern von Daten verwendet wird (%). Die stündlichen Meldungen werden im Systemprotokoll und auf der seriellen Konsole abgelegt, wenn eine verbunden ist.

```
# log view
Jun 27 12:11:33 localhost rpc.mountd: authenticated unmount
request from perfsun-g.emc.com:668 for /ddr/col1/segfs (/ddr/
col1/segfs)

Jun 27 12:28:54 localhost sshd(pam_unix)[998]: session opened
for user jsmith10 by (uid=0)

Jun 27 13:00:00 localhost logger: at 1:00pm up 3 days, 3:42,
52324 NFS ops, 84763 GiB data col. (1%)
```

Hinweis

GiB = Gibibyte = die binäre Entsprechung von Gigabyte.

Informationen über Protokollmeldungen

Schlagen Sie Fehlermeldungen im Fehlermeldungskatalog für Ihre DD OS-Version nach.

In der Protokolldatei befindet sich Text, der dem Folgenden ähnelt.

```
Jan 31 10:28:11 syrah19 bootbin: HINWEIS: MSG-SMTOOL-00006: No
replication throttle schedules found: setting throttle to
unlimited.
```

Die Komponenten der Meldung sind:

```
DateTime Host Process [PID]: Severity: MSG-Module-MessageID: Message
```

Schweregrade, in absteigender Reihenfolge, nämlich: Notfall, Warnmeldung, kritisch, Fehler, Warnung, Hinweis, Informationen, Debug.

Vorgehensweise

1. Rufen Sie die Onlinesupport-Website unter https://support.emc.com auf, geben Sie im Suchfeld *Fehlermeldungskatalog* ein und klicken Sie auf die Schaltfläche zum Suchen.
2. Suchen Sie in der Ergebnisliste den Katalog für Ihr System und klicken Sie auf den Link.
3. Suchen Sie mit der Suchfunktion Ihres Browsers nach einer eindeutigen Textzeichenfolge in der Meldung.

   Die Fehlermeldungsbeschreibung sieht der folgenden Anzeige ähnlich.

   ```
   ID: MSG-SMTOOL-00006 - Severity: NOTICE - Audience:
   customerMessage: No replication throttle schedules found:
   setting throttle to unlimited.

   Description: The restorer cannot find a replication
   throttle schedule. Replication is running with throttle
   set to unlimited.

   Action: To set a replication throttle schedule, run the
   replication throttle add command.
   ```

4. Um ein Problem zu beheben, führen Sie die empfohlene Aktion aus.

   Basierend auf der Beispielmeldungsbeschreibung können Sie den Befehl `replication throttle add` ausführen, um die Drosselung festzulegen.

Speichern einer Kopie von Protokolldateien

Speichern Sie Protokolldateikopien auf einem anderen Gerät, wenn Sie diese Dateien archivieren möchten.

Verwenden Sie NFS-, CIFS-Mount oder FTP, um die Dateien auf einen anderen Rechner zu kopieren. Wenn Sie CIFS- oder NFS verwenden, mounten Sie /ddvar auf Ihren Desktop und kopieren die Dateien aus dem Mount-Punkt. Im folgenden Verfahren wird beschrieben, wie Sie FTP verwenden, um Dateien auf einen anderen Rechner zu verschieben.

Vorgehensweise

1. Verwenden Sie im Data Domain-System den Befehl `adminaccess show ftp` , um zu sehen, ob der FTP-Service aktiviert ist. Wenn der Service deaktiviert ist, verwenden Sie den Befehl `adminaccess enable ftp`.
2. Verwenden Sie auf dem Data Domain-System den Befehl `adminaccess show ftp` , um festzustellen, ob die FTP-Zugriffsliste die IP-Adresse des Remotecomputers enthält. Wenn die Adresse nicht in der Liste enthalten ist, verwenden Sie den Befehl `adminaccess add ftp` *ipaddr*.

3. Öffnen Sie auf dem Remoterechner einen Webbrowser.
4. Verwenden Sie im Feld **Address** am oberen Rand des Webbrowsers FTP, um auf das Data Domain-System zuzugreifen, wie im folgenden Beispiel gezeigt.

   ```
   ftp://Data Domain system_name.yourcompany.com/
   ```

   Hinweis

   Einige Webbrowser fordern nicht automatisch eine Anmeldung an, wenn ein Rechner keine anonymen Anmeldungen akzeptiert. In diesem Fall fügen Sie einen Benutzernamen und ein Passwort in der FTP-Zeile hinzu. Beispiel: `ftp://sysadmin:your-pw@Data Domain system_name.yourcompany.com/`

5. Im Pop-up-Fenster für die Anmeldung melden Sie sich beim Data Domain-System als Benutzer `sysadmin` an.
6. Im Data Domain-System befinden Sie sich im Verzeichnis genau über dem Protokollverzeichnis. Öffnen Sie das Protokollverzeichnis, um die Meldungsdateien aufzulisten.
7. Kopieren Sie die zu speichernde Datei. Klicken Sie mit der rechten Maustaste auf das Dateisymbol und wählen Sie im Menü **Copy to Folder** aus. Wählen Sie einen Speicherort für die Dateikopie aus.
8. Wenn Sie den FTP-Service auf dem Data Domain-System nach Abschluss des Kopiervorgangs deaktivieren möchten, verwenden Sie SSH für die Anmeldung beim Data Domain-System als Systemadministrator und führen Sie den Befehl `adminaccess disable ftp` aus.

Übertragung von Protokollmeldungen an Remotesysteme

Einige Protokollmeldungen können vom Data Domain-System an andere Systeme gesendet werden. Die Bekanntmachung von Protokollmeldungen an Remotesysteme erfolgt bei DD OS über Syslog.

Ein Data Domain-System exportiert die folgenden Standort-/Prioritätsselektoren für Protokolldateien. Informationen zum Managen der Selektoren und zum Empfangen von Meldungen eines Drittanbietersystems finden Sie in der vom Anbieter des Empfangssystems bereitgestellten Dokumentation.

- *.notice – Sendet alle Meldungen mit der Stufe „Notice“ und höher.
- *.alert – Sendet alle Meldungen mit der Stufe „Alert“ und höher („Alerts“ sind in *.notice inbegriffen).
- kern.* – Sendet alle Kernel-Meldungen (kern.info-Protokolldateien).

Die Befehle `log host` managen den Prozess zum Senden von Protokollmeldungen an andere Systeme:

Anzeigen der Konfiguration für die Übertragung der Protokolldatei

Verwenden Sie den CLI-Befehl `log host show`, um anzuzeigen, ob die Übertragung von Protokolldateien aktiviert ist und welche Hosts Protokolldateien empfangen.

Vorgehensweise

1. Geben Sie zum Anzeigen der Konfiguration den Befehl `log host show` ein.

```
# log host show
Remote logging is enabled.
```

```
Remote logging hosts
     log-server
```

Aktivieren oder Deaktivieren der Übertragung von Protokollmeldungen

Zum Aktivieren oder Deaktivieren der Übertragung von Protokollmeldungen müssen Sie CLI-Befehle verwenden.

Vorgehensweise

1. Um den Versand von Protokollmeldungen an andere Systeme zu aktivieren, verwenden Sie den Befehl `log host enable`.
2. Um den Versand von Protokollmeldungen an andere Systeme zu deaktivieren, verwenden Sie den Befehl `log host disable`.

Hinzufügen oder Entfernen eines Empfängerhosts

Zum Hinzufügen oder Entfernen eines Empfängerhosts müssen Sie CLI-Befehle verwenden.

Vorgehensweise

1. Verwenden Sie den Befehl `log host add`, um ein System zu der Liste hinzufügen, die Data Domain-Systemprotokollmeldungen erhält.
2. Um ein System aus der Liste zu entfernen, die Data Domain-Systemprotokollmeldungen erhält, verwenden Sie den folgenden Befehl: `log host del`.

Mit dem folgenden Befehl wird das System namens *log-server* zu den Hosts hinzugefügt, die Protokollmeldungen erhalten.

```
log host add log-server
```

Mit dem folgenden Befehl wird das System namens *log-server* von den Hosts entfernt, die Protokollmeldungen erhalten.

```
log host del log-server
```

Mit dem folgenden Befehl wird das Senden von Protokollen deaktiviert und die Liste der Zielhostnamen gelöscht.

```
log host reset
```

Energiemanagement des Remotesystems mit IPMI

Wählen Sie DD-Systeme aus, die das Energiemanagement mithilfe der Intelligent Platform Management Interface (IPMI) unterstützen und auch das Remotemonitoring der Startsequenz mithilfe von Serial over LAN (SOL) unterstützen.

Das IPMI-Energiemanagement erfolgt zwischen einem IPMI-Initiator und einem IPMI-Remotehost. Der IPMI-Initiator ist der Host, der die Stromversorgung auf dem Remotehost steuert. Zur Unterstützung des Remote-Energiemanagements von einem Initiator muss der Remotehost mit einem IPMI-Benutzernamen und Passwort konfiguriert werden. Der Initiator muss diesen Benutzernamen und das Passwort bereitstellen, wenn er versucht, die Stromversorgung auf einem Remotehost zu managen.

IPMI wird unabhängig von DD OS ausgeführt und ermöglicht es einem IPMI-Benutzer, die Systemstromversorgung zu managen, solange das Remotesystem mit einer

Stromquelle und einem Netzwerk verbunden ist. Eine IP-Netzwerkverbindung ist zwischen einem Initiator und einem Remotesystem erforderlich. Wenn das IPMI-Management ordnungsgemäß konfiguriert und verbunden ist, ist Ihre physische Anwesenheit zum Ein- oder Ausschalten eines Remotesystems nicht mehr erforderlich.

Mit DD System Manager und der CLI können Sie IPMI-Benutzer auf einem Remotesystem konfigurieren. Nachdem Sie IPMI auf einem Remotesystem konfiguriert haben, können Sie die IPMI-Initiator-Funktionen auf einem anderen System verwenden, um sich anzumelden und die Stromversorgung zu managen.

Hinweis

Wenn ein System aufgrund von hardware- oder softwarebedingten Beschränkungen IPMI nicht unterstützen kann, zeigt DD System Manager eine Benachrichtigung an, wenn versucht wird, zu einer Konfigurationsseite zu navigieren.

SOL wird verwendet, um die Startsequenz nach einem Aus- und erneuten Einschalten auf einem Remotesystem anzuzeigen. SOL ermöglicht, dass Textkonsolendaten, die normalerweise zu einem seriellen Port oder einer direkt angeschlossenen Konsole angezeigt würden, über ein LAN gesendet und von einem Managementhost angezeigt werden.

Auf der DD OS-CLI können Sie ein Remotesystem für SOL konfigurieren und die Remotekonsolenausgabe anzeigen. Diese Funktion wird nur von der CLI unterstützt.

HINWEIS

Die IPMI-Stromabschaltung wird für Notfallsituationen zur Verfügung gestellt, in denen Versuche, das System mithilfe der DD OS-Befehle auszuschalten, fehlschlagen. Bei der IPMI-Stromabschaltung wird einfach die Stromversorgung zum System unterbrochen, das DD OS-Dateisystem wird nicht ordnungsgemäß heruntergefahren. Die korrekte Methode, die Stromversorgung zu unterbrechen und wieder herzustellen, ist die Verwendung des DD OS-Befehls `system reboot`. Die korrekte Methode, die Systemstromversorgung zu unterbrechen, ist die Verwendung des DD OS-Befehls `system poweroff` und darauf zu warten, dass mit dem Befehl das Dateisystem ordnungsgemäß heruntergefahren wird.

IPMI- und SOL-Einschränkungen

Die IPMI- und SOL-Unterstützung ist auf einigen Data Domain-Systemen eingeschränkt.

- IPMI wird auf allen Systemen unterstützt, die von dieser Version unterstützt werden, mit Ausnahme der folgenden Systeme: DD140, DD610 und DD630.
- Die IPMI-Benutzerunterstützung unterscheidet sich wie folgt.
  - Modell DD990: Maximale Benutzer-IDs = 15. Drei Standardbenutzer (NULL, anonymous, root). Maximal verfügbare Benutzer-IDs = 12.
  - Modelle DD640, DD4200, DD4500, DD7200 und DD9500: Maximale Benutzer-IDs = 10. Zwei Standardbenutzer (NULL, root). Maximal verfügbare Benutzer-IDs = 8.
- SOL wird auf den folgenden Systemen unterstützt: DD160, DD620, DD640, DD670, DD860, DD890, DD990, DD2200, DD2500 (erfordert DD OS 5.4.0.6 oder höher), DD4200, DD4500, DD7200 und DD9500.

Hinweis

Der Benutzer „root“ wird für IPMI-Verbindungen auf DD160-Systemen nicht unterstützt.

Hinzufügen und Löschen von IPMI-Benutzern mit DD System Manager

Jedes System enthält eine eigene Liste der konfigurierten IPMI-Benutzer, die zur Kontrolle des Zugriffs auf lokale Energiemanagementfunktionen verwendet wird. Ein anderes System, das als IPMI-Initiator agiert, kann die Stromversorgung für das Remotesystem nur managen, nachdem ein gültiger Benutzername und ein Passwort bereitgestellt wurden.

Um einem IPMI-Benutzer die Berechtigung zum Management der Stromversorgung auf mehreren Remotesystemen zu erteilen, müssen Sie diesen Benutzer zu jedem der Remotesysteme hinzufügen.

Hinweis

Die IPMI-Benutzerlisten der einzelnen Remotesysteme unterscheiden sich von den DD System Manager-Listen für Administratorzugriff und lokale Benutzer. Administratoren und lokale Benutzer erben keine Autorisierung für das IPMI-Energiemanagement.

Vorgehensweise

1. Wählen Sie **Maintenance** > **IPMI** aus.
2. Führen Sie zum Hinzufügen eines Benutzers die folgenden Schritte aus.
   a. Klicken Sie über der Tabelle „IPMI Users“ auf **Add**.
   b. Geben Sie im Dialogfeld „Add User“ den Benutzernamen (höchstens 16 Zeichen) und das Passwort in die entsprechenden Felder ein. (Geben Sie das Passwort erneut in das Feld **Verify Password** ein.)
   c. Klicken Sie auf **Create**.

      Der Benutzereintrag wird in der Tabelle **IPMI Users** angezeigt.
3. Führen Sie zum Löschen eines Benutzers die folgenden Schritte aus.
   a. Wählen Sie in der Liste der IPMI-Benutzer einen Benutzer aus und klicken Sie auf **Delete**.
   b. Klicken Sie im Dialogfeld „Delete User“ auf **OK**, um das Löschen des Benutzers zu bestätigen.

Ändern des Passworts eines IPMI-Benutzers

Ändern Sie das Passwort des IPMI-Benutzers, um eine Verwendung des alten Passworts für das Energiemanagement zu vermeiden.

Vorgehensweise

1. Wählen Sie **Maintenance** > **IPMI** aus.
2. Wählen Sie in der Tabelle der IPMI-Benutzer einen Benutzer aus und klicken Sie auf **Change Password**.
3. Geben Sie das Passwort im Dialogfeld „Change Password“ in das entsprechende Textfeld und erneut in das Feld **Verify Password** ein.
4. Klicken Sie auf **Update**.

Konfigurieren eines IPMI-Ports

Wenn Sie einen IPMI-Port für ein System konfigurieren, wählen Sie den Port aus einer Liste mit Netzwerkports aus und geben die IP-Konfigurationsparameter für diesen Port ein. Die Auswahl der angezeigten IPMI-Ports wird durch das Data Domain-Systemmodell bestimmt.

Einige Systeme unterstützen einen oder mehrere dedizierte Ports, die nur für IPMI-Datenverkehr verwendet werden können. Andere Systeme unterstützen Ports, die für IPMI-Datenverkehr sowie den gesamten IP-Datenverkehr verwendet werden können, der von den physischen Schnittstellen in der Ansicht **Hardware** > **Ethernet** > **Interfaces** unterstützt wird. Gemeinsam genutzte Ports werden auf Systemen mit dedizierten IPMI-Ports nicht bereitgestellt.

Die Portnamen in der Liste der IPMI-Netzwerkports verwenden das Präfix „bmc“, das für „Baseboard Management Controller“ steht. Um zu ermitteln, ob ein Port ein dedizierter Port oder ein gemeinsam genutzter Port ist, vergleichen Sie den Rest des Portnamens mit den Ports in der Liste der Netzwerkschnittstellen. Wenn der Rest des IPMI-Portnamens mit einer Schnittstelle in der Liste der Netzwerkschnittstellen übereinstimmt, ist der Port ein gemeinsam genutzter Port. Wenn der Rest des IPMI-Portnamens nicht mit einer Schnittstelle in der Liste der Netzwerkschnittstellen übereinstimmt, ist der Port ein dedizierter IPMI-Port.

Hinweis

Eine Ausnahme der zuvor beschriebenen Benennungsregeln bilden die Systeme DD4200, DD4500 und DD7200. Auf diesen Systemen entspricht der IPMI-Port „bmc0a“ dem gemeinsam genutzten Port „ethMa“ in der Liste der Netzwerkschnittstellen. Reservieren Sie, wenn möglich, den gemeinsam genutzten Port „ethMa“ für IPMI-Datenverkehr und den Managementdatenverkehr des Systems (mithilfe von Protokollen wie HTTP, Telnet und SSH). Backupdatenverkehr sollte an andere Ports weitergeleitet werden.

Wenn IPMI- und Nicht-IPMI-IP-Datenverkehr gemeinsam einen Ethernetport nutzen, verwenden Sie die Funktion der Linkzusammenfassung auf der freigegebenen Schnittstelle nicht (wenn möglich), da sich Änderungen des Linkstatus auf die IPMI-Konnektivität auswirken können.

Vorgehensweise

1. Wählen Sie **Maintenance** > **IPMI** aus.

   Im Bereich „IPMI Configuration“ wird die IPMI-Konfiguration für das verwaltete System angezeigt. In der Tabelle „Network Ports“ werden die Ports aufgelistet, auf denen IPMI aktiviert und konfiguriert werden kann. In der Tabelle „IPMI Users“ werden die IPMI-Benutzer aufgelistet, die auf das verwaltete System zugreifen können.

   Tabelle 56 Spaltenbeschreibungen der Liste „Network Ports“

Element	Beschreibung
Port	Der logische Name für einen Port, der IPMI-Kommunikationen unterstützt.
Aktiviert	Gibt an, ob der Port für IPMI aktiviert ist („Yes“ oder „No“).

Tabelle 56 Spaltenbeschreibungen der Liste „Network Ports“ (Fortsetzung)

Element	Beschreibung
DHCP	Gibt an, ob der Port DHCP verwendet, um seine IP-Adresse festzulegen („Yes“ oder „No“).
MAC-Adresse	Die Hardwareadresse (MAC-Adresse) für den Port.
IP-Adresse	Die IP-Adresse des Ports.
Netzmaske	Die Subnetzmaske für den Port.
Gateway	Die Gateway-IP-Adresse für den Port.

Tabelle 57 Spaltenbeschreibungen der Liste „IPMI Users“

Element	Beschreibung
Benutzername	Der Name eines Benutzers, der zur Verwaltung der Stromversorgung des Remotesystems berechtigt ist.

2. Wählen Sie in der Tabelle **Network Ports** den Port aus, den Sie konfigurieren möchten.

   Hinweis

   Wenn der IPMI-Port auch IP-Datenverkehr (für Administratorzugriff oder Backupdatenverkehr) unterstützt, muss der Schnittstellenport aktiviert werden, bevor Sie IPMI konfigurieren.

3. Klicken Sie über der Tabelle **Network Ports** auf **Configure**.

   Das Dialogfeld „Configure Port“ wird angezeigt.

4. Wählen Sie aus, wie Informationen zur Netzwerkadresse zugewiesen werden.
   - Um die IP-Adresse, Netzmaske und Gatewaykonfiguration von einem DHCP-Server zu erfassen, wählen Sie **Dynamic (DHCP)** aus.
   - Um die Netzwerkkonfiguration zu definieren, wählen Sie **Static (Manual)** aus und geben Sie die IP-Adresse, die Netzmaske und die Gatewayadresse ein.

5. Um einen deaktivierten IPMI-Netzwerkport zu aktivieren, wählen Sie den Netzwerkport in der Tabelle **Network Ports** aus und klicken Sie auf **Enable**.
6. Um einen aktivierten IPMI-Netzwerkport zu deaktivieren, wählen Sie den Netzwerkport in der Tabelle **Network Ports** aus und klicken Sie auf **Disable**.
7. Klicken Sie auf **Anwenden**.

Vorbereitungen für das Remoteenergiemanagement und das -konsolenmonitoring mit der Befehlszeilenoberfläche

Beim Remotekonsolenmonitoring wird die SOL-Funktion (Serial over Lan) verwendet, um das Anzeigen der textbasierten Konsolenausgabe ohne seriellen Server zu ermöglichen. Die Einrichtung eines Systems für das Remoteenergiemanagement und das Remotekonsolenmonitoring ist nur über die Befehlszeilenoberfläche möglich.

Das Remotekonsolenmonitoring wird normalerweise in Kombination mit dem Befehl `ipmi remote power cycle` verwendet, um die Startsequenz des Remotesystems

anzuzeigen. Dieses Verfahren sollte auf jedem System verwendet werden, für das Sie möglicherweise die Konsole während der Startsequenz remote anzeigen möchten.

Vorgehensweise

1. Verbinden Sie die Konsole direkt oder remote mit dem System.
   - Verwenden Sie die folgenden Anschlüsse für eine direkte Verbindung.
     - DIN-Ports für PS/2-Tastatur
     - Port mit USB-A-Buchse für eine USB-Tastatur
     - DB15-Buchse für einen VGA-Monitor

     Hinweis

     Die Systeme DD4200, DD4500 und DD7200 unterstützen keine direkte Verbindung, einschließlich KVM.

   - Verwenden Sie für eine serielle Verbindung einen Standard-DB9-Stecker oder eine Micro-DB9-Buchse. Die Systeme DD4200, DD4500 und DD7200 bieten eine Micro-DB9-Buchse. Für eine typische Laptopverbindung ist ein Nullmodemkabel mit Mikro-DB-9-Buchse und standardmäßiger DB-9-Buchse enthalten.
   - Für eine Remote-IPMI-/SOL-Verbindung verwenden Sie den entsprechenden RJ45-Anschluss wie folgt.
     - Für DD990-Systeme verwenden Sie den Standardport eth0d.
     - Für andere Systeme verwenden Sie den Wartungs- oder Serviceport. Informationen zu den Portstandorten finden Sie in der Systemdokumentation, beispielsweise im Hardwareüberblick oder dem Installations- und Konfigurationshandbuch.
2. Verwenden Sie die BIOS-Einstellungen, um das Remotekonsolenmonitoring zu unterstützen.
3. Geben Sie zum Anzeigen des IPMI-Portnamens `ipmi show config` ein.
4. Geben Sie zum Aktivieren von IPMI `ipmi enable {`*`port`* `| all}` ein.
5. Um den IPMI-Port zu konfigurieren, geben Sie `ipmi config port { dhcp | ipaddress` *`ipaddr`* `netmask` *`mask`* `gateway` *`ipaddr`* `}` ein.

   Hinweis

   Wenn der IPMI-Port auch IP-Datenverkehr (für Administratorzugriff oder Backupdatenverkehr) unterstützt, muss der Schnittstellenport mit dem Befehl`net enable` aktiviert werden, bevor Sie IPMI konfigurieren.

6. Wenn dies die erste Verwendung von IPMI ist, führen Sie `ipmi user reset` aus, um IPMI-Benutzer zu löschen, die möglicherweise nicht über eine Synchronisierung zwischen zwei Ports verfügen, und um Standardbenutzer zu deaktivieren.
7. Geben Sie zum Hinzufügen eines neuen IPMI-Benutzers `ipmi user add`*`user`* ein.
8. Gehen Sie wie folgt vor, um SOL zu konfigurieren:
   a. Geben Sie `system option set console lan` ein.

b. Geben Sie nach Aufforderung `y`, um das System neu zu starten.

Managen der Stromversorgung mit DD System Manager

Nachdem IPMI korrekt auf einem Remotesystem konfiguriert ist, können Sie DD System Manager als IPMI-Initiator verwenden, um sich bei dem Remotesystem anzumelden und den Stromversorgungsstatus anzuzeigen und zu ändern.

Vorgehensweise

1. Wählen Sie **Maintenance** > **IPMI** aus.
2. Klicken Sie auf **Login to Remote System**.

   Das Dialogfeld „IPMI Power Management“ wird angezeigt.

3. Geben Sie die IP-Adresse oder den Hostnamen (IPMI) für das Remotesystem und den Benutzernamen und das Passwort für IPMI ein und klicken Sie dann auf **Connect**.
4. Zeigen Sie den IPMI-Status an.

   Das Dialogfeld „IPMI Power Management“ wird angezeigt. Darin werden die Zielsystemidentifizierung und der aktuelle Stromversorgungsstatus angezeigt. Im Statusbereich wird immer der aktuelle Status angezeigt.

   Hinweis

   Das Symbol zum Aktualisieren (blaue Pfeile) neben dem Status kann verwendet werden, um den Konfigurationsstatus zu aktualisieren (z. B. wenn die IPMI-IP-Adresse oder die Benutzerkonfiguration innerhalb der letzten 15 Minuten mithilfe von CLI-Befehlen geändert wurden).

5. Klicken Sie zum Ändern des IPMI-Stromversorgungsstatus auf die entsprechende Schaltfläche.
   - **Power Up**: Wird angezeigt, wenn das Remotesystem ausgeschaltet ist. Klicken Sie auf diese Schaltfläche, um das Remotesystem einzuschalten.
   - **Power Down**: Wird angezeigt, wenn das Remotesystem eingeschaltet ist. Klicken Sie auf diese Schaltfläche, um das Remotesystem auszuschalten.
   - **Power Cycle**: Wird angezeigt, wenn das Remotesystem eingeschaltet ist. Klicken Sie auf diese Schaltfläche, um das Remotesystem ein- und auszuschalten.
   - **Manage Another System**: Klicken Sie auf diese Schaltfläche, um sich bei einem anderen Remotesystem für IPMI Power Management anzumelden.
   - **Done**: Klicken Sie auf diese Schaltfläche, um das Dialogfeld „IPMI Power Management“ zu schließen.

   HINWEIS

   Die IPMI-Funktion „Power Down“ führt kein ordnungsgemäßes Herunterfahren von DD OS durch. Diese Option kann verwendet werden, wenn DD OS hängt und nicht verwendet werden kann, um ein System ordnungsgemäß herunterzufahren.

Managen der Stromversorgung mit der Befehlszeilenoberfläche

Mithilfe der Befehlszeilenoberfläche (Command Line Interface, CLI) können Sie die Stromversorgung auf einem Remotesystem managen und das Remotekonsolenmonitoring starten.

Hinweis

Das Remotesystem muss ordnungsgemäß eingerichtet sein, bevor Sie die Stromversorgung managen oder das System überwachen können.

Vorgehensweise

1. Stellen Sie eine CLI-Sitzung auf dem System her, über das Sie ein Remotesystem überwachen möchten.
2. Um die Stromversorgung auf dem Remotesystem zu managen, geben Sie`ipmi remote power {on | off | cycle | status} ipmi-target <`*ipaddr*hostname `| > user` *user* ein.
3. Um das Remotekonsolenmonitoring zu starten, geben Sie `ipmi remote console ipmi-target <`*ipaddr* `|` *hostname*`> user` *user* ein.

   Hinweis

   Der Benutzername ist ein IPMI-Benutzername, der für IPMI auf dem Remotesystem definiert ist. DD OS-Benutzernamen werden nicht automatisch von IPMI unterstützt.

4. Um die Remotekonsolenmonitoring-Sitzung zu beenden und zur Befehlszeile zurückzukehren, geben Sie das at-Symbol (@) ein.
5. Um das Remotekonsolenmonitoring zu beenden, geben Sie das Tildesymbol ein (~).

KAPITEL 4

Monitoring von Data Domain-Systemen

Inhalt dieses Kapitels:

Anzeigen von Status- und Identitätsinformationen einzelner Systeme

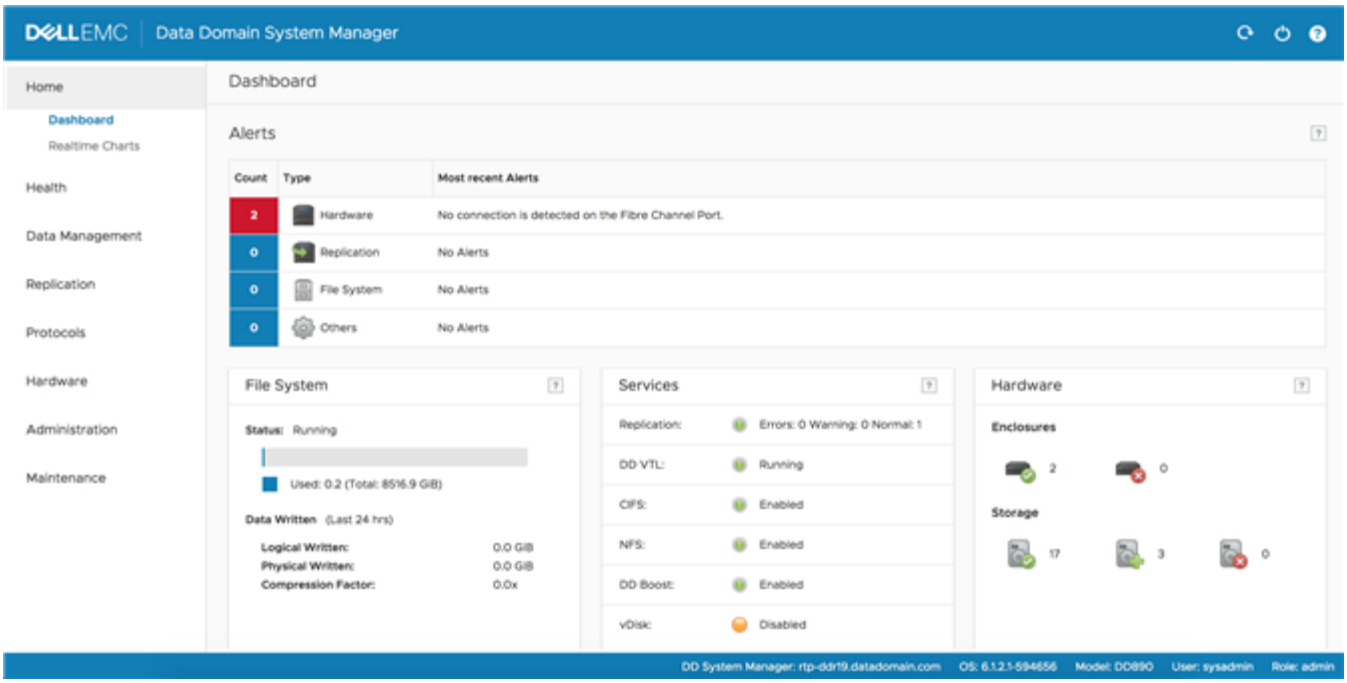
Im Bereich **Dashboard** werden Übersichten und Status von Warnmeldungen, Dateisystem, lizenzierten Services und Hardwaregehäusen angezeigt. Der Bereich **Maintenance System** zeigt zusätzliche Systeminformationen an, einschließlich Systemverfügbarkeit und Seriennummern für das System und Gehäuse.

Systemname, Softwareversion und Benutzerinformationen werden in der Fußzeile jederzeit angezeigt.

Vorgehensweise

1. Klicken Sie zum Anzeigen des System-Dashboard auf **Home** > **Dashboard**.

   Abbildung 4 System-Dashboard



2. Um Systembetriebszeit und Identitätsinformationen anzuzeigen, wählen Sie **Maintenance** > **System** aus.

   Systemverfügbarkeits- und Identifikationsinformationen werden im Bereich „System“ angezeigt.

Bereich „Dashboard Alerts“

Der Bereich „Dashboard Alerts“ zeigt die Anzahl, den Typ und den Text der letzten Warnmeldungen im System für jedes Subsystem (Hardware, Replikation, Dateisystem und andere) an. Klicken Sie in den Bereich „Alerts“, um weitere Informationen über die aktuellen Warnmeldungen anzuzeigen.

Tabelle 58 Dashboard Alerts – Spaltenbeschreibungen

Spalte	Beschreibung
Count	Anzahl der aktuellen Warnmeldungen für den in der benachbarten Spalte angegebenen Subsystemtyp. Die Hintergrundfarbe kennzeichnet den Schweregrad der Warnmeldung.
Type	Subsystem, das die Warnmeldung generiert hat
Most recent alerts	Text der letzten Warnmeldung für den in der benachbarten Spalte angegebenen Subsystemtyp

Bereich „Dashboard File System“

Im Bereich „Dashboard File System“ werden Statistiken für das gesamte Dateisystem angezeigt. Klicken Sie in den Bereich „File System“, um weitere Informationen anzuzeigen.

Tabelle 59 Beschreibungen der Spaltenbezeichnungen im Bereich „File System“

Spalte	Beschreibung
Status	Aktueller Status des Dateisystems
X.Xx	Durchschnittlicher Komprimierungsfaktor für das Dateisystem
Used	Verwendeter Gesamtspeicherplatz des Dateisystems
Data Written: Pre-compression	Vom System empfangene Datenmenge vor der Komprimierung
Data Written: Post-compression	Auf dem System gespeicherte Datenmenge nach der Komprimierung

Bereich „Dashboard Services“

Im Bereich „Dashboard Services“ wird der Status der folgenden Services angezeigt: Replikation, DD VTL, CIFS, NFS, DD Boost und vDisk. Klicken Sie auf einen Service, um detaillierte Informationen über diesen Service anzuzeigen.

Tabelle 60 Beschreibungen der Spalten im Bereich „Services“

Spalte	Beschreibung
Linke Spalte	In der linken Spalte werden die Services aufgeführt, die möglicherweise auf dem System verwendet werden. Zu diesen Services können Replikation, DD VTL, CIFS, NFS, DD Boost und vDisk gehören.

Tabelle 60 Beschreibungen der Spalten im Bereich „Services“ (Fortsetzung)

Spalte	Beschreibung
Rechte Spalte	In der rechten Spalte wird der Betriebsstatus der Services angezeigt. Bei den meisten Services lautet dieser Status „Enabled“, „Disabled“ oder „Not licensed“. In der Zeile für den Replikationsservice wird die Anzahl der Replikationskontexte im Normal-, Warnungs- und Fehlerzustand angezeigt. Ein farbiges Feld wird bei Normalbetrieb grün, in Warnsituationen gelb und bei Fehlern rot angezeigt.

Bereich „Dashboard HA Readiness“

In HA-Systemen gibt der HA-Bereich an, ob das System bei Bedarf ein Failover vom aktiven Node zum Stand-by-Node durchführen kann.

Klicken Sie auf **HA panel**, um zum Bereich **High Availability** unter **HEALTH** zu navigieren.

Bereich „Dashboard Hardware“

Im Bereich „Dashboard Hardware“ wird der Status der Systemgehäuse und Laufwerke angezeigt. Klicken Sie in den Bereich „Hardware“, um weitere Informationen über diese Komponenten anzuzeigen.

Tabelle 61 Beschreibungen der Spaltenbezeichnungen im Bereich „Hardware“

Bezeichnung	Beschreibung
Gehäuse	In den Gehäusesymbolen wird die Anzahl der Gehäuse im Normalzustand (grünes Häkchen) und im heruntergestuften Zustand (rotes X) angezeigt.
Speicher	In den Speichersymbolen wird die Anzahl der Festplattenlaufwerke im Normalzustand (grünes Häkchen), im Ersatzzustand (grünes +) und im Fehlerzustand (rotes X) angezeigt.

Bereich „Maintenance System“

Im Bereich „Maintenance System“ werden Systemmodellnummer, DD OS-Version, Systembetriebszeit sowie System- und Gehäuseseriennummer angezeigt.

Tabelle 62 Beschreibungen der Spaltenbezeichnungen im Bereich „System“

Bezeichnung	Beschreibung
Modellnummer	Die Modellnummer ist die dem Data Domain-System zugewiesene Nummer.

Tabelle 62 Beschreibungen der Spaltenbezeichnungen im Bereich „System“ (Fortsetzung)

Bezeichnung	Beschreibung
Version	Die Version ist die DD OS-Version und die Build-Nummer der auf dem System ausgeführten Software.
System Uptime	Die Systembetriebszeit ist die Dauer des Systembetriebs seit dem letzten Systemstart. Der Wert in Klammern ist der Zeitpunkt der letzten Aktualisierung der Systembetriebszeit.
System Serial No.	Die Systemseriennummer ist die dem System zugewiesene Seriennummer. Bei neueren Systemen wie DD4500 und DD7200 ist die Seriennummer des Systems unabhängig von der Gehäuseseriennummer und bleibt während vieler Arten von Wartungsereignissen unverändert, einschließlich beim Gehäuseaustausch. Auf Legacy-Systemen wie DD990 und früher wird die Seriennummer des Systems nach der Gehäuseseriennummer festgelegt.
Chassis Serial No.	Die Gehäuseseriennummer ist die Seriennummer des Gehäuses des aktuellen Systems.

Bereich „Health Alerts“

Warnmeldungen werden von Systemservices und Subsystemen generiert, um Systemevents zu melden. Im Bereich „Health“ > „Alerts“ werden Registerkarten angezeigt, auf denen Sie aktuelle und nicht aktuelle Warnmeldungen, die konfigurierten Gruppen für Warnmeldungsbenachrichtigungen und die Konfiguration für Benutzer anzeigen können, die tägliche Zusammenfassungsberichte zu Warnmeldungen erhalten möchten.

Warnmeldungen werden auch als SNMP-Traps gesendet. Die vollständige Liste von Traps finden Sie in der *MIB-Kurzübersicht* oder SNMP-MIB.

Anzeigen und Löschen aktueller Warnmeldungen

Auf der Registerkarte „Current Alerts“ werden eine Liste aller aktuellen Warnmeldungen sowie detaillierte Informationen für eine ausgewählte Warnmeldung angezeigt. Eine Warnmeldung wird automatisch aus der Liste „Current Alerts“ gelöscht, wenn die zugrunde liegende Situation korrigiert oder die Warnmeldung manuell gelöscht wird.

Vorgehensweise

1. Um alle aktuelle Warnmeldungen anzuzeigen, wählen Sie **Health** > **Alerts** > **Current Alerts**.
2. Gehen Sie wie folgt vor, um die Anzahl der Einträge in der Liste der aktuellen Warnmeldungen zu begrenzen.

a. Wählen Sie im Bereich „Filter By“ eine **Severity** und eine **Class** aus, um nur Warnmeldungen zuzulassen, auf die diese Auswahlen zutreffen.

b. Klicken Sie auf **Update**.

Alle Warnmeldungen, die nicht dem Schweregrad und der Klasse entsprechen, werden aus der Liste entfernt.

3. Um zusätzliche Informationen für eine bestimmte Warnmeldung im Bereich **Details** anzuzeigen, klicken Sie in der Liste auf die Warnmeldung.
4. Um eine Warnmeldung zu löschen, aktivieren Sie in der Liste das Kontrollkästchen für die Warnmeldung und klicken Sie auf **Clear.**

   Eine gelöschte Warnmeldung wird nicht mehr in der Liste der aktuellen Warnmeldungen angezeigt, ist aber weiterhin im Warnmeldungsverlauf enthalten.

5. Um die Filterung zu entfernen und zur vollständigen Auflistung aktueller Warnmeldungen zurückzukehren, klicken Sie auf **Reset**.

Registerkarte „Current Alerts“

Auf der Registerkarte „Current Alerts“ werden eine Liste der Warnmeldungen sowie detaillierte Informationen über eine ausgewählte Warnmeldung angezeigt.

Tabelle 63 Warnmeldungsliste, Beschreibungen der Spaltenbezeichnungen

Element	Beschreibung
Meldung	Der Text der Warnmeldung
Severity	Der Schweregrad der Warnmeldung. Beispiel: Warnung, kritisch, Informationen oder Notfall.
Datum	Datum und Uhrzeit des Auftretens der Warnmeldung
Klasse	Das Subsystem, in dem die Warnmeldung aufgetreten ist
Objekt	Die physische Komponente, in der die Warnmeldung auftritt

Tabelle 64 Bereich „Details“, Beschreibungen der Zeilenbezeichnungen

Element	Beschreibung
Name	Eine Textkennung der Warnmeldung
Meldung	Der Text der Warnmeldung
Severity	Der Schweregrad der Warnmeldung. Beispiel: Warnung, kritisch, Informationen, Notfall.
Klasse	Das Subsystem und Gerät, in dem die Warnmeldung aufgetreten ist
Datum	Datum und Uhrzeit des Auftretens der Warnmeldung
Object ID	Die physische Komponente, in der die Warnmeldung auftritt
Ereignis-ID	Eine Eventkennung
Tenant Units	Eine Liste der betroffenen Mandanteneinheiten
Beschreibung	Nähere Informationen zur Warnmeldung

Tabelle 64 Bereich „Details“, Beschreibungen der Zeilenbezeichnungen (Fortsetzung)

Element	Beschreibung
Aktion	Ein Vorschlag zur Behebung der Warnmeldung
Object Info	Weitere Informationen zum betroffenen Objekt
SNMP OID	SNMP-Objekt-ID

Anzeigen des Warnmeldungsverlaufs

Auf der Registerkarte „Alerts History“ werden eine Liste aller gelöschten Warnmeldungen sowie detaillierte Informationen für eine ausgewählte Warnmeldung angezeigt.

Vorgehensweise

1. Um die gesamte Warnmeldungshistorie anzuzeigen, wählen Sie **Health** > **Alerts** > **Alerts History**.
2. Gehen Sie wie folgt vor, um die Anzahl der Einträge in der Liste der aktuellen Warnmeldungen zu begrenzen.
   a. Wählen Sie im Bereich „Filter By“ eine **Severity** und eine **Class** aus, um nur Warnmeldungen zuzulassen, auf die diese Auswahlen zutreffen.
   b. Klicken Sie auf **Update**.

      Alle Warnmeldungen, die nicht dem Schweregrad und der Klasse entsprechen, werden aus der Liste entfernt.
3. Um zusätzliche Informationen für eine bestimmte Warnmeldung im Bereich **Details** anzuzeigen, klicken Sie in der Liste auf die Warnmeldung.
4. Um die Filterung zu entfernen und zur vollständigen Auflistung gelöschter Warnmeldungen zurückzukehren, klicken Sie auf **Reset**.

Registerkarte „Alerts History“

Auf der Registerkarte „Alerts History“ werden eine Liste der gelöschten Warnmeldungen sowie Details für eine ausgewählte Warnmeldung angezeigt.

Tabelle 65 Warnmeldungsliste, Beschreibungen der Spaltenbezeichnungen

Element	Beschreibung
Meldung	Der Text der Warnmeldung
Severity	Der Schweregrad der Warnmeldung. Beispiel: Warnung, kritisch, Informationen oder Notfall.
Datum	Datum und Uhrzeit des Auftretens der Warnmeldung
Klasse	Das Subsystem, in dem die Warnmeldung aufgetreten ist
Objekt	Die physische Komponente, in der die Warnmeldung auftritt
Status	Gibt an, ob der Status veröffentlicht oder gelöscht ist. Eine veröffentlichte Warnmeldung wird nicht gelöscht.

Tabelle 66 Bereich „Details“, Beschreibungen der Zeilenbezeichnungen

Element	Beschreibung
Name	Eine Textkennung der Warnmeldung
Meldung	Der Text der Warnmeldung
Severity	Der Schweregrad der Warnmeldung. Beispiel: Warnung, kritisch, Informationen, Notfall.
Klasse	Das Subsystem und Gerät, in dem die Warnmeldung aufgetreten ist
Datum	Datum und Uhrzeit des Auftretens der Warnmeldung
Objekt-ID	Die physische Komponente, in der die Warnmeldung auftritt
Ereignis-ID	Eine Eventkennung
Tenant Units	Eine Liste der betroffenen Mandanteneinheiten
Zusätzliche Informationen	Nähere Informationen zur Warnmeldung
Status	Gibt an, ob der Status veröffentlicht oder gelöscht ist. Eine veröffentlichte Warnmeldung wird nicht gelöscht.
Beschreibung	Nähere Informationen zur Warnmeldung
Aktion	Ein Vorschlag zur Behebung der Warnmeldung

Anzeigen des Status der Hardwarekomponenten

Im Bereich "Hardware Chassis" wird ein Blockdiagramm der einzelnen Gehäuse in einem System, einschließlich der Gehäuseseriennummer und des Gehäusestatus, angezeigt. In jedem Blockdiagramm finden Sie die Gehäusekomponenten wie Laufwerke, Lüfter, Netzteile, NVRAM, CPUs und Arbeitsspeicher. Die angezeigten Komponenten hängen vom Systemmodell ab.

Auf Systemen mit DD OS 5.5.1 und höher wird auch die Seriennummer des Systems angezeigt. Bei neueren Systemen wie DD4500 und DD7200 ist die Seriennummer des Systems unabhängig von der Gehäuseseriennummer und bleibt während vieler Arten von Wartungsereignissen unverändert, einschließlich beim Gehäuseaustausch. Auf Legacy-Systemen wie DD990 und früher wird die Seriennummer des Systems nach der Gehäuseseriennummer festgelegt.

Vorgehensweise

1. Wählen Sie **Hardware** > **Chassis** aus.

   In der Ansicht „Chassis“ werden die Systemgehäuse angezeigt. „Enclosure 1“ ist der Systemcontroller. Die restlichen Gehäuse werden unterhalb von „Enclosure 1“ angezeigt.

   Komponenten mit Problemen werden gelb (Warnung) oder rot (Fehler) angezeigt, andernfalls wird für die Komponenten „OK“ angezeigt.

2. Wenn Sie den Mauszeiger über eine Komponente bewegen, wird ein detaillierter Status angezeigt.

Lüfterstatus

Lüfter sind nummeriert und die Nummern entsprechen ihrer Position im Gehäuse. Bewegen Sie den Mauszeiger über einen Systemlüfter, um eine Kurzinformation für dieses Gerät anzuzeigen.

Tabelle 67 Lüfterkurzinformation, Beschreibungen der Spaltenbezeichnungen

Element	Beschreibung
Beschreibung	Der Name des Lüfters.
Level	Der aktuelle Bereich der Betriebsgeschwindigkeit (Low, Medium, High). Die Betriebsgeschwindigkeit ändert sich je nach Temperatur innerhalb des Gehäuses.
Status	Die Integrität des Lüfters.

Temperaturstatus

Für Data Domain-Systeme und einige Komponenten ist ein bestimmter Betriebstemperaturbereich konfiguriert, der durch ein nicht konfigurierbares Temperaturprofil definiert wird. Bewegen Sie den Mauszeiger über das Feld „Temperature“, um die Temperaturkurzinformation anzuzeigen.

Tabelle 68 Temperaturkurzinformation, Beschreibungen der Spaltenbezeichnungen

Element	Beschreibung
Beschreibung	Position im Gehäuse, an der gemessen wird. Die aufgeführten Komponenten sind modellabhängig und häufig abgekürzt angegeben. Dazu gehören zum Beispiel: • CPU 0 Temp (CPU, Central Processing Unit) • MLB Temp 1 (Hauptplatine) • BP middle temp (Rückwandplatine) • LP temp (flaches Profil von I/O-Riser-FRU) • FHFL temp (vollständige Höhe und Länge von I/O-Riser-FRU) • FP temp (Vorderseite)
C/F	In der Spalte C/F wird die Temperatur in Grad Celsius und Grad Fahrenheit angezeigt. Wenn in der Beschreibung für eine CPU *relative* (CPU-*n*-relativ) angegeben ist, wird in dieser Spalte die Gradzahl angezeigt, die jede CPU unterhalb der maximal zulässigen Temperatur und der tatsächlichen Temperatur für das Innere des Gehäuses (Gehäuseumgebungstemperatur) liegt.
Status	Zeigt den Temperaturstatus an: • OK: Die Temperatur ist akzeptabel. • Critical: Die Temperatur ist höher als die Abschalttemperatur.

Tabelle 68 Temperaturkurzinformation, Beschreibungen der Spaltenbezeichnungen (Fortsetzung)

Element	Beschreibung
	• Warning: Die Temperatur ist höher als die Warntemperatur (aber niedriger als die Abschalttemperatur). • Strich (-): Für diese Komponente sind keine Temperaturschwellenwerte konfiguriert, sodass kein Status gemeldet wird.

Status des Managementbereichs

DD6300-, DD6800- und DD9300-Systeme haben einen festen Managementbereich mit einem Ethernetport für das Managementnetzwerk auf der Rückseite des Gehäuses. Bewegen Sie den Mauszeiger über den Ethernetport, um eine Kurzinformation anzuzeigen.

Tabelle 69 Managementbereich-Kurzinformation, Beschreibung der Spaltenbezeichnungen

Element	Beschreibung
Beschreibung	Der Typ der im Managementbereich installierten NIC
Anbieter	Der Hersteller der Management-NIC
Ports	Der Name des Managementnetzwerks (Ma)

SSD-Status (nur DD6300)

DD6300 unterstützt bis zu zwei SSDs in den Steckplätzen auf der Rückseite des Gehäuses. Die SSD-Steckplätze sind nummeriert und die Nummern entsprechen ihrer Position im Gehäuse. Bewegen Sie den Mauszeiger über eine SSD, um eine Kurzinformation für dieses Gerät anzuzeigen.

Tabelle 70 SSD-Kurzinformation, Beschreibungen der Spaltenbezeichnungen

Element	Beschreibung
Beschreibung	Der Name der SSD
Status	Der Status der SSD
Life Used	Der Prozentsatz der bereits verwendeten geschätzten Lebensdauer der SSD

Netzteilstatus

Die Kurzinformation zeigt den Status des Netzteils an (OK oder DEGRADED, wenn ein Netzteil fehlt oder fehlerhaft ist). Sie können auch die LED auf der Rückseite des Gehäuses für jedes Netzteil prüfen, um zu identifizieren, welche Netzteile ersetzt werden müssen.

PCI-Steckplatzstatus

In der Gehäuseansicht werden alle PCI-Steckplätze mit den entsprechenden Nummern angezeigt. Kurzinformationen zeigen den Komponentenstatus für jede Karte in einem PCI-Steckplatz. Beispielsweise zeigt die Kurzinformation für ein NVRAM-Kartenmodell die Arbeitsspeichergröße, Temperaturdaten und Batterielevel an.

NVRAM-Status

Bewegen Sie den Mauszeiger über „NVRAM“, um Informationen zum nicht flüchtigen RAM, den Batterien und anderen Komponenten anzuzeigen.

Tabelle 71 NVRAM-Kurzinformation, Beschreibungen der Spaltenbezeichnungen

Element	Beschreibung
Komponente	Die Komponentenliste enthält abhängig vom auf dem System installierten NVRAM folgende Elemente: • Firmwareversion • Speichergröße • Fehleranzahl • Fehleranzahl für Flash-Controller • Platinentemperatur • CPU-Temperatur • Batterieanzahl (Die Anzahl der Batterien hängt vom Systemtyp ab.) • Aktuelle Steckplatznummer für NVRAM
C/F	Zeigt die Temperatur für ausgewählte Komponenten im Celsius-/Fahrenheit-Format an.
Wert	Werte werden für ausgewählte Komponenten zur Verfügung gestellt und beschreiben Folgendes. • Firmware-Versionsnummer • Speicherkapazität der angezeigten Geräte • Fehleranzahl für Speicher, PCI und Controller • Fehleranzahl für Flash-Controller in den folgenden Gruppen: Konfigurationsfehler (Cfg Err), Fehlerbedingungen (Panic), Bus Hang, Warnungen für defekte Blöcke (Bad Blk Warn), Backupfehler (Bkup Err) und Wiederherstellungsfehler (Rstr Err) • Batterieinformationen, wie Ladezustand und Status (aktiviert oder deaktiviert)

Anzeigen von Systemstatistiken

Im Bereich „Realtime Charts“ werden bis zu sieben Diagramme mit Echtzeit-Subsystemperformancestatistiken angezeigt, beispielsweise zur CPU-Auslastung und zum Festplattendatenverkehr.

Vorgehensweise

1. Wählen Sie **Home** > **Realtime Charts**.

   Im Bereich „Performance Graphs“ werden die aktuell ausgewählten Diagramme angezeigt.
2. Zum Ändern der Auswahl der anzuzeigenden Diagramme aktivieren und deaktivieren Sie die Kontrollkästchen für Diagramme im Listenfeld.
3. Zum Anzeigen bestimmter Datenpunktinformationen bewegen Sie den Mauszeiger über einen Diagrammpunkt.
4. Wenn ein Diagramm mehrere Daten enthält, können Sie mithilfe der Kontrollkästchen in der rechten oberen Ecke des Diagramms auswählen, was angezeigt werden soll. Wenn beispielsweise „Read“ im oberen rechten Bereich des Diagramms zur Festplattenaktivität nicht ausgewählt ist, werden nur Schreibdaten im Diagramm angezeigt.

Ergebnisse

In jedem Diagramm wird die Nutzung in den letzten 200 Sekunden angezeigt. Klicken Sie auf **Pause**, um die Anzeige vorübergehend anzuhalten. Klicken Sie auf **Resume**, um die Anzeige neu zu starten und Punkte anzuzeigen, die während der Pause verpasst wurden.

Performancestatistikdiagramme

Die Performancestatistikdiagramme zeigen Statistiken für wichtige Komponenten und Funktionen des Systems.

DD Boost Active Connections

Das Diagramm „DD Boost Active Connections“ zeigt die Anzahl der aktiven DD Boost-Verbindungen für die letzten 200 Sekunden an. Separate Zeilen im Diagramm zeigen die Anzahl der Leseverbindungen (Recovery) und Schreibverbindungen (Backup).

DD Boost Data Throughput

Im Diagramm „DD Boost Data Throughput“ werden die pro Sekunde übertragenen Bytes für die letzten 200 Sekunden angezeigt. Separate Zeilen im Diagramm zeigen die Raten für Datenlesevorgänge vom System durch DD Boost-Clients und für Datenschreibvorgänge zum System durch DD Boost-Clients an.

Disk

Im Diagramm „Disk“ wird die Datenmenge, die an alle Laufwerke im System übertragen oder von allen Laufwerken übertragen werden, in der entsprechenden Einheit, z. B. KiB oder MiB pro Sekunde, basierend auf den empfangenen Daten angezeigt.

File System Operations

Im Diagramm „File System Operations“ wird die Anzahl der Vorgänge pro Sekunde angezeigt, die in den letzten 200 Sekunden durchgeführt wurden.

Separate Zeilen im Diagramm Grafik zeigen die NFS- und CIFS-Vorgänge pro Sekunde an.

Network

Im Diagramm „Network“ wird die Datenmenge, die über jede Ethernetverbindung übertragen wird, in der entsprechenden Einheit, z. B. KiB oder MiB pro Sekunde, basierend auf den empfangenen Daten angezeigt. Für jeden Ethernetport wird eine Zeile angezeigt.

Recent CPU Usage

Im Diagramm „Recent CPU Usage“ wird der Prozentsatz der CPU-Auslastung der letzten 200 Sekunden angezeigt.

Replication (DD Replicator muss lizenziert sein)

Im Diagramm „Replication“ wird die Menge der Replikationsdaten angezeigt, die in den letzten 200 Sekunden über das Netzwerk übertragen wurden. Separate Zeilen zeigen die ein- und ausgehenden Daten folgendermaßen an:

- In: Die Gesamtanzahl der Maßeinheiten, z. B. Kilobyte pro Sekunde, die auf dieser Seite von der anderen Seite des DD Replicator-Paars empfangen wurden. Für das Ziel umfasst der Wert Backupdaten, Replikationsoverhead und Netzwerkoverhead. Für die Quelle umfasst der Wert Replikationsoverhead und Netzwerkoverhead.
- Out: Die Gesamtanzahl der Maßeinheiten, z. B. Kilobyte pro Sekunde, die von dieser Seite an die andere Seite des DD Replicator-Paars gesendet wurden. Für die Quelle umfasst der Wert Backupdaten, Replikationsoverhead und Netzwerkoverhead. Für das Ziel umfasst der Wert Replikationsoverhead und Netzwerkoverhead.

Anzeigen aktiver Benutzer

Auf der Registerkarte „Active Users“ werden die Namen der beim System angemeldeten Benutzer sowie Statistiken zu den aktuellen Benutzersitzungen angezeigt.

Vorgehensweise

1. Wählen Sie **Administration** > **Access** > **Active Users**.

   Die Liste „Active Users“ wird angezeigt. Darin werden Informationen zu jedem Benutzer angezeigt.

Tabelle 72 Liste „Active Users“, Beschreibungen der Spaltenbezeichnungen

Element	Beschreibung
Name	Benutzername des angemeldeten Benutzers
Idle	Zeit seit der letzten Aktivität des Benutzers
Last Login From	System, von dem der Benutzer sich angemeldet hat
Last Login Time	Zeitstempel, wann der Benutzer sich angemeldet hat
TTY	Terminalschreibweise für die Anmeldung. Die GUI wird für DD System Manager-Benutzer angezeigt.

Hinweis

Um lokale Benutzer zu managen, klicken Sie auf **Go to Local Users**.

Verlaufsberichtmanagement

Mit DD System Manager können Sie Berichte erzeugen, um die Speicherplatznutzung auf einem Data Domain-System über einen Zeitraum von bis zu zwei Jahren nachverfolgen zu können. Sie können auch Berichte erzeugen, um den Replikationsfortschritt zu verdeutlichen, sowie tägliche und kumulative Berichte zum Dateisystem anzeigen.

Die Ansicht „Reports“ ist in zwei Bereiche aufgeteilt. Im oberen Bereich können Sie die verschiedenen Arten von Berichten erstellen. Im unteren Bereich können Sie gespeicherte Berichte anzeigen und managen.

Berichte werden je nach Berichtstyp im Tabellenformat und als Diagramme angezeigt. Sie können einen Bericht für ein bestimmtes Data Domain-System auswählen und einen bestimmten Zeitraum bereitstellen.

Die Berichte enthalten historische Daten, keine Echtzeitdaten. Nach der Erstellung eines Berichts bleiben die Diagramme statisch und werden nicht mehr aktualisiert. Folgende Arten von Informationen können Sie mit den Berichten abrufen:

- Die Datenmenge, die auf dem System gesichert wurde, und die Menge der Deduplizierung, die erreicht wurde
- Schätzungen dazu, wann das Data Domain-System voll sein wird, basierend auf wöchentlichen Speicherplatznutzungstrends
- Backup- und Komprimierungsnutzung basierend auf ausgewählten Intervallen
- Verlaufsdaten zur Bereinigungsperformance, einschließlich Dauer des Bereinigungszyklus, Menge des Speicherplatzes, der bereinigt werden kann, und Menge des Speicherplatzes, der zurückgewonnen wurde
- Menge der WAN-Bandbreite, die von der Replikation verwendet wird, für Quelle und Ziel, und ob die Bandbreite ausreicht, um Replikationsanforderungen zu erfüllen
- Systemperformance und Ressourcenauslastung

Berichtstypen

Im Bereich „New Report“ werden die Berichtstypen aufgeführt, die Sie auf dem System erzeugen können.

Hinweis

Replikationsberichte können nur erstellt werden, wenn das System eine Replikationslizenz enthält und ein gültiger Replikationskontext konfiguriert ist.

Bericht zur kumulativen Speicherplatznutzung des Dateisystems

Der Bericht „File System Cumulative Space Usage“ zeigt 3 Diagramme an, in denen die Speicherplatznutzung auf dem System während der angegebenen Dauer detailliert dargestellt wird. Mit diesem Bericht wird analysiert, wie viele Daten gesichert werden, welchen Umfang die durchgeführte Deduplizierung hat und wie viel Speicherplatz belegt ist.

Tabelle 73 Beschreibungen der Elemente des Diagramms „File System – Usage“

Element	Beschreibung
Data Written (GiB)	Die Menge der geschriebenen Daten vor der Komprimierung. Dies wird im Bericht mit einem lila schattierten Bereich angezeigt.
Zeit	Der Zeitrahmen für Daten, die geschrieben wurden. Die Zeit, die in diesem Bericht angezeigt wird, ändert sich je nach dem, welche Dauer zum Zeitpunkt der Diagrammerstellung ausgewählt war.
Total Compression Factor	Der Gesamtkomprimierungsfaktor gibt die Komprimierungsrate an.

Tabelle 74 Beschreibungen der Elemente des Diagramms „File System – Consumption“

Element	Beschreibung
Used (GiB)	Der nach der Komprimierung verwendete Speicherplatz.
Time	Das Datum, an dem die Daten geschrieben wurden. Die Zeit, die in diesem Bericht angezeigt wird, ändert sich je nach dem, welche Dauer zum Zeitpunkt der Diagrammerstellung ausgewählt war.
Used (Post Comp)	Der nach der Komprimierung verwendete Speicher.
Usage Trend	Die schwarz gepunktete Linie zeigt den Trend der Speichernutzung an. Wenn die Linie die rote Linie oben erreicht, ist der Speicher fast voll.
Capacity	Gesamtkapazität auf einem Data Domain-System.
Cleaning	„Cleaning“ ist der Bereinigungszyklus (Start- und Endzeit für jeden Bereinigungszyklus). Anhand dieser Informationen können Administratoren den optimalen Zeitpunkt für eine Speicherplatzbereinigung sowie die optimale Drosselungseinstellung bestimmen.

Tabelle 75 Beschreibungen der Elemente des Diagramms „File System Weekly Cumulative Capacity“

Element	Beschreibung
Date (oder Time für einen 24-Stunden-Bericht)	Der letzte Tag jeder Woche basierend auf den für den Bericht festgelegten Kriterien. Der 24-Stunden-Zeitraum in Berichten reicht von Mittag bis Mittag.
Data Written (Pre-Comp)	Die kumulierten, vor der Komprimierung geschriebenen Daten für den angegebenen Zeitraum.
Used (Post-Comp)	Die kumulierten, nach der Komprimierung geschriebenen Daten für den angegebenen Zeitraum.
Compression Factor	Der Gesamtkomprimierungsfaktor. Dieser wird im Bericht als schwarze Linie angezeigt.

Bericht zur täglichen Speicherplatznutzung des Dateisystems

Der Bericht „File System Daily Space Usage“ zeigt fünf Diagramme an, in denen die Speicherplatznutzung während der angegebenen Dauer detailliert dargestellt wird. Dieser Bericht wird zur Analyse der täglichen Aktivitäten verwendet.

Tabelle 76 Beschreibungen der Elemente des Diagramms „File System Daily Space Usage“

Element	Beschreibung
Space Used (GiB)	Die Menge des verwendeten Speicherplatzes. Der rot schattierte Bereich ist der verwendete Speicherplatz nach der Komprimierung. Der lila schattierte Bereich ist der verwendete Speicherplatz vor der Komprimierung.
Time	Das Datum, an dem die Daten geschrieben wurden.
Compression Factor	Der Gesamtkomprimierungsfaktor. Dieser wird im Bericht als schwarzes Quadrat angezeigt.

Tabelle 77 Beschreibungen der Elemente des Diagramms „File System Daily Capacity Utilization“

Element	Beschreibung
Datum	Das Datum, an dem die Daten geschrieben wurden.
Data Written (Pre-Comp)	Die Menge der geschriebenen Daten vor der Komprimierung.
Used (Post-Comp)	Der nach der Komprimierung verwendete Speicher.
Total Compression Factor	Der Gesamtkomprimierungsfaktor.

Tabelle 78 Beschreibungen der Elemente des Diagramms „File System Weekly Capacity Utilization“

Element	Beschreibung
Start Date	Der erste Tag der Woche für diese Zusammenfassung.
End Date	Der letzte Tag der Woche für diese Zusammenfassung.
Available	Die Gesamtmenge des verfügbaren Speicherplatzes.
Consumed	Die Gesamtmenge des verwendeten Speicherplatzes.
Data (Post-Comp)	Die kumulierten, vor der Komprimierung geschriebenen Daten für den angegebenen Zeitraum.
Replication (Post-Comp)	Die kumulierten, nach der Komprimierung geschriebenen Daten für den angegebenen Zeitraum.
Overhead	Zusätzlicher Speicherplatz, der nicht für Daten verwendet wird.
Reclaimed by Cleaning	Die Gesamtmenge des Speicherplatzes, der nach der Bereinigung zurückgewonnen wurde.

Tabelle 79 Beschreibungen der Elemente des Diagramms „File System Compression Summary“

Element	Beschreibung
Time	Der Zeitraum der Datenerfassung für diesen Bericht.
Data Written (Pre-Comp)	Die Menge der geschriebenen Daten vor der Komprimierung.
Used (Post-Comp)	Der nach der Komprimierung verwendete Speicher.
Total Compression Factor	Der Gesamtkomprimierungsfaktor.

Tabelle 80 Beschreibungen der Elemente des Diagramms „File System Cleaning Activity“

Element	Beschreibung
Start Time	Der Zeitpunkt, zu dem die Bereinigung gestartet wurde.
End Time	Der Zeitpunkt, zu dem die Bereinigung abgeschlossen wurde.
Duration (Hours)	Die für die Bereinigung erforderliche Gesamtdauer in Stunden.
Space Reclaimed	Der zurückgewonnene Speicherplatz in Gibibytes (GiB).

Replikationsstatusbericht

Der Replikationsstatusbericht zeigt drei Diagramme an, die den Status des aktuellen Replikationsjobs enthalten, der auf dem System ausgeführt wird. Dieser Bericht bietet einen Snapshot aller Replikationskontexte, damit Sie den Gesamtreplikationsstatus auf einem Data Domain-System verstehen.

Tabelle 81 Beschreibungen der Bezeichnungen des zusammenfassenden Diagramms für den Replikationskontext

Element	Beschreibung
ID	Die Replikationskontextkennung
Source	Der Quellsystemname
Destination	Der Zielsystemname
Type	Der Typ des Replikationskontexts: MTree, Verzeichnis, Sammlung oder Pool
Status	Es gibt folgende Replikationsstatustypen: Error, Normal.
Sync as of Time	Zeit- und Datumsstempel der letzten Synchronisierung
Estimated Completion	Geschätzter Zeitpunkt, an dem die Replikation abgeschlossen sein sollte
Pre-Comp Remaining	Die Menge der zu replizierenden vorkomprimierten Daten. Dies gilt nur für den Typ „Collection“.
Post-Comp Remaining	Die Menge der zu replizierenden nachkomprimierten Daten. Dies gilt nur für die Typen „Directory“ und „Pool“.

Tabelle 82 Beschreibungen der Bezeichnungen des Fehlerstatusdiagramms für den Replikationskontext

Element	Beschreibung
ID	Die Replikationskontextkennung
Source	Der Quellsystemname
Destination	Der Zielsystemname
Type	Replikationskontexttyp: Directory oder Pool.
Status	Es gibt folgende Replikationsstatustypen: Error, Normal und Warning.
Beschreibung	Beschreibung des Fehlers

Tabelle 83 Beschreibungen der Bezeichnungen des Diagramms für verfügbaren Speicherplatz des Replikationsziels

Element	Beschreibung
Destination	Der Zielsystemname
Space Availability (GiB)	Gesamte verfügbare Speichermenge

Replikationsübersichtsbericht

Der Replikationsübersichtsbericht bietet Performanceinformationen zur gesamten eingehenden und ausgehenden Nutzung des Netzwerks eines Systems für die Replikation sowie pro Kontextlevel über einen bestimmten Zeitraum. Sie wählen aus einer Liste die Kontexte aus, die analysiert werden sollen.

Tabelle 84 Beschreibungen der Bezeichnungen des Replikationsübersichtsberichts

Element	Beschreibung
Network In (MiB)	Die Menge der Daten, die in das System gesendet werden. „Network In“ wird durch eine dünne grüne Linie angezeigt.
Network Out (MiB)	Die Menge der Daten, die aus dem System gesendet werden. „Network Out“ wird durch eine dicke orangefarbene Linie angezeigt.
Time	Das Datum, an dem die Daten geschrieben wurden
Pre-Comp Remaining (MiB)	Die Menge der zu replizierenden vorkomprimierten Daten. „Pre-Comp Remaining“ wird durch eine blaue Linie angezeigt.

Anzeigen des Aufgabenprotokolls

Im Aufgabenprotokoll wird eine Liste der derzeit ausgeführten Jobs wie Replikation oder Systemupgrades angezeigt. DD System Manager kann mehrere Systeme managen und Aufgaben auf diesen Systemen initiieren. Wenn eine Aufgabe auf einem Remotesystem initiiert wird, wird der Fortschritt dieser Aufgabe im Aufgabenprotokoll der Managementstation und nicht im Aufgabenprotokoll des Remotesystems nachverfolgt.

Vorgehensweise

1. Wählen Sie **Health** > **Jobs**.

   Die Ansicht „Tasks“ wird angezeigt.

2. Wählen Sie einen Filter für die Anzeige des Aufgabenprotokolls aus der Liste „Filter by“ aus. Zur Auswahl stehen **All**, **In Progress**, **Failed** oder **Completed**.

   In der Ansicht „Tasks“ wird der Status aller Aufgaben basierend auf dem von Ihnen ausgewählten Filter angezeigt und alle 60 Sekunden aktualisiert.

3. Führen Sie zum manuellen Aktualisieren der Aufgabenliste eine der folgenden Aktionen aus.

   - Klicken Sie auf **Update**, um das Aufgabenprotokoll zu aktualisieren.
   - Klicken Sie auf **Reset**, um alle Aufgaben anzuzeigen und alle festgelegten Filter zu entfernen.

4. Zum Anzeigen detaillierter Informationen zu einer Aufgabe wählen Sie die Aufgabe in der Aufgabenliste aus.

Tabelle 85 Detailed Information, Beschreibung der Bezeichnungen

Element	Beschreibung
System	Systemname
Beschreibung der Aufgabe	Beschreibung der Aufgabe
Status	Status der Aufgabe (Completed, Failed oder In Progress)
Start Time	Datum und Uhrzeit, zu denen die Aufgabe gestartet wurde
End Time	Datum und Uhrzeit, zu denen die Aufgabe beendet wurde
Error Message	Eine zutreffende Fehlermeldung, sofern vorhanden

HA-Status des Systems anzeigen

Sie können den Bereich **High Availability** verwenden, um detaillierte Informationen zum HA-Status des Systems anzuzeigen und dazu, ob das System gegebenenfalls ein Failover durchführen kann.

Vorgehensweise

1. Wählen Sie im DD System Manager **Health > High Availability** aus.

   Der Bildschirm **Health High Availability** wird angezeigt.
   Ein grünes Häkchen weist darauf hin, dass das System normal ausgeführt wird und bereit für das Failover ist.

   Der Bildschirm zeigt den aktiven Node, in der Regel de Node 0.

2. Bewegen Sie den Mauszeiger über einen Node, um seinen Status anzuzeigen.

   Der Node wird in Blau hervorgehoben, wenn er aktiv ist.

3. Klicken Sie auf das Drop-down-Menü im Banner, wenn Sie die Ansicht vom aktiven Node zum Stand-by-Node ändern möchten, in der Regel Node 1.

HA-Status

Die Ansicht **Health High Availability** (HA) informiert Sie über den Systemstatus unter Verwendung eines Diagramms der Nodes und ihres verbundenen Speichers. Darüber hinaus können Sie auch alle aktuellen Warnmeldungen sowie detaillierte Informationen über das System sehen.

Sie können bestimmen, ob der aktive Node und der Speicher betriebsbereit sind, indem Sie den Cursor über sie bewegen. Die Elemente sind in Blau hervorgehoben, wenn sie normal funktionieren. Der Stand-by-Node sollte in Grau angezeigt werden.

Sie können auch die Warnmeldungstabelle filtern, indem Sie auf eine Komponente klicken. Nur Warnmeldungen im Zusammenhang mit den ausgewählten Komponenten werden angezeigt.

Abbildung 5 Anzeigen für Integrität/HA

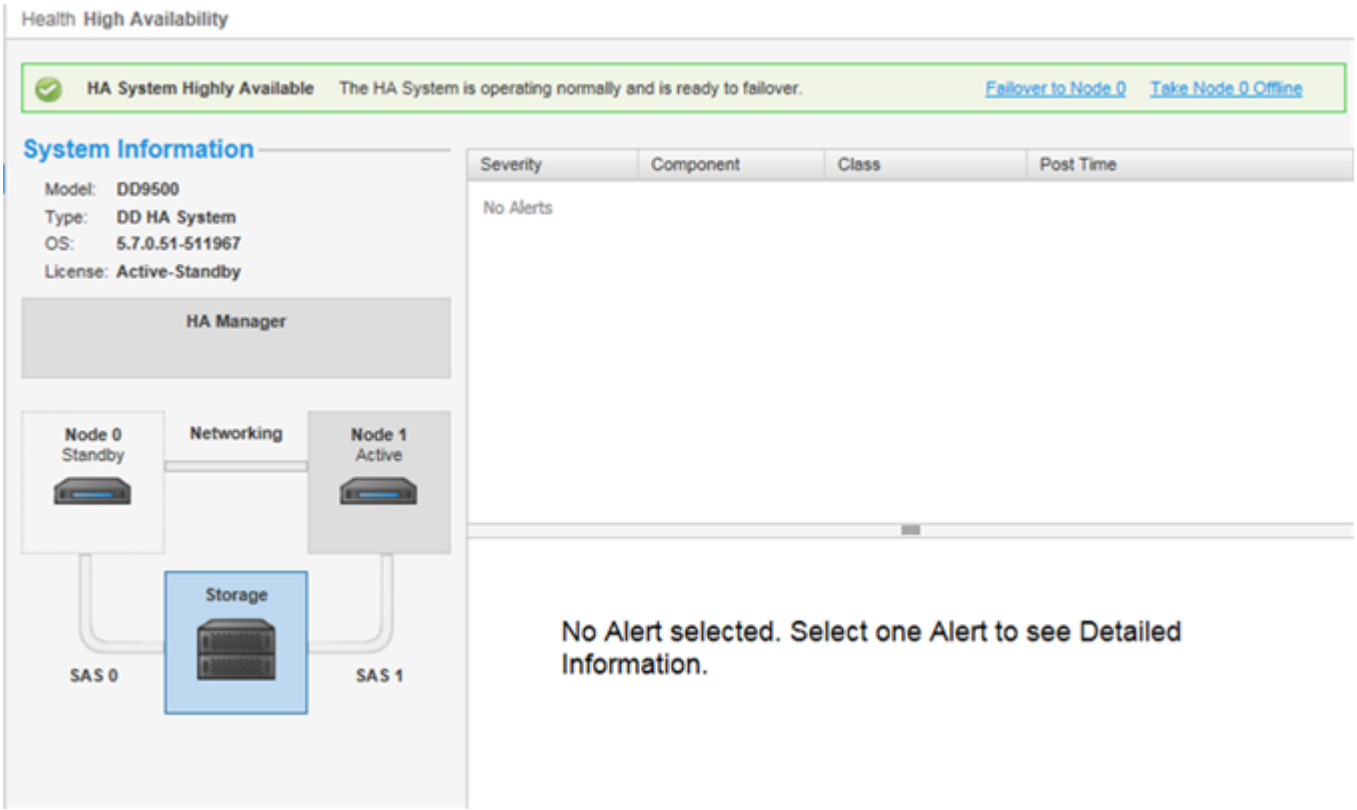


Tabelle 86 Anzeigen für HA

Element	Beschreibung
HA System bar	Zeigt ein grünes Häkchen an, wenn das System normal ausgeführt wird und bereit für das Failover ist.
Failover to Node 0	Ermöglicht Ihnen das manuelle Failover auf den Stand-by-Node.
Take Node 1 Offline	Ermöglicht Ihnen das Offlineschalten des aktiven Node bei Bedarf.

Tabelle 86 Anzeigen für HA (Fortsetzung)

Element	Beschreibung
Systeminformationen	Listet Data Domain-Systemmodell, Systemtyp, Version des verwendeten Data Domain-Betriebssystems und die angewendete HA-Lizenz auf.
HA Manager	Zeigt die Nodes, ihren angebundenen Speicher, das HA-Interconnect und die Verkabelung an.
Severity	Gibt den Schweregrad der Warnmeldungen an, die sich auf den HA-Status des Systems auswirken könnten.
Komponente	Gibt an, welche Komponente betroffen ist.
Klasse	Gibt die Klasse der empfangenen Warnmeldung an, wie Hardware, Umgebung und andere.
Post Time	Gibt die Uhrzeit und das Datum der Warnmeldungsveröffentlichung an.

KAPITEL 5

Dateisystem

Dieses Kapitel enthält die folgenden Themen:

Übersicht über das Dateisystem

Dieser Abschnitt enthält Informationen zur Verwendung des Dateisystems.

Datenspeicherung durch das Dateisystem

Die Speicherkapazität von Data Domain-Systemen lässt sich am besten managen, indem mehrere Backups erstellt und 20 % des Speicherplatzes frei gehalten werden, um diese Backups bis zur nächsten Bereinigung zu speichern. Die Speicherplatznutzung ist in erster Linie von der Größe und Komprimierbarkeit der Daten sowie von der Aufbewahrungsfrist abhängig.

Ein Data Domain-System ist als besonders zuverlässiges Onlinesystem für Backups und Archivdaten ausgelegt. Wenn neue Backups zum System hinzugefügt werden, werden alte Backups aufgrund ihres Alters gelöscht. Derartige Entfernungsvorgänge können in der Regel unter der Kontrolle der Backup- oder Archivierungssoftware durchgeführt werden, basierend auf der konfigurierten Aufbewahrungsfrist.

Falls die Backupsoftware ein altes Backup aus einem Data Domain-System ablaufen lässt oder entfernt, wird der Speicherplatz auf dem Data Domain-System nur verfügbar, wenn das Data Domain-System die Daten der abgelaufenen Backups von der Festplatte löscht. Eine gute Möglichkeit, Speicherplatz auf einem Data Domain-System zu managen, besteht darin, so viele Onlinebackups wie möglich aufzubewahren, wobei der unbelegte Speicherplatz (ca. 20 % des verfügbaren Gesamtspeicherplatzes) bequem Backups bis zur nächsten geplanten Bereinigung, die standardmäßig einmal wöchentlich ausgeführt wird, aufnehmen kann.

Ein Teil der Speicherkapazität wird von Data Domain-Systemen für interne Indizes und andere Metadaten verwendet. Die Menge an Speicher, die im Laufe der Zeit für Metadaten verwendet wird, hängt vom Typ der gespeicherten Daten und Größe der gespeicherten Dateien ab. Bei zwei ansonsten identischen Systemen hat ein System möglicherweise im Laufe der Zeit mehr Speicherplatz für Metadaten reserviert und weniger Speicherplatz für tatsächliche Backupdaten als das andere, wenn verschiedene Datensätze zu jedem System gesendet werden.

Die Speicherplatznutzung auf einem Data Domain-System wird hauptsächlich von folgenden Faktoren beeinflusst:

- Die Größe und Komprimierbarkeit der Backupdaten
- Die in der Backupsoftware angegebene Aufbewahrungsfrist

Hohe Komprimierungslevel werden erzielt, wenn Datasets mit zahlreichen Duplikaten gespeichert und über längere Zeiträume aufbewahrt werden.

Berichte zur Speicherplatznutzung des Dateisystems

Die Speicherkapazität wird in allen Fenstern und Systembefehlen von DD System Manager mithilfe binärer Berechnungen angezeigt. Beispielsweise werden mit einem Befehl, der 1 GiB belegten Speicherplatz anzeigt, 2^{30} Byte =1.073.741.824 Byte gemeldet.

- 1 KiB = 2^{10} = 1.024 Bytes
- 1 MiB = 2^{20} = 1.048.576 Bytes
- 1 GiB = 2^{30} = 1.073.741.824 Bytes
- 1 TiB = 2^{40} = 1.099.511.627.776 Bytes

So verwendet das Dateisystem die Komprimierung

Das Dateisystem verwendet eine Komprimierung, um den verfügbaren Speicherplatz beim Speichern von Daten zu optimieren. Der Speicherplatz wird auf zweierlei Weise berechnet: physisch und logisch. (Weitere Informationen finden Sie im Abschnitt zu den Arten der Komprimierung.) Physischer Speicherplatz ist der tatsächliche Speicherplatz, der im Data Domain-System verwendet wird. Logischer Speicherplatz ist die Menge der nicht komprimierten Daten, die auf das System geschrieben werden.

Die Reportingtools für den Dateisystemspeicherplatz (DD System Manager-Diagramme und der Befehl `filesys show space` oder der Alias `df`) zeigen sowohl den physischen als auch den logischen Speicherplatz an. Diese Tools berichten auch die Größe und die Menge des verwendeten und verfügbaren Speicherplatzes.

Wenn ein Data Domain-System gemountet ist, können die üblichen Tools zum Anzeigen der physischen Speicherplatznutzung eines Dateisystems verwendet werden.

Das Data Domain-System erzeugt Warnmeldungen, wenn das Dateisystem seine maximale Speicherkapazität erreicht. Die folgenden Informationen über die Datenkomprimierung enthalten Richtlinien für die Festplattennutzung über die Zeit.

Die Menge des über die Zeit von einem Data Domain-System verwendeten Speicherplatzes hängt von folgenden Faktoren ab:

- Der Größe des anfänglichen kompletten Backups
- Der Anzahl zusätzlicher Backups (inkrementell und komplett), die über die Zeit aufbewahrt werden
- Der Wachstumsrate des Backup-Dataset
- Der Änderungsrate der Daten

Für Datasets mit typischen Änderungs- und Wachstumsraten entspricht die Datenkomprimierung in der Regel den folgenden Richtlinien:

- Für das erste komplette Backup an ein Data Domain-System liegt der Komprimierungsfaktor normalerweise bei 3:1.
- Für jedes inkrementelle Backup zum ersten kompletten Backup liegt der Komprimierungsfaktor normalerweise in einem Bereich von 6:1.
- Das nächste komplette Backup verfügt über einen Komprimierungsfaktor von etwa 60:1.

Bei einer Planung, die wöchentliche komplette und tägliche inkrementelle Backups umfasst, liegt der aggregierte Komprimierungsfaktor über die Zeit für alle Daten bei rund 20:1. Der Komprimierungsfaktor ist für rein inkrementelle Daten oder für Backups mit weniger doppelten Daten niedriger. Die Komprimierung ist höher, wenn alle Backups komplette Backups sind.

Komprimierungstypen

Data Domain komprimiert Daten auf zwei Leveln: global und lokal. Bei der globalen Komprimierung werden empfangene Daten mit den Daten verglichen, die bereits auf Festplatten gespeichert sind. Doppelte Daten müssen nicht erneut gespeichert werden, während Daten, die neu sind, lokal komprimiert werden, bevor sie auf Festplatte geschrieben werden.

Lokale Komprimierung
Ein Data Domain-System verwendet einen lokalen Komprimierungsalgorithmus, der speziell entwickelt wurde, um den maximalen Durchsatz zu erreichen, während Daten auf die Festplatte geschrieben werden. Der Standardalgorithmus (LZ) ermöglicht

kürzere Backupzeitfenster für Backupjobs, verwendet jedoch mehr Speicherplatz. Es sind zwei andere Arten der lokalen Komprimierung verfügbar: „gzfast“ und „GZ“. Beide bieten eine höhere Komprimierung über „LZ“, jedoch auf Kosten zusätzlicher CPU-Last. Lokale Komprimierungsoptionen bieten einen Kompromiss zwischen langsamerer Performance und Speichernutzung. Es ist auch möglich, die lokale Komprimierung zu deaktivieren. Um die Komprimierung zu ändern, lesen Sie den Abschnitt zum Ändern der lokalen Komprimierung.

Nachdem Sie die Komprimierung geändert haben, verwenden alle neuen Schreibvorgänge den neuen Komprimierungstyp. Vorhandene Daten werden während der Bereinigung in den neuen Komprimierungstyp umgewandelt. Es dauert einige Bereinigungsrunden, um alle Daten neu zu komprimieren, die vor der Komprimierungsänderung vorhanden waren.

Die erste Bereinigung nach der Komprimierungsänderung kann länger als gewöhnlich dauern. Wenn Sie den Komprimierungstyp ändern, überwachen Sie das System eine oder zwei Wochen lang sorgfältig, um zu überprüfen, ob es ordnungsgemäß funktioniert.

Implementierung der Datenintegrität durch das Dateisystem

Mehrere Ebenen der Datenverifizierung werden von dem DD OS-Dateisystem für Daten durchgeführt, die von Backupanwendungen eingehen, um sicherzustellen, dass die Daten korrekt auf die Festplatten des Data Domain-Systems geschrieben werden. Damit wird ermöglicht, dass die Daten ohne Fehler abgerufen werden können.

DD OS ist speziell für Datensicherheit entwickelt und seine Architektur ist für Datenunverletzlichkeit ausgelegt. Das Hauptaugenmerk liegt dabei auf vier wichtigen Bereichen, die in den folgenden Abschnitten beschrieben werden.

End-to-End-Verifizierung

Bei End-to-End-Prüfungen werden alle Dateisystemdaten und Metadaten geschützt. Wenn Daten im System eingehen, wird eine starke Prüfsumme berechnet. Die Daten werden dedupliziert und im Dateisystem gespeichert. Nachdem alle Daten auf die Festplatte geschrieben wurden, werden sie zurückgelesen und erneut mit einer Prüfsumme versehen. Die Prüfsummen werden verglichen, um zu überprüfen, ob die Daten und die Dateisystemmetadaten korrekt gespeichert wurden.

Fehlervermeidung und Fehlerbegrenzung

Data Domain verwendet ein protokollstrukturiertes Dateisystem, das vorhandene Daten niemals überschreibt oder aktualisiert. Neue Daten werden immer in neue Container geschrieben und an die vorhandenen alten Container angehängt. Die alten Container und Referenzen bleiben bestehen und können selbst bei Software- oder Hardwarefehlern geschützt werden, die bei der Speicherung neuer Backups auftreten könnten.

Kontinuierliche Fehlererkennung und Fehlerkorrektur

Kontinuierliche Fehlererkennung und Fehlerkorrektur schützt vor Speichersystemfehlern. Das System überprüft regelmäßig die Integrität der RAID-Stripes und nutzt die Redundanz des RAID-Systems bei der Korrektur eventueller Fehler. Bei einem Lesevorgang wird die Datenintegrität erneut verifiziert und alle Fehler werden direkt behoben.

Wiederherstellbarkeit des Dateisystems

Daten werden in einem selbstbeschreibenden Format geschrieben. Bei Bedarf kann das Dateisystem durch Scannen des Protokolls und Wiederherstellung des Systems auf Basis der mit den Daten gespeicherten Metadaten neu erstellt werden.

Speicherplatzrückgewinnung des Dateisystems mithilfe der Dateisystembereinigung

Wenn Daten in der Backupanwendung (z. B.NetBackup oder NetWorker) ablaufen, werden die Daten zur Löschung durch das Data Domain-System markiert. Die Daten werden jedoch nicht unmittelbar gelöscht, sondern bei der Bereinigung entfernt.

- Während des Bereinigungsvorgangs steht das Dateisystem für den gesamten Normalbetrieb zur Verfügung. Dazu zählen Backups (Schreibvorgänge) und Wiederherstellungen (Lesevorgänge).
- Obwohl die Bereinigung eine erhebliche Anzahl von Systemressourcen beansprucht, verfügt die Bereinigung über eine Eigendrosselung und gibt bei Vorhandensein von Benutzerverkehr Systemressourcen frei.
- Data Domain empfiehlt, einen Bereinigungsvorgang nach dem ersten kompletten Backup auf ein Data Domain-System auszuführen. Die erste lokale Komprimierung auf einem kompletten Backup hat in der Regel einen Faktor von 1,5 bis 2,5. Ein sofortiger Bereinigungsvorgang bietet zusätzliche Komprimierung durch einen weiteren Faktor von 1,15 bis 1,2 und gewinnt entsprechend viel Speicherplatz wieder.
- Wenn der Bereinigungsvorgang abgeschlossen ist, wird eine Meldung in das Systemprotokoll gesendet, die den Prozentsatz von Speicherplatz angibt, der zurückgewonnen wurde.

Eine Standardplanung führt den Bereinigungsvorgang jeden Dienstag um 6 Uhr aus (tue 0600). Sie können die Planung ändern oder den Vorgang manuell ausführen (siehe Abschnitt zum Ändern einer Bereinigungsplanung).

Data Domain empfiehlt, den Bereinigungsvorgang einmal wöchentlich auszuführen.

Jeder Vorgang, der das Dateisystem während einer Bereinigung deaktiviert oder ein Data Domain-System herunterfährt (z. B .eine Systemabschaltung oder ein Neustart), bricht den Bereinigungsvorgang ab. Der Bereinigungsvorgang startet nicht sofort beim Systemneustart neu. Sie können den Bereinigungsvorgang manuell neu starten oder bis zum nächsten geplanten Bereinigungsvorgang warten.

Bei Sammelreplikation können Daten in einem Replikationskontext auf dem Quellsystem, die nicht repliziert wurden, nicht für die Dateisystembereinigung verarbeitet werden. Kann die Dateisystembereinigung nicht abgeschlossen werden, da Quell- und Zielsysteme nicht mehr synchron sind, meldet das System den Status des Bereinigungsvorgangs als `partial` und nur begrenzte Systemstatistiken stehen für die Bereinigung zur Verfügung. Wenn die Sammelreplikation deaktiviert ist, erhöht sich die Menge der Daten, die nicht für die Dateisystembereinigung verarbeitet werden können, da die Quell- und Zielsysteme für die Replikation nicht mehr synchron sind. KB-Artikel *Data Domain: An overview of Data Domain File System (DDFS) clean/garbage collection (GC) phases*, verfügbar auf der Online Support-Website unter https:// support.emc.com bietet weitere Informationen.

Wenn bei der MTree-Replikation eine Datei erstellt und gelöscht wird, während ein Snapshot repliziert wird, verfügt der nächste Snapshot nicht über ausreichend Informationen über diese Datei und das System repliziert keinen Inhalt, der dieser Datei zugeordnet ist. Die Verzeichnisreplikation repliziert sowohl die Erstellung als auch das Löschen, auch wenn sie dicht nacheinander passieren.

Mit dem Replikationsprotokoll, das die Verzeichnisreplikation verwendet, werden Vorgänge wie Löschen, Umbenennen usw. als Single Stream durchgeführt. Dies kann den Replikationsdurchsatz reduzieren. Die Verwendung von Snapshots durch die MTree-Replikation vermeidet dieses Problem.

Unterstützte Schnittstellen

Vom Dateisystem unterstützte Schnittstellen:

- NFS
- CIFS
- DD Boost
- DD VTL

Unterstützte Backupsoftware

Richtlinien zum Einrichten von Backupsoftware und Backupservern für die Verwendung mit Data Domain-Systemen finden Sie unter support.emc.com.

An ein Data Domain-System gesendete Datenstreams

Für eine optimale Performance empfiehlt Data Domain folgende Grenzwerte für gleichzeitige Streams zwischen Data Domain-Systemen und Ihren Backupservern.

Im Kontext der folgenden Tabelle bezieht sich ein Datenstream auf einen großen Bytestream, der mit einem sequenziellen Dateizugriff verknüpft ist, beispielsweise ein Schreibstream zu einer Backupdatei oder ein Lesestream von einem Wiederherstellungs-Image. Ein Replikationsquell- oder -zielstream bezieht sich auf einen Verzeichnisreplikationsvorgang oder einen DD Boost-Dateireplikationsstream, der mit einem Dateireplikationsvorgang verknüpft ist.

Tabelle 87 An ein Data Domain-System gesendete Datenstreams

Modell	RAM/ NVRAM	Backupschreibstreams	Backupslesestreams	Repl[a]-Quellstreams	Repl[a]-Zielstreams	Gemischt
DD140, DD160, DD610	4 GB oder 6 GB/0,5 GB	16	4	15	20	w<= 16 ; r<= 4 ReplSrc<=15; ReplDest<=20; ReplDest+w<=16; w+r+ReplSrc <=16;Total<=20
DD620, DD630, DD640	8 GB/0,5 GB oder 1 GB	20	16	30	20	w<=20; r<=16; ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; Total<=30
DD640, DD670	16 GB oder 20 GB/1 GB	90	30	60	90	w<=90; r<=30; ReplSrc<=60; ReplDest<=90; ReplDest+w<=90; Total<=90
DD670, DD860	36 GB/1 GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD860	72 GB[b]/1 GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90

Tabelle 87 An ein Data Domain-System gesendete Datenstreams (Fortsetzung)

Modell	RAM/ NVRAM	Backupschreibstreams	Backuplesestreams	Repl[a]-Quellstreams	Repl[a]-Zielstreams	Gemischt
DD890	96 GB/2 GB	180	50	90	180	w<=180; r<=50; ReplSrc <=90;ReplDest<=180; ReplDest +w<=180; Total<=180
DD990	128 oder 256 GB[b]/4 GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD2200	8 GB	20	16	16	20	w<=20; r<=16; ReplSrc<=16; ReplDest<=20; ReplDest+w<=20; Total<=20
DD2200	16 GB	60	16	30	60	w<=60; r<=16; ReplSrc<=30; ReplDest<=60; ReplDest+w<=60; Total<=60
DD2500	32 GB oder 64 GB/2 GB	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; Total<=180
DD4200	128 GB[b]/4 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD4500	192 GB[b]/4 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD7200	128 oder 256 GB[b]/4 GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD9500	256/512 GB	1.885	300	540	1.080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest+w<=1080; Total<=1885
DD9800	256/768 GB	1.885	300	540	1.080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest+w<=1080; Total<=1885
DD6300	48/96 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD6800	192 GB	400	110	220	400	w<=400; r<=110; ReplSrc<=220; ReplDest<=400; ReplDest +w<=400; Total<=400
DD9300	192/384 GB	800	220	440	800	w<=800; r<=220; ReplSrc<=440; ReplDest<=800; ReplDest +w<=800; Total<=800
Data Domain Virtual Edition (DD VE)	6 TB oder 8 TB oder 16 TB/ 0,5 TB oder 32 TB oder	16	4	15	20	w<= 16 ; r<= 4 ReplSrc<=15; ReplDest<=20; ReplDest+w<=16; w+r+ReplSrc <=16;Total<=20

Tabelle 87 An ein Data Domain-System gesendete Datenstreams (Fortsetzung)

Modell	RAM/ NVRAM	Backupsc hreibstrea ms	Backuples estreams	Repl[a]- Quellstrea ms	Repl[a]- Zielstrea ms	Gemischt
	48 TB oder 64 TB oder 96 TB					

a. DirRepl, OptDup, MTreeRepl-Streams
b. Die Data Domain Extended Retention-Softwareoption ist für diese Geräte nur mit erweitertem (maximalem) Arbeitsspeicher verfügbar.

Einschränkungen des Dateisystems

Dateisystemeinschränkungen, einschließlich: Beschränkungen im Hinblick auf die Anzahl der Dateien, den Akku usw.

Begrenzungen für die Anzahl von Dateien in einem Data Domain-System

Beachten Sie bei der Speicherung von mehr als 1 Milliarde Dateien folgende Konsequenzen und Überlegungen.

Data Domain empfiehlt, nicht mehr als 1 Milliarde Dateien auf einem System zu speichern. Das Speichern einer größeren Anzahl von Dateien kann die Performance und die Dauer für die Bereinigung beeinträchtigen und einige Prozesse wie die Dateisystembereinigung nimmt bei einer sehr großen Anzahl von Dateien viel mehr Zeit in Anspruch. Beispielsweise kann die Enumerationsphase der Bereinigung je nach Anzahl von Dateien im System von einigen Minuten bis zu mehreren Stunden dauern.

Hinweis

Die Gesamtperformance für das Data Domain-System fällt auf ein inakzeptables Niveau, wenn das System die maximale Dateimenge unterstützen muss und der Workload von den Clientrechnern nicht sorgfältig kontrolliert wird.

Wenn das Dateisystem die Grenze von einer Milliarde Dateien überschreitet, werden mehrere Prozesse oder Vorgänge beeinträchtigt, darunter die folgenden:

- Die Bereinigung kann sehr viel Zeit in Anspruch nehmen, möglicherweise sogar einige Tage.
- AutoSupport-Vorgänge dauern möglicherweise länger.
- Es ist jeder Prozess betroffen, der alle Dateien enumerieren muss.

Wenn eine große Anzahl kleiner Dateien vorhanden ist, müssen andere Überlegungen berücksichtigt werden:

- Die Anzahl der separaten Dateien, die pro Sekunde erstellt werden können, ist möglicherweise (selbst wenn die Dateien sehr klein sind) eine größere Einschränkung als die Anzahl der MB/s, die in ein Data Domain-System verschoben werden können. Wenn Dateien groß sind, hat die Dateierstellungsrate keine Bedeutung, aber wenn Dateien klein sind, ist die Dateierstellungsrate dominant und kann zu einem Faktor werden. Die Dateierstellungsrate liegt je nach Anzahl von MTrees und CIFS-Verbindungen bei rund 100 bis 200 Dateien pro Sekunde. Diese Rate sollte bei der Systemdimensionierung berücksichtigt werden,

wenn eine Massenaufnahme einer großen Anzahl von Dateien in einer Kundenumgebung erforderlich ist.

- Dateizugriffslatenzen werden durch die Anzahl der Dateien in einem Verzeichnis beeinträchtigt. Es wird empfohlen, soweit möglich Verzeichnisgrößen von weniger als 250.000 einzuhalten. Bei größeren Verzeichnisgrößen kommt es evtl. zu langsameren Antworten auf Metadatenvorgänge wie das Auflisten der Dateien im Verzeichnis und das Öffnen oder Erstellen einer Datei.

Einschränkungen hinsichtlich des Akkus

Bei Systemen, die NVRAM verwenden, erzeugt das Betriebssystem eine Warnmeldung, wenn die Akkuladung unter 80 % der Kapazität fällt. In diesem Fall wird das Dateisystem deaktiviert.

HINWEIS

Das Data Domain DD2200-System verwendet NVRAM nicht, sodass durch Firmwareberechnungen entschieden wird, ob die Akkuladung ausreicht, um die Daten zu speichern. Das Dateisystem wird deaktiviert, wenn es zu einem Verlust von Wechselstrom kommt.

Maximale Anzahl unterstützter Inodes

Eine NFS- oder CIFS-Clientanforderung führt dazu, dass ein Data Domain-System eine Kapazität von etwa zwei Milliarden Inodes meldet (Dateien und Verzeichnisse). Ein Data Domain-System kann diese Zahl überschreiten, aber das Reporting auf dem Client ist dann möglicherweise nicht korrekt.

Maximale Länge des Pfadnamens

Die maximale Länge eines vollständigen Pfadnamens (einschließlich der Zeichen in `/data/col1/backup`) beträgt 1.023 Byte. Die maximale Länge des symbolischen Links beträgt ebenfalls 1.023 Byte.

Eingeschränkter Zugriff während eines HA-Failover

Der Zugriff auf Dateien kann während eines Failover auf HA-Systemen bis zu 10 Minuten unterbrochen sein. (DD Boost und NFS erfordern zusätzlich Zeit.)

Überwachen der Dateisystemnutzung

Zeigen Sie Echtzeitstatistiken zum Datenspeicher an.

Die Dateisystemansicht verfügt über Registerkarten und Steuerelemente, die Zugriff auf die Datenspeicherstatistiken in Echtzeit, Cloudspeichereinheitinformationen, Verschlüsselungsinformationen und Diagramme zum Umfang der Speicherplatznutzung, zu Verbrauchsfaktoren und zu Trends zu geschriebenen Daten ermöglichen. Des Weiteren finden Sie hier einige Steuerelemente für das Managen der Dateisystembereinigung, der Erweiterung, des Kopiervorgangs und der Löschung.

Zugreifen auf die Ansicht „File System“

In diesem Abschnitt wird die Dateisystemfunktion beschrieben.

Vorgehensweise

- Wählen Sie **Data Management** > **File System**

Informationen über den Bereich „File System Status“

Zeigt den Status der Dateisystemservices.

Wenn Sie auf den Bereich „File System Status“ zugreifen möchten, klicken Sie auf **Data Management** > **File System** > **Show Status of File System Services**.

Dateisystem
Das Feld **File System** enthält einen Link **Enable/Disable** und zeigt den Betriebsstatus des Dateisystems an.

- Enabled and running – und die längste aufeinanderfolgende Dauer, über die das Dateisystem aktiv war.
- Disabled and shutdown.
- Enabling and disabling – im Begriff, aktiviert bzw. deaktiviert zu werden.
- Destroyed – wenn das Dateisystem gelöscht wurde.
- Error – wenn ein Fehler auftritt, wie z. B. ein Problem bei der Initialisierung des Dateisystems.

Cloud File Recall
Das Feld **Cloud File Recall** enthält den Link **Recall** zum Initiieren eines Dateiabrufs vom Cloud-Tier. Der Link **Details** ist verfügbar, wenn aktive Abrufe vorhanden sind. Weitere Informationen finden Sie im Thema „Abrufen einer Datei aus dem Cloud-Tier“.

Messungen der physischen Kapazität
Das Feld **Physical Capacity Measurement** enthält die Schaltfläche **Enable**, wenn der Status der physischen Kapazitätsmessung deaktiviert ist. Wenn diese Option aktiviert ist, zeigt das System die Schaltflächen **Disable** und **View** an. Klicken Sie auf **View**, um die derzeit ausgeführten physischen Kapazitätsmessungen anzuzeigen: MTree, Priority, Submit Time, Start Time und Duration.

Datenverschiebung
Das Feld **Data Movement** enthält die Schaltflächen **Start/Stop** und zeigt das Datum der letzten abgeschlossenen Datenverschiebung, die Anzahl der kopierten Dateien und die Menge an kopierten Daten an. Das System zeigt die Schaltfläche **Start** an, wenn die Datenverschiebung verfügbar ist, und **Stop**, wenn eine Datenverschiebung ausgeführt wird.

Bereinigung des aktiven Tier
Das Feld **Active Tier Cleaning** enthält eine Schaltfläche **Start/Stop** und zeigt das Datum des letzten Bereinigungsvorgangs oder den aktuellen Bereinigungsstatus an, wenn der Bereinigungsvorgang derzeit ausgeführt wird. Beispiel:

```
Cleaning finished at 2009/01/13 06:00:43
```

oder, wenn das Dateisystem deaktiviert ist, wird Folgendes angezeigt:

```
Nicht verfügbar
```

Bereinigung des Cloud-Tier
Das Feld **Cloud Tier Cleaning** enthält eine Schaltfläche **Start/Stop** und zeigt das Datum des letzten Bereinigungsvorgangs oder den aktuellen Bereinigungsstatus an, wenn der Bereinigungsvorgang derzeit ausgeführt wird. Beispiel:

```
Cleaning finished at 2009/01/13 06:00:43
```

oder, wenn das Dateisystem deaktiviert ist, wird Folgendes angezeigt:

```
Nicht verfügbar
```

Informationen über die Registerkarte „Summary“

Klicken Sie auf die Registerkarte „Summary“, um die Statistiken zur Speichernutzung für aktive und Cloud-Tiers anzuzeigen und auf Steuerelemente für die Anzeige des Dateisystemstatus, die Konfiguration von Dateisystemeinstellungen, das Durchführen eines FastCopy-Vorgangs, das Erweitern der Kapazität und das Entfernen des Dateisystems zuzugreifen.

Für jeden Tier umfassen die Statistiken zur Speichernutzung Folgendes:

- **Size** – Gesamtmenge des physischen Laufwerkspeichers, der für Daten verfügbar ist.
- **Used** – Physischer Speicherplatz, der für komprimierte Daten verwendet wird. Warnmeldungen werden an das Systemprotokoll gesendet und es wird eine E-Mail-Warnmeldung erzeugt, wenn die Nutzung die Werte 90 %, 95 % und 100 % erreicht. Bei 100 % nimmt das Data Domain-System keine weiteren Daten von den Backupservern an.
  Wenn die Menge für „Used“ immer hoch ist, prüfen Sie in der Bereinigungsplanung, wie oft der Bereinigungsvorgang automatisch ausgeführt wird. Verwenden Sie dann das Verfahren zur Änderung einer Bereinigungsplanung, um den Vorgang öfter auszuführen. Ziehen Sie auch eine Reduzierung der Datenaufbewahrungsfrist oder eine Abspaltung eines Teils der Backupdaten auf ein anderes Data Domain-System in Erwägung.
- **Available** (GiB) – Gesamtmenge des für Datenspeicher verfügbaren Speicherplatzes. Diese Zahl kann sich ändern, da ein interner Index erweitert werden kann, wenn das Data Domain-System mit Daten gefüllt wird. Die Indexerweiterung reduziert den unter „Avail GiB“ angegebenen Speicherplatz.
- **Pre-Compression** (GiB) – Vor der Komprimierung geschriebene Daten.
- **Total Compression Factor (Reduction %)** – Vor der Komprimierung/nach der Komprimierung.
- **Cleanable** (GiB) – Speicherplatz, der zurückgewonnen werden kann, wenn eine Bereinigung ausgeführt wird.

Für den Cloud-Tier enthält das Feld **Cloud File Recall** den Link **Recall** zum Initiieren eines Dateiabrufs aus dem Cloud-Tier. Der Link **Details** ist verfügbar, wenn aktive Abrufe vorhanden sind. Weitere Informationen finden Sie im Thema „Abrufen einer Datei aus dem Cloud-Tier“.

Separate Bereiche bieten die folgenden Statistiken für die letzten 24 Stunden für jeden Tier:

- **Pre-Compression** (GiB) – Vor der Komprimierung geschriebene Daten.
- **Post-Compression** (GiB) – Nach der Komprimierung verwendeter Speicher.
- **Global Compression Factor** – Vor der Komprimierung/Größe nach der globalen Komprimierung.
- **Local Compression Factor** – Größe nach der globalen Komprimierung/nach der Komprimierung.
- **Total Compression Factor (Reduction %)** – [(vor der Komprimierung - nach der Komprimierung)/vor der Komprimierung] * 100.

Informationen über Dateisystemeinstellungen

Sie können Systemoptionen sowie die aktuelle Bereinigungsplanung anzeigen und ändern.

Klicken Sie zum Zugriff auf das Dialogfeld der Dateisystemeinstellungen auf **Data Management** > **File System** > **Settings**.

Tabelle 88 Allgemeine Einstellungen

Allgemeine Einstellungen	Beschreibung
Local Compression Type	Der Typ der verwendeten lokalen Komprimierung. • Eine Übersicht finden Sie im Abschnitt zu den Komprimierungstypen. • Weitere Informationen finden Sie im Abschnitt zur Änderung der lokalen Komprimierung.
Cloud Tier Local Comp	Typ der Komprimierung, der für den Cloud-Tier verwendet wird. • Eine Übersicht finden Sie im Abschnitt zu den Komprimierungstypen. • Weitere Informationen finden Sie im Abschnitt zur Änderung der lokalen Komprimierung.
Report Replica as Writable	So wird Anwendungen ein Replikat angezeigt. • Weitere Informationen finden Sie im Abschnitt zur Änderung der Schreibschutzeinstellungen.
Staging Reserve	Verwalten der Laufwerksbereitstellung. • Weitere Informationen finden Sie im Abschnitt zur Arbeit mit der Laufwerksbereitstellung. • Weitere Informationen finden Sie im Abschnitt zur Konfiguration der Laufwerksbereitstellung.
Marker Type	Markierungen der Backupsoftware (es werden Bandmarkierungen, Tag-Kopfzeilen oder andere Namen verwendet) in den Datenstreams. Weitere Informationen finden Sie im Abschnitt zu den Einstellungen der Bandmarkierungen.
Throttle	Weitere Informationen finden Sie im Abschnitt zum Festlegen der Drosselung für die Messung der physischen Kapazität.
Cache	Bei der Initialisierung des physischen Kapazitätscache werden die Caches bereinigt und die Messgeschwindigkeit wird optimiert.

Sie können den Workload-Ausgleich des Dateisystems zur Steigerung der Performance basierend auf Ihrer Nutzung anpassen.

Tabelle 89 Einstellungen des Workload-Ausgleichs

Einstellungen des Workload-Ausgleichs	Beschreibung
Random workloads (%)	Sofortiger Zugriff und Wiederherstellungen erzielen durch die Verwendung zufälliger Workloads eine bessere Performance.
Sequential workloads (%)	Herkömmliche Backups und Wiederherstellungen erzielen durch sequenzielle Workloads eine bessere Performance.

Tabelle 90 Einstellungen der Datenverschiebung

Einstellungen der Datenverschiebungs-Policy	Beschreibung
File Age Threshold	Wenn die Datenverschiebung beginnt, werden alle Dateien, die nicht in der im Schwellenwert angegebenen Anzahl von Tagen geändert wurden, aus dem aktiven in den Aufbewahrungs-Tier verschoben.
Schedule	Tag- und Uhrzeitdaten werden verschoben.
Throttle	Der Prozentsatz der verfügbaren Ressourcen, die das System für die Datenverschiebung verwendet. Der Drosselungswert 100 % ist die Standardeinstellung der Drosselung und bedeutet, dass die Datenverschiebung nicht gedrosselt wird.

Tabelle 91 Einstellungen der Bereinigung

Einstellungen der Bereinigungsplanung	Beschreibung
Zeit	Die Uhrzeit, wann der Bereinigungsvorgang ausgeführt wird. • Weitere Informationen finden Sie im Abschnitt zur Änderung einer Bereinigungsplanung.
Throttle	Die Ressourcenzuweisung des Systems. • Weitere Informationen finden Sie im Abschnitt zur Drosselung eines Bereinigungsvorgangs.

Informationen über die Registerkarte „Cloud Units“

Zeigt zusammenfassende Informationen über Cloudeinheiten, das Hinzufügen und Ändern von Cloudeinheiten und Managen von Zertifikaten an.

Die Registerkarte „Cloud Units“ auf der Seite „File System“ wird nur angezeigt, wenn die optionale DD Cloud Tier-Lizenz aktiviert ist. In dieser Ansicht werden zusammenfassende Informationen (Status, Netzwerkbandbreite, Lesezugriff, lokale Komprimierung, Datenverschiebung und Datenstatus), der Name des Cloudanbieters, die genutzte Kapazität und die lizenzierte Kapazität aufgelistet. Für die Bearbeitung der Cloudeinheit, das Managen von Zertifikaten und das Hinzufügen einer neuen Cloudeinheit werden Steuerelemente bereitgestellt.

Informationen über die Registerkarte „Retention Units“

Zeigen Sie Aufbewahrungseinheiten sowie deren Zustand, Status und Größe an.

Die Registerkarte „Retention Units“ auf der Seite „File System“ wird nur angezeigt, wenn die optionale DD Lizenz zur erweiterten Aufbewahrung aktiviert ist. In dieser Ansicht wird die Aufbewahrungseinheit aufgelistet, zudem werden ihr Zustand (neu, versiegelt oder Ziel), ihr Status (deaktiviert oder bereit) und ihre Größe angezeigt. Wenn die Einheit versiegelt wurde, was bedeutet, dass keine Daten mehr hinzugefügt werden können, wird das Datum angegeben, an dem sie versiegelt wurde.

Wählen Sie das rautenförmige Symbol rechts neben einer Spaltenüberschrift aus, um die Reihenfolge der Werte in umgekehrter Richtung zu sortieren.

Informationen über die Registerkarte „DD Encryption“

Zeigen Sie Status, Fortschritt, Algorithmen usw. einer Verschlüsselung an.

Tabelle 92 DD-Verschlüsselungseinstellungen

Einstellung	Beschreibung
DD System	Die folgenden Status sind möglich: • Not licensed: Es werden keine weiteren Informationen bereitgestellt. • Not configured: Die Verschlüsselung ist lizenziert, aber nicht konfiguriert. • Enabled: Die Verschlüsselung ist aktiviert und wird ausgeführt. • Disabled: Die Verschlüsselung ist deaktiviert.
Active Tier	Anzeigen des Verschlüsselungsstatus für den aktiven Tier: • Enabled: Die Verschlüsselung ist aktiviert und wird ausgeführt. • Disabled: Die Verschlüsselung ist deaktiviert.
Cloud Unit	Anzeigen des Verschlüsselungsstatus anhand der Cloudeinheit: • Enabled: Die Verschlüsselung ist aktiviert und wird ausgeführt. • Disabled: Die Verschlüsselung ist deaktiviert.
Encryption Progress	Zeigen Sie Details zum Verschlüsselungsstatus für den aktiven Tier in Bezug auf die Anwendung von Änderungen und die erneute Verschlüsselung von Daten an. Die folgenden Status sind möglich: • None • Pending • Running • Done Klicken Sie auf „View Details“, um das Dialogfeld „Encryption Status Details“ anzuzeigen, in dem Sie die folgenden Informationen für den aktiven Tier finden: • Type (Beispiel: Wenden Sie Änderungen an, wenn die Verschlüsselung bereits initialisiert wurde oder wenden Sie die erneute Verschlüsselung an, wenn die Verschlüsselung das

Tabelle 92 DD-Verschlüsselungseinstellungen (Fortsetzung)

Einstellung	Beschreibung
	Ergebnis von zuvor beschädigten Daten ist – beispielsweise bei einem zuvor beschädigten Schlüssel.) • Status (Beispiel: Pending) • Details: (Beispiel: Angefordert am xx/xx/xx Dezember und Übernahme nach der nächsten Systembereinigung.)
Encryption Algorithm	Der für die Verschlüsselung der Daten verwendete Algorithmus: • AES 256-Bit (CBC) (Standard) • AES 256-Bit (GCM) (sicherer, aber langsamer) • AES 128-Bit (CBC) (nicht so sicher wie 256-Bit) • AES 128-Bit (GCM) (nicht so sicher wie 256-Bit) Ausführliche Informationen finden Sie unter „Ändern des Verschlüsselungsalgorithmus“.
Encryption Passphrase	Wenn sie konfiguriert ist, wird sie als „*****“ angezeigt. Informationen zum Ändern der Passphrase finden Sie unter „Managen der System-Passphrase“.
File System Lock	
Status	Die Dateisystemsperre kann die folgenden Status haben: • Unlocked: Die Funktion ist nicht aktiviert. • Locked: Die Funktion ist aktiviert.
Key Management	
Key Manager	Entweder der in Data Domain integrierte Key Manager oder der optionale RSA Data Protection Manager (DPM) Key Manager. Klicken Sie auf **Configure**, um zwischen den Key Managern zu wechseln (wenn beide konfiguriert sind) oder die Key Manager-Optionen zu ändern.
Server	Name des RSA Key Manager-Servers
Server Status	Online oder offline oder die vom RSA Key Manager-Server zurückgegebenen Fehlermeldungen
Key Class	Eine spezielle Art von Sicherheitsklasse, die vom optionalen RSA Data Protection Manager (DPM) Key Manager verwendet wird, der kryptografische Schlüssel mit ähnlichen Eigenschaften gruppiert. Das Data Domain-System ruft einen Schlüssel vom RSA-Server nach Schlüsselklasse ab. Eine einzurichtende Schlüsselklasse, um entweder den aktuellen Schlüssel zurückzugeben oder jedes Mal einen neuen Schlüssel zu erzeugen. **Hinweis** Das Data Domain-System unterstützt nur Schlüsselklassen, die so konfiguriert sind, dass sie den aktuellen Schlüssel zurückgeben.
Port	Portnummer des RSA-Servers

Tabelle 92 DD-Verschlüsselungseinstellungen (Fortsetzung)

Einstellung	Beschreibung
FIPS mode	Ob das importierte Hostzertifikat FIPS-vorgabenkonform ist oder nicht. Der Standardmodus ist „Enabled“.
Encryption Keys	Listet Schlüssel nach ID-Nummern auf. Zeigt an, wann ein Schlüssel erstellt wurde, wie lange er gültig ist, seinen Typ (RSA DPM Key Manager oder der interne Data Domain)-Schlüssel, seinen Status (siehe „Arbeiten mit dem RSA DPM Key Manager“ und „Von Data Domain unterstützte DPM-Chiffrierschlüsselstatus) und die Menge der mit dem Schlüssel verschlüsselten Daten. Das System zeigt den zuletzt aktualisierten Zeitpunkt für Schlüsselinformationen über der rechten Spalte an. In der Liste können die folgenden Schlüssel ausgewählt werden: • „Synchronized“, sodass in der Liste neue Schlüssel angezeigt werden, die dem RSA-Server hinzugefügt wurden (aber erst verwendet werden können, wenn das Dateisystem neu gestartet wurde). • Deleted. • Destroyed.

Informationen über die Ansicht „Space Usage“ (Dateisystem)

Sie können eine visuelle (statische) Darstellung der Datennutzung für das Dateisystem zu bestimmten Points-in-Time anzeigen.

Klicken Sie auf **Data Management** > **File System** > **Charts**. Wählen Sie **Space Usage** aus der Drop-down-Liste „Charts“ aus.

Klicken Sie auf einen Punkt auf der Linie des Diagramms, um Daten für diesen Punkt anzuzeigen. Die Linien des Diagramms bezeichnen die Messungen für folgende Elemente:

- Pre-Comp Written: Die Gesamtdatenmenge der an den MTree vom Backupserver gesendeten Daten. Daten vor der Komprimierung auf einem MTree sind das, was der Backupserver als die Gesamtmenge unkomprimierter Daten erkennt, die in einem als Speichereinheit verwendeten MTree enthalten sind, wobei der Speicherplatz (links) auf der vertikalen Achse des Diagramms angezeigt wird.
- Post-comp Used: Die Gesamtmenge des auf dem MTree verwendeten Speicherplatzes, angezeigt auf der vertikalen Achse „Space Used“ (links) des Diagramms
- Comp Factor: Die Menge der Komprimierung, die das Data Domain-System mit den empfangenen Daten durchgeführt hat (Komprimierungsverhältnis), angezeigt auf der vertikalen Achse „Compression Factor“ (rechts) des Diagramms.

Überprüfen des Verlaufs der Speicherplatznutzung
In der Grafik „Space Usage“ können Sie durch Klicken auf einen Datumsbereich (d. h. „1w“, „1m“, „3m“, „1y“ oder „All“) über der Grafik die Anzahl der Tage der in der Grafik angezeigten Daten von einer Woche bis hin zu allen Daten ändern.

Informationen über die Ansicht „Consumption“

Zeigen Sie den über einen bestimmten Zeitraum verwendeten Speicherplatz im Verhältnis zur Gesamtsystemkapazität an.

Klicken Sie auf **Data Management** > **File System** > **Charts**. Wählen Sie in der Drop-down-Liste „Chart“ die Option **Consumption** aus.

Klicken Sie auf einen Punkt auf der Linie des Diagramms, um Daten für diesen Punkt anzuzeigen. Die Linien des Diagramms bezeichnen die Messungen für folgende Elemente:

- „Capacity“ ist die Gesamtmenge des verfügbaren Festplattenspeichers für Daten im Data Domain-System. Die Menge wird mit der vertikalen Diagrammachse des Diagramms („Space Used“, links) angezeigt. Wenn Sie auf das Kontrollkästchen „Capacity“ klicken, wird die Linie ein- und ausgeblendet.
- „Post-comp“ bezeichnet die Gesamtmenge des auf dem Data Domain-System genutzten Festplattenspeichers. Wird im Verhältnis zur vertikalen Diagrammachse des genutzten Speicherplatzes („Space Used“, links) angezeigt.
- „Comp Factor“ bezeichnet die Menge der vom Data Domain-System komprimierten, empfangenen Daten (Komprimierungsverhältnis). Wird im Verhältnis zur vertikalen Diagrammachse des Komprimierungsfaktors („Comp Factor“, rechts) angezeigt.
- „Cleaning“: Ein graues rautenförmiges Symbol wird jedes Mal im Diagramm angezeigt, wenn ein Bereinigungsvorgang für das Dateisystem gestartet wurde.
- „Data Movement“ ist die Menge des Festplattenspeichers, der in den Archivierungsspeicherbereich verschoben wurde (wenn die Archivlizenz aktiviert ist).

Überprüfen der historischen Speicherplatznutzung
In der Grafik „Consumption“ können Sie durch Klicken auf einen Datumsbereich (d. h. „1w“, „1m“, „3m“, „1y“ oder „All“) über der Grafik die Anzahl der Tage der in der Grafik angezeigten Daten von einer Woche bis hin zu allen Daten ändern.

Informationen über die Ansicht „Daily Written“ (Dateisystem)

Zeigt den Datenfluss im Lauf der Zeit. Die über einen bestimmten Zeitraum dargestellten Datenmengen beziehen sich auf vor- und nachkomprimierte Daten.

Klicken Sie auf **Data Management** > **File System** > **Charts**. Wählen Sie **Daily Written** aus der Drop-down-Liste „Charts“ aus.

Klicken Sie auf einen Punkt auf der Linie des Diagramms, um ein Feld mit den Daten für diesen Punkt anzuzeigen. Die Linien des Diagramms bezeichnen die Messungen für folgende Elemente:

- Pre-Comp Written: Die Gesamtmenge der Daten, die von Backupservern auf das Dateisystem geschrieben wurden. Vorkomprimierte Daten auf dem Dateisystem werden einem Backupserver als die Gesamtmenge der nicht komprimierten Daten angezeigt, die in einem Dateisystem gespeichert werden.
- Post-Comp Written: Die Gesamtmenge der Daten, die nach der Komprimierung auf das Dateisystem geschrieben wurden, dargestellt in GiB.
- Total Comp Factor: Der Gesamtbetrag der Komprimierung, die das Data Domain-System mit den empfangenden Daten durchgeführt hat (Komprimierungsrate), angezeigt mit dem Gesamtkomprimierungsfaktor (rechts) als vertikale Achse der Grafik.

Prüfen von historischen geschriebenen Daten
In der Grafik „Daily Written“ können Sie durch Klicken auf einen Datumsbereich (d. h. „1w“, „1m“, „3m“, „1y“ oder „All“) über der Grafik die Anzahl der Tage der in der Grafik angezeigten Daten von einer Woche bis hin zu allen Daten ändern.

Wenn das Dateisystem voll oder fast voll ist

Data Domain-Systeme haben drei steigende Levels der Belegung. Beim Erreichen eines Levels sind jeweils mehr Vorgänge nicht mehr zulässig. Auf jedem Level kann durch Löschen von Daten und Ausführen einer Dateisystembereinigung Speicherplatz freigegeben werden.

Hinweis

Durch das Löschen von Dateien und Snapshots wird nicht sofort Speicherplatz zurückgewonnen; dies geschieht erst beim nächsten Bereinigungsvorgang.

- Ebene 1: Auf der ersten Ebene der Belegung, können keine neuen Daten auf das Dateisystem geschrieben werden. Es wird eine informative Warnmeldung zum mangelnden Speicherplatz erzeugt.
  Abhilfe: Löschen Sie nicht benötigte Datensätze, reduzieren Sie die Aufbewahrungsfrist, löschen Sie Snapshots und führen Sie eine Dateisystembereinigung durch.
- Ebene 2: Auf der zweiten Ebene der Belegung, können Dateien nicht gelöscht werden. Das ist darauf zurückzuführen, dass das Löschen von Dateien auch freien Speicherplatz benötigt, aber das System über so wenig freien Speicher verfügt, dass es noch nicht einmal Dateien löschen kann.
  Abhilfe: Lassen Sie Snapshots ablaufen und führen Sie eine vollständige Dateisystembereinigung durch.
- Ebene 3: Auf der dritten und letzten Ebene der Belegung schlagen Versuche, Snapshots ablaufen zu lassen, Dateien zu löschen oder neue Daten zu schreiben fehl.
  Abhilfe: Führen Sie eine Dateisystembereinigung durch, um genügend Speicherplatz freizugeben, damit Sie zumindest einige Dateien löschen oder einige Snapshots ablaufen lassen und die Bereinigung dann erneut ausführen können.

Überwachen der Speicherplatznutzung mit E-Mail-Warnmeldungen

Warnmeldungen werden erzeugt, wenn das Dateisystem bis 90 %, 95 % und 100 % ausgelastet ist. Um diese Warnmeldungen zu senden, fügen Sie den Benutzer zu der Warnmeldungs-E-Mail-Liste hinzu.

Hinweis

Informationen zum Hinzufügen zur Warnmeldungs-E-Mail-Liste finden Sie unter „Anzeigen und Löschen von Warnmeldungen“.

Managen von Dateisystemvorgängen

In diesem Abschnitt wird die Durchführung von Dateisystembereinigungen und allgemeinen Vorgängen beschrieben.

Durchführen grundlegender Vorgänge

Zu den grundlegenden Dateisystemvorgängen gehören das Aktivieren und Deaktivieren des Dateisystems und, in seltenen Fällen, das Löschen eines Dateisystems.

Erstellen des Dateisystems

Erstellen Sie ein Dateisystem auf der Seite „Data Management“ > „File System“ unter Verwendung der Registerkarte „Summary“.

Es gibt drei Gründe, ein Dateisystem zu erstellen:

- für ein neues Data Domain-System
- wenn ein System nach einer Neuinstallation gestartet wird
- nachdem ein Dateisystem zerstört wurde

So erstellen Sie das Dateisystem:

Vorgehensweise

1. Vergewissern Sie sich, dass Speicher installiert und konfiguriert wurde (weitere Informationen finden Sie im Abschnitt zur Anzeige von Systemspeicherinformationen). Wenn das System diese Voraussetzung nicht erfüllt, wird eine Warnmeldung angezeigt. Installieren und konfigurieren Sie den Speicher, bevor Sie versuchen, das Dateisystem zu erstellen.
2. Wählen Sie **Data Management** > **File System** > **Summary** > **Create** aus.

   Der File System Create Wizard wird gestartet. Folgen Sie den bereitgestellten Anweisungen.

Aktivieren oder Deaktivieren des Dateisystems

Die Option zum Aktivieren oder Deaktivieren des Dateisystems hängt vom aktuellen Status des Dateisystems ab – ist es aktiviert, können Sie es deaktivieren und umgekehrt.

- Durch die Aktivierung des Dateisystems können Data Domain-Systemvorgänge gestartet werden. Diese Funktion ist nur für Administratorbenutzer verfügbar.
- Durch die Deaktivierung des Dateisystems werden alle Data Domain-Systemvorgänge, einschließlich der Bereinigung, angehalten. Diese Funktion ist nur für Administratorbenutzer verfügbar.

⚠ ACHTUNG

Wird das Dateisystem deaktiviert, wenn eine Backupanwendung Daten an das System sendet, kann der Backupprozess fehlschlagen. Einige Backupsoftwareanwendungen können wiederhergestellt werden, indem sie an der entsprechenden Stelle neu gestartet werden, wenn sie das Kopieren von Dateien erfolgreich fortsetzen können. Andere schlagen möglicherweise fehl und hinterlassen dem Benutzer ein unvollständiges Backup.

Vorgehensweise

1. Wählen Sie **Data Managment** > **File System** > **Summary** aus.
2. Wählen Sie für **File System** die Option **Enable** oder **Disable** aus.
3. Klicken Sie im Bestätigungsdialogfeld auf **Close**.

Erweitern des Dateisystems

Sie müssen möglicherweise die Größe eines Dateisystems erweitern, wenn Sie mithilfe der Vorschläge aus dem Abschnitt „Wenn das Dateisystem voll oder fast voll ist“ nicht genug Speicherplatz für normale Vorgänge freigeben können.

Ein Dateisystem kann möglicherweise jedoch aus folgenden Gründen nicht erweitert werden:

- Das Dateisystem ist nicht aktiviert.
- In den aktiven, Aufbewahrungs- oder Cloud-Tiers befinden sich nicht verwendete Laufwerke oder Gehäuse.
- Eis ist keine Lizenz für erweiterten Speicher installiert.
- Es sind nicht genügend Kapazitätslizenzen installiert.

DD6300-Systeme unterstützen die Option zur Verwendung von ES30-Gehäusen mit 4-TB-Laufwerken (43,6 TiB) bei 50 % Auslastung (21,8 TiB) im aktiven Tier, wenn die verfügbare lizenzierte Kapazität genau 21,8 TiB beträgt. Die folgenden Richtlinien gelten für die Verwendung von partiellen Kapazitätseinschüben.

- Für die Verwendung von partieller Kapazität werden keine anderen Gehäusetypen oder Laufwerksgrößen unterstützt.
- Ein partieller Einschub kann nur im aktiven Tier vorhanden sein.
- Im aktiven Tier kann nur ein partieller ES30 vorhanden sein.
- Sobald ein partieller Einschub in einem Tier vorhanden ist, können keine zusätzlichen ES30s in diesem Tier konfiguriert werden, bis der partielle Einschub bei voller Kapazität hinzugefügt wird.

  Hinweis

  Dies erfordert die Lizenzierung von ausreichend zusätzlicher Kapazität, um die verbleibenden 21,8 TiB des partiellen Einschubs zu verwenden.

- Wenn die verfügbare Kapazität 21,8 TB überschreitet, kann kein partieller Einschub hinzugefügt werden.
- Das Löschen einer 21-TiB-Lizenz konvertiert einen vollständig genutzen Einschub nicht automatisch in einen partiellen Einschub. Der Einschub muss entfernt und wieder als partieller Einschub hinzugefügt werden.

So erweitern Sie das Dateisystem:

Vorgehensweise

1. Wählen Sie **Data Managment** > **File System** > **Summary** > **Expand Capacity** aus.

   Die Expand File System Capacity Wizard wird gestartet. Die Drop-down-Liste **Storage Tier** enthält immer den aktiven Tier und kann entweder Extended Retention-Tier oder Cloud-Tier als sekundäre Auswahlmöglichkeit enthalten. Im Assistenten wird die aktuelle Kapazität des Dateisystems für jeden Tier angezeigt und angegeben, wie viel zusätzlicher Speicherplatz für eine Erweiterung verfügbar ist.

Hinweis

Die Kapazität des Dateisystems kann nur erweitert werden, wenn die physischen Laufwerke auf dem System installiert sind und das Dateisystem aktiviert ist.

2. Wählen Sie aus der Drop-down-Liste **Storage Tier** einen Tier aus.
3. Wählen Sie im Bereich **Addable Storage** die zu verwendenden Speichergeräte aus und klicken Sie auf **Add to Tier**.
4. Befolgen Sie die Anweisungen des Assistenten. Wenn die Bestätigungsseite angezeigt wird, klicken Sie auf **Close**.

Löschen des Dateisystems

Das Löschen des Dateisystems sollte nur unter der Anleitung des Customer Service durchgeführt werden. Durch diese Aktion werden alle Daten im Dateisystem gelöscht, einschließlich virtueller Bänder. Gelöschte Daten sind nicht wiederherstellbar. Bei diesem Vorgang werden auch die Konfigurationseinstellungen für die Replikation entfernt.

Dieser Vorgang wird verwendet, wenn es erforderlich ist, vorhandene Daten zu bereinigen, ein neues Sammelreplikationsziel zu erstellen oder eine Sammlungsquelle zu ersetzen. Er kann zudem aus Sicherheitsgründen erforderlich sein, wenn das System außer Betrieb genommen wird.

⚠ ACHTUNG

Mit dem optionalen Vorgang Write zeros to disk werden Nullen an alle Dateisystemlaufwerke geschrieben, wodurch effektiv alle Spuren von Daten entfernt werden. Wenn das Data Domain-System eine große Datenmenge enthält, kann dieser Vorgang mehrere Stunden oder einen Tag dauern.

Hinweis

Da es sich um ein destruktives Verfahren handelt, ist dieser Vorgang nur für administrative Benutzer verfügbar.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Summary** > **Destroy** aus.
2. Geben Sie Dialogfeld „Destroy File System“ das Passwort des Systemadministrators ein (es ist das einzige akzeptierte Passwort).
3. Klicken Sie optional auf das Kontrollkästchen für **Write zeros to disk**, um Daten komplett zu entfernen.
4. Klicken Sie auf **OK**.

Bereinigung

In diesem Abschnitt werden das Starten und Beenden der Bereinigung sowie das Ändern von Bereinigungsplanungen beschrieben.

Starten der Bereinigung

So starten Sie sofort einen Bereinigungsvorgang:

Vorgehensweise

1. Wählen Sie **Data Managment** > **File System** > **Summary** > **Settings** > **Cleaning** aus.

   Die Registerkarte „Cleaning“ des Dialogfelds „File System Setting“ zeigt die konfigurierbaren Einstellungen für jeden Tier an.

2. Für den aktiven Tier:

   a. Geben Sie im Textfeld „Throttle %“ einen Wert für die Systemdrosselung ein. Dies ist der Prozentsatz der CPU-Auslastung, der für die Bereinigung reserviert ist. Die Standardeinstellung ist 50 %.

   b. Wählen Sie in der Drop-down-Liste „Frequency“ eine der folgenden Frequenzen aus: „Never“, „Daily“, „Weekly“, „Biweekly“ und „Monthly“. Die Standardeinstellung ist „Weekly“.

   c. Konfigurieren Sie für die Option „At“ einen bestimmten Zeitpunkt.

   d. Wählen Sie für die Option „On“ einen Wochentag aus.

3. Für den Cloud-Tier:

   a. Geben Sie im Textfeld „Throttle %“ einen Wert für die Systemdrosselung ein. Dies ist der Prozentsatz der CPU-Auslastung, der für die Bereinigung reserviert ist. Die Standardeinstellung ist 50 %.

   b. Wählen Sie in der Drop-down-Liste „Frequency“ eine der folgenden Frequenzen aus: „Never“, „After every 'N' Active Tier cleans“.

   Hinweis

   Wenn auf eine Cloudeinheit während der Cloud-Tier-Bereinigung nicht zugegriffen werden kann, wird die Cloudeinheit in dieser Ausführung übersprungen. Die Bereinigung auf dieser Cloudeinheit erfolgt in der nächsten Ausführung, wenn die Cloudeinheit verfügbar wird. Der Zeitplan für die Bereinigung bestimmt die Dauer zwischen zwei Ausführungen. Wenn die Cloudeinheit verfügbar wird und es Ihnen nicht möglich ist, auf die nächste geplante Ausführung zu warten, können Sie die Bereinigung manuell starten.

4. Klicken Sie auf **Save**.

Beenden der Bereinigung

So beenden Sie sofort einen Bereinigungsvorgang:

Vorgehensweise

1. Wählen Sie **Data Managment** > **File System** > **Summary** > **Settings** > **Cleaning** aus.

   Die Registerkarte „Cleaning“ des Dialogfelds „File System Setting“ zeigt die konfigurierbaren Einstellungen für jeden Tier an.

2. Für den aktiven Tier:

   a. Wählen Sie in der Drop-down-Liste „Frequency“ die Option „Never“ aus.

3. Für den Cloud-Tier:

   a. Wählen Sie in der Drop-down-Liste „Frequency“ die Option „Never“ aus.

4. Klicken Sie auf **Save**.

Durchführen einer Bereinigung

Zum Einhalten behördlicher Richtlinien muss eine Systembereinigung, die auch als Daten-Shredding bezeichnet wird, durchgeführt werden, wenn klassifizierte oder sensible Daten in ein System geschrieben werden, das nicht für das Speichern solcher Daten genehmigt ist.

Wenn es zu einem Vorfall kommt, muss der Systemadministrator sofort Maßnahmen ergreifen, um die Daten gründlich zu vernichten, die versehentlich geschrieben wurden. Ziel ist es, das Speichergerät effektiv auf einen Status wiederherzustellen, als hätte das Event nicht stattgefunden. Wenn der Datenverlust mit sensiblen Daten erfolgt, muss der gesamte Speicher mithilfe des Verfahrens für die sichere Datenlöschung von Data Domain Professional Services bereinigt werden.

Mit dem Data Domain-Bereinigungsbefehl kann der Administrator Dateien auf dem logischen Level löschen, unabhängig davon, ob es sich um einen Backupsatz oder einzelne Dateien handelt. In den meisten Dateisystemen besteht das Löschen einer Datei lediglich darin, die Datei zu kennzeichnen oder Verweise auf die Daten auf der Festplatte zu löschen und so den physischen Speicherplatz freizugeben, damit er zu einem späteren Zeitpunkt genutzt werden kann. Allerdings führt diese einfache Aktion zu dem Problem, dass eine Restdarstellung von zugrunde liegenden Daten physisch auf Festplatten verbleibt. Auch deduplizierte Speicherumgebungen sind von diesem Problem betroffen.

Die Vernichtung von Daten in einem System bedeutet die Vermeidung der Restdarstellung dieser Daten und damit der Möglichkeit, dass nach der Vernichtung auf die Datei zugegriffen werden kann. Der Bereinigungsansatz von Data Domain ist vorgabenkonform mit den 2007-Versionen der folgenden Spezifikationen des Department of Defense (DoD) 5220.22 :

- *US Department of Defense 5220.22-M Clearing and Sanitization Matrix*
- *National Institute of Systems and Technology (NIST) Special Publication 800-88 Guidelines for Media Sanitization*

Bereinigung dedupizierter Daten

Data Domain-Systeme bereinigen Daten vor Ort in ihrem nativen, deduplizierten Zustand.

Deduplizierungsspeichersysteme extrahieren gemeinsame Datenmuster aus Dateien, die an das System gesendet wurden, und speichern nur einzigartige Kopien dieser Muster, die alle redundanten Instanzen referenzieren. Da diese Datenmuster oder Segmente möglicherweise von einer großen Anzahl an Dateien im System gemeinsam genutzt werden, muss der Bereinigungsprozess zuerst bestimmen, ob jedes der Segmente der infizierten Datei mit einer sauberen Datei gemeinsam genutzt wird, um dann nur die Segmente, die nicht gemeinsam genutzt werden, zusammen mit infizierten Metadaten zu löschen.

Alle Storage Tiers, Caches, sämtliche ungenutzte Kapazität und der freie Speicherplatz werden bereinigt, sodass jede Kopie jedes Segments beseitigt wird, das exklusiv zu den gelöschten Dateien gehört. Das System fordert den gesamten Speicher, der von diesen Segmenten belegt wird, zurück und überschreibt ihn, um das Speichergerät effektiv in einem Status wiederherzustellen, als ob die infizierten Dateien nie auf diesem System vorhanden waren.

Bereinigungslevel 1: Datenentfernung oder Shredding

Wenn die zu entfernenden Daten nicht klassifiziert sind, wie in der „US Department of Defense 5220.22-M Clearing and Sanitization Matrix“ definiert, kann das

Bereinigungslevel 1 verwendet werden, um den betroffenen Speicher einmal zu überschreiben. Dies stellt die Grundlage für die Handhabung der meisten Daten-Shredding- und Systembereinigungsfälle dar.

Die Bereinigungsfunktion des Data Domain-Systems sorgt dafür, dass jede Kopie jedes Segments, das nur zu gelöschten Dateien gehört, mithilfe eines Einmal-Mechanismus zum Überschreiben mit Nullen überschrieben wird. Bereinigte Daten im System, das bereinigt wird, sind online und für Benutzer verfügbar.

Vorgehensweise

1. Löschen Sie die kontaminierten Dateien oder Backups mithilfe der Backupsoftware oder des entsprechenden Clients. Achten Sie im Fall von Backups darauf, die Backupsoftware angemessen zu verwalten, um sicherzugehen, dass die zugehörigen Dateien auf diesem Image zusammengeführt, Katalogdatensätze wie erforderlich verwaltet werden usw.
2. Führen Sie auf dem kontaminierten Data Domain-System den Befehl `system sanitize start` aus, um den gesamten zuvor verwendeten Speicherplatz einmal zu überschreiben (siehe Abbildung unten).
3. Warten Sie, bis das betroffene System bereinigt wurde. Die Bereinigung kann durch Verwendung des Befehls `system sanitize watch` überwacht werden.

   Wenn für das betroffene Data Domain-System die Replikation aktiviert ist, müssen alle Systeme, die Replikate enthalten, in ähnlicher Weise bereinigt werden. Je nachdem, wie viele Daten im System vorhanden sind und wie diese verteilt sind, kann die Ausführung des Befehls `system sanitize` einige Zeit in Anspruch nehmen. Während dieser Zeit sind jedoch alle bereinigten Daten im System für Benutzer verfügbar.

Bereinigungslevel 2: vollständige Systembereinigung

Wenn die zu entfernenden Daten klassifiziert sind, wie in der „US Department of Defense 5220.22-M Clearing and Sanitization Matrix“ definiert, ist das Bereinigungslevel 2, eine vollständige Systembereinigung, erforderlich.

Data Domain empfiehlt Blancco für ein mehrfaches Überschreiben der Daten mit einem beliebigen Überschreibungsmuster und einem Zertifikat. Dies stellt die Grundlage für die Handhabung von universellen Department of Defense-Anforderungen dar, in denen eine vollständige Systembereinigung erforderlich ist. Weitere Informationen finden Sie hier:

https://www.emc.com/auth/rcoll/servicekitdocument/cp_datadomaindataerase_psbasddde.pdf

Ändern der grundlegenden Einstellungen

Ändern Sie den verwendeten Komprimierungstyp, die Markierungstypen, den Replikatschreibvorgangs-Status und den Bereitstellungs-Reserveprozentsatz, wie in diesem Abschnitt beschrieben.

Ändern der lokalen Komprimierung

Verwenden Sie die Registerkarte „General“ des Dialogfelds der Dateisystemeinstellungen, um den lokalen Komprimierungstyp zu konfigurieren.

Hinweis

Ändern Sie den Typ der lokalen Komprimierung nur, wenn es erforderlich ist.

Vorgehensweise

1. Wählen Sie **Data Managment** > **File System** > **Summary** > **Settings** > **General** aus.
2. Wählen Sie aus der Drop-down-Liste „Local Compression Type“ einen Komprimierungstyp aus.

Tabelle 93 Komprimierungstyp

Option	Beschreibung
NONE	Es werden keine Daten komprimiert.
LZ	Der Standardalgorithmus, der den besten Durchsatz bietet. Data Domain empfiehlt die Option „lz“.
GZFAST	Eine Komprimierung im Zip-Stil, die weniger Speicherplatz für komprimierte Daten verwendet, allerdings auch mehr CPU-Zyklen benötigt (doppelt so viel wie „lz“). „Gzfast“ ist die empfohlene Alternative für Standorte, die mehr Komprimierung auf Kosten niedrigerer Performance wünschen.
GZ	Eine Komprimierung im Zip-Stil, bei der die geringste Menge an Speicherplatz für Daten verwendet wird (durchschnittlich 10 % bis 20 % weniger als „lz“; wobei einige Datasets jedoch eine sehr viel höhere Komprimierung erzielen). Hierbei werden auch die meisten CPU-Zyklen benötigt (bis zu fünfmal mehr als „lz“). Der Komprimierungstyp „gz“ wird häufig für Nearline-Storage-Anwendungen mit niedrigen Performanceanforderungen verwendet.

3. Klicken Sie auf **Save**.

Ändern der Schreibschutzeinstellungen

Ändern Sie das Replikat in beschreibbar. Einigen Backupanwendungen muss ein Replikat als beschreibbar angezeigt werden, damit ein Wiederherstellungs- oder Vault-Vorgang vom Replikat durchgeführt werden kann.

Vorgehensweise

1. Wählen Sie **Data Managment** > **File System** > **Summary** > **Settings** > **General** aus.
2. Wechseln Sie im Bereich „Report Replica as Writable“ nach Bedarf zwischen **Disabled** and **Enabled**.
3. Klicken Sie auf **Save**.

Arbeiten mit der Laufwerksbereitstellung

Mit der Laufwerksbereitstellung kann ein Data Domain-System als Bereitstellungsgerät fungieren, in dem das System über eine CIFS-Share oder einen NFS-Mount-Punkt als Basislaufwerk angezeigt wird.

Die Laufwerksbereitstellung kann zusammen mit der Backupsoftware verwendet werden, z. B. NetWorker oder Symantec NBU (NetBackup). Sie erfordert keine Lizenz und ist standardmäßig deaktiviert.

Hinweis

Die DD VTL-Funktion ist nicht erforderlich oder wird nicht unterstützt, wenn das Data Domain-System als Laufwerksbereitstellungsgerät verwendet wird.

Einige Backupanwendungen verwenden Laufwerksbereitstellungsgeräte, um Bandlaufwerke kontinuierlich zu streamen. Nachdem die Daten auf Band kopiert wurden, werden sie solange auf dem Laufwerk aufbewahrt, wie Speicherplatz verfügbar ist. Wenn eine Wiederherstellung eines aktuellen Backups erforderlich ist, ist es mehr als wahrscheinlich, dass die Daten noch auf dem Laufwerk vorhanden sind und von dort aus bequemer als von Band wiederhergestellt werden können. Wenn das Laufwerk voll ist, können alte Backups gelöscht werden, um Speicherplatz freizugeben. Durch dieses Löschen nach Bedarf wird die Laufwerksverwendung maximiert.

Im normalen Betrieb wird Speicherplatz von gelöschten Dateien nur durch Ausführung eines Bereinigungsvorgangs zurückgewonnen. Dies ist nicht kompatibel mit Backupsoftware, die in einem Bereitstellungsmodus ausgeführt wird. Hier wird erwartet, dass Speicherplatz zurückgewonnen wird, wenn Dateien gelöscht werden. Wenn Sie die Laufwerksbereitstellung konfigurieren, reservieren Sie einen bestimmten Prozentsatz des gesamten Speicherplatzes – in der Regel 20 bis 30 Prozent –, damit das System die sofortige Freigabe von Speicherplatz simulieren kann.

Die Menge des verfügbaren Speicherplatzes wird durch die Menge der Bereitstellungsreserve reduziert. Wenn die Menge der gespeicherten Daten den gesamten verfügbaren Speicherplatz verwendet, ist das System voll. Wann immer jedoch eine Datei gelöscht wird, wird vom System geschätzt, wie viel Speicherplatz durch eine Bereinigung wiederhergestellt werden kann. Diese Menge wird dann von der Bereitstellungsreserve geliehen, um den verfügbaren Speicherplatz um diese Menge zu erhöhen. Wenn ein Bereinigungsvorgang durchgeführt wird, wird der Speicherplatz tatsächlich zurückgewonnen und die Reserve auf die Anfangsgröße wiederhergestellt. Da die Menge des Speicherplatzes, die durch das Löschen von Dateien verfügbar wird, nur eine Schätzung ist, stimmt der tatsächlich durch die Bereinigung zurückgewonnene Speicherplatz möglicherweise nicht mit der Schätzung überein. Das Ziel der Laufwerksbereitstellung ist es, genügend Reserven zu konfigurieren, damit Sie über ausreichend Speicherplatz verfügen, bis die geplante Bereinigung ausgeführt wird.

Konfigurieren der Festplattenbereitstellung

Aktivieren Sie die Festplattenbereitstellung und geben Sie den für die Bereitstellung zu reservierenden Prozentsatz an.

Vorgehensweise

1. Wählen Sie **Data Managment** > **File System** > **Summary** > **Settings** > **General** aus.
2. Wechseln Sie im Bereich „Staging Reserve“ nach Bedarf zwischen **Disabled** and **Enabled**.
3. Wenn die Funktion „Staging Reserve“ aktiviert ist, geben Sie einen Wert in das Feld „% of Total Space“ ein.

   Dieser Wert stellt den Prozentsatz des gesamten Festplattenspeicherplatzes dar, der für die Festplattenbereitstellung reserviert wird (in der Regel 20 bis 30 %).
4. Klicken Sie auf **Save**.

Einstellungen der Bandmarkierungen

Backupsoftware von verschiedenen Anbietern fügt Markierungen (auch als Bandmarkierungen, Tag-Header o. ä. bezeichnet) in allen Datenstreams ein (Dateisystem- und DD VTL-Backups), die an ein Data Domain-System gesendet werden.

Markierungen können die Datenkomprimierung auf einem Data Domain-System erheblich beeinträchtigen. Daher wird der Standardmarkierungstyp automatisch festgelegt und kann nicht vom Anwender geändert werden. Wenn diese Einstellung nicht mit Ihrer Backupsoftware kompatibel ist, wenden Sie sich an Ihren vertraglich festgelegten Supportanbieter.

Hinweis

Informationen dazu, wie Anwendungen in einer Data Domain-Umgebung arbeiten, finden Sie unter *So werden EMC Data Domain-Systeme in die Speicherumgebung integriert*. Sie können diese Matrizen und Integrationsleitfäden dazu verwenden, anbieterbezogene Probleme zu beheben.

Freigabe von zufälligen SSD-Workloads

Der Wert für den Schwellenwert, mit dem zufällige I/O-Operationen auf dem Data Domain-System begrenzt werden sollen, kann vom Standardwert zur Berücksichtigung von Änderungsanforderungen und I/O-Mustern angepasst werden.

Standardmäßig setzt das Data Domain-System die zufällige Workload-Freigabe von SSD auf 40 %. Dieser Wert kann je nach Bedarf nach oben oder unten angepasst werden. Wählen Sie **Data Management** > **File System** > **Summary** > **Settings** > **Workload Balance** und stellen Sie den Schieberegler ein.

Klicken Sie auf **Save**.

FastCopy-Vorgänge

Mit einem FastCopy-Vorgang werden Dateien und Verzeichnisstrukturen eines Quellverzeichnisses in ein Zielverzeichnis auf einem Data Domain-System kopiert.

Mit der Option `force` kann das Zielverzeichnis überschrieben werden, sofern vorhanden. Bei Ausführung eines FastCopy-Vorgangs wird ein Statusdialogfeld mit dem Fortschritt angezeigt.

Hinweis

Durch einen FastCopy-Vorgang wird ein Ziel mit der Quelle identisch, allerdings nicht zu einem bestimmten Zeitpunkt. Es gibt keine Garantie dafür, dass die beiden Verzeichnisse jemals identisch waren oder sein werden, wenn Sie einen der Ordner während dieses Vorgangs ändern.

Durchführen eines FastCopy-Vorgangs

Kopiert eine Datei oder eine Verzeichnisstruktur von einem Data Domain-System-Quellverzeichnis auf ein anderes Ziel auf dem Data Domain-System.

Vorgehensweise

1. Wählen Sie **Data Managment** > **File System** > **Summary** > **Fast Copy** aus.

   Das Dialogfeld „Fast Copy“ wird angezeigt.

2. Geben Sie in das Feld Source den Pfadnamen des Verzeichnisses ein, in dem sich die zu kopierenden Daten befinden. Beispiel: `/data/col1/backup/.snapshot/`*`snapshot-name`*`/dir1`.

   Hinweis

   col1 verwendet ein kleines L, gefolgt von der Zahl 1.

3. Geben Sie in das Textfeld „Destination“ den Pfadnamen des Verzeichnisses ein, an das die Daten kopiert werden. Beispiel: `/data/col1/backup/dir2`. Dieses Zielverzeichnis muss leer sein, andernfalls schlägt der Vorgang fehl.
   - Wenn das Zielverzeichnis vorhanden ist, klicken Sie auf das Kontrollkästchen **Overwrite existing destination if it exists**.
4. Klicken Sie auf **OK**.
5. Klicken Sie im daraufhin angezeigten Fortschrittsdialogfeld auf **Close**, um den Vorgang zu beenden.

KAPITEL 6

MTrees

Dieses Kapitel enthält die folgenden Themen:

Überblick über MTrees

Ein MTree ist eine logische Partition des Dateisystems.

Verwenden Sie MTrees wie folgt: für DD Boost-Speichereinheiten, DD VTL-Pools oder NFS-/CIFS-Shares. MTrees ermöglichen granulares Management von Snapshots, Quotas und DD Retention Lock. Bei Systemen, die DD Extended Retention und granulares Management der Datenmigrations-Policies vom aktiven Tier zum Aufbewahrungs-Tier haben, können MTree-Vorgänge auf einem bestimmten MTree anstatt im gesamten Dateisystem durchgeführt werden.

Hinweis

Es können so viele MTrees für MTree-Replikationskontexte vorgesehen sein, wie maximal konfigurierbar sind.

Platzieren Sie Benutzerdateien nicht im obersten Verzeichnis eines MTree.

Mtrees-Limits

MTree-Limits für Data Domain-Systeme

Tabelle 94 Unterstützte MTrees

Data Domain-System	DD OS-Version	Unterstützte konfigurierbare MTrees	Unterstützte gleichzeitig aktive MTrees
DD9800	6.0 und höher	256	256
DD9500	5.7 und höher	256	256
DD6800, DD9300	6.0 und höher	128	128
DD6300	6.0 und höher	100	32
DD2500, DD4200, DD4500, DD7200	5.7 und höher	128	128
Alle anderen DD-Systeme	5.7 und höher	100	Bis zu 32 auf Basis des Modells
DD9500	5.6	100	64
DD990, DD890	5.3 und höher	100	Bis zu 32 auf Basis des Modells
DD7200, DD4500, DD4200	5.4 und höher	100	Bis zu 32 auf Basis des Modells
Alle anderen DD-Systeme	5.2 und höher	100	Bis zu 14 auf Basis des Modells

Quoten

MTree-Quotas gelten nur für die logischen Daten, die in den MTree geschrieben werden.

Ein Administrator kann eine Speicherplatzbegrenzung für einen MTree, eine Speichereinheit oder einen DD VTL-Pool festlegen, um die Nutzung von überschüssigem Speicherplatz zu vermeiden. Es gibt zwei Arten von Quota-Limits: harte Limits und weiche Limits. Sie können entweder ein weiches Limit oder ein hartes Limit oder beide Limits festlegen. Beide Werte müssen Ganzzahlen sein und der weiche Wert muss kleiner als der harte Wert sein.

Wenn ein weiches Limit festgelegt wurde, wird eine Warnmeldung ausgegeben, wenn die MTree-Größe das Limit überschreitet, aber es können noch Daten in ihn geschrieben werden. Wenn ein hartes Limit festgelegt wurde, können keine Daten mehr in den MTree geschrieben werden, wenn das harte Limit erreicht wird. Aus diesem Grund schlagen alle Schreibvorgänge fehl, bis Daten aus einem MTree entfernt wurden.

Weitere Informationen finden Sie im Abschnitt zur Konfiguration von MTree-Quotas.

Erzwingung von Quotas

Aktivieren oder deaktivieren Sie die Erzwingung von Quotas.

Informationen über den MTree-Bereich

Hier werden alle aktiven MTrees im System aufgeführt und Echtzeitstatistiken zum Datenspeicher angezeigt. Die Informationen im Übersichtsbereich sind nützlich für die Visualisierung der Trends der Speicherplatznutzung.

Wählen Sie **Data Management** > **MTree**.

- Aktivieren Sie ein Kontrollkästchen eines MTree in der Liste, um Details anzuzeigen und in der Ansicht „Summary“ eine Konfiguration durchzuführen.
- Geben Sie Text (Platzhalter werden unterstützt) in das Feld „Filter By MTree Name“ ein und klicken Sie auf **Update**, um bestimmte MTree-Namen aufzulisten.
- Löschen Sie den Filtertext und klicken Sie auf **Reset**, um zur Standardliste zurückzukehren.

Tabelle 95 Informationen der MTree-Übersicht

Element	Beschreibung
MTree Name	Pfadname des MTree
Quota Hard Limit	Prozentsatz der verwendeten festen Quotabegrenzung.
Quota Soft Limit	Prozentsatz der verwendeten variablen Quotabegrenzung.
Last 24 Hr Pre-Comp (pre-compression)	Menge der Rohdaten der Backupanwendung, die in den letzten 24 Stunden geschrieben wurde.
Last 24 Hr Post-Comp (post-compression)	Menge des nach der Komprimierung verwendeten Speichers in den letzten 24 Stunden.
Last 24 hr Comp Ratio	Komprimierungsverhältnis für die letzten 24 Stunden.
Weekly Avg Post-Comp	Durchschnittliche Menge des verwendeten komprimierten Speichers in den letzten fünf Wochen.

Tabelle 95 Informationen der MTree-Übersicht (Fortsetzung)

Element	Beschreibung
Last Week Post-Comp	Durchschnittliche Menge des verwendeten komprimierten Speichers in den letzten sieben Tagen.
Weekly Avg Comp Ratio	Durchschnittliches Komprimierungsverhältnis für die letzten fünf Wochen.
Last Week Comp Ratio	Durchschnittliches Komprimierungsverhältnis für die letzten sieben Tage.

Informationen über die Ansicht „Summary“

Zeigen Sie wichtige Dateisystemstatistiken an.

Anzeigen detaillierter Informationen

Wählen Sie einen MTree, um Informationen anzuzeigen.

Tabelle 96 Detaillierte MTree-Informationen für einen ausgewählten MTree

Element	Beschreibung
Full Path	Pfadname des MTree
Pre-Comp Used	Die aktuelle Menge an Rohdaten aus der Backupanwendung, die an den MTree geschrieben wurden
Status	Status des MTree (Kombinationen werden unterstützt) Mögliche Statuswerte: • D: Gelöscht • RO: Schreibgeschützt • RW: Lesen/Schreiben • RD: Replication destination • RLCE: DD Retention Lock Compliance aktiviert • RLCD: DD Retention Lock Compliance deaktiviert • RLGE: DD Retention Lock Governance aktiviert • RLGD: DD Retention Lock Governance deaktiviert
Quota	
Quota-Durchsetzung	„Enabled“ oder „Disabled“.
Pre-Comp Soft Limit	Aktueller Wert. Klicken Sie auf „Configure“, um die Quota-Limits zu überarbeiten.
Pre-Comp Hard Limit	Aktueller Wert. Klicken Sie auf „Configure“, um die Quota-Limits zu überarbeiten.
Quota Summary	Der Prozentsatz des verwendeten festen Grenzwerts.
Protokolle	
CIFS Shared	Status der CIFS-Share. Mögliche Statuswerte:

Tabelle 96 Detaillierte MTree-Informationen für einen ausgewählten MTree (Fortsetzung)

Element	Beschreibung
	• Yes: Der MTree oder sein übergeordnetes Verzeichnis ist freigegeben. • Partial: Das Unterverzeichnis unter diesem MTree ist freigegeben. • No: Dieser MTree und sein über- oder untergeordnetes Verzeichnis sind nicht freigegeben. Klicken Sie auf den Link „CIFS“, um zur CIFS-Ansicht zu wechseln.
NFS Exported	Status des NFS-Exports. Mögliche Statuswerte: • Yes: Der MTree oder sein übergeordnetes Verzeichnis ist exportiert. • Partial: Das Unterverzeichnis unter diesem MTree ist exportiert. • No: Dieser MTree und sein über- oder untergeordnetes Verzeichnis werden nicht exportiert. Klicken Sie auf den Link „NFS“, um zur NFS-Ansicht zu wechseln.
DD Boost Storage Unit	DD Boost-Exportstatus. Mögliche Statuswerte: • Yes: Der MTree ist exportiert. • No: Dieser MTree ist nicht exportiert. • Unknown: Es sind keine Informationen vorhanden. Klicken Sie auf den Link „DD Boost“, um zur DD Boost-Ansicht zu wechseln.
VTL Pool	Falls zutreffend, der Name des DD VTL-Pools, der in einen MTree konvertiert wurde
vDisk Pool	Status des vDisk-Berichts Mögliche Statuswerte: • Unknown: Der vDisk-Service ist nicht aktiviert. • No: Der vDisk-Service ist aktiviert, aber der MTree ist kein vDisk-Pool. • Yes: Der vDisk-Service ist aktiviert und der MTree ist ein vDisk-Pool.
Messungen der physischen Kapazität	
Used (Post-Comp)	MTree-Speicherplatz, der verwendet wird, nachdem komprimierte Daten aufgenommen wurden
Komprimierung	Globaler Komprimierungsfaktor
Last Measurement Time	Zeitpunkt der letzten Messung des MTree durch das System
Planungen	Anzahl der zugewiesenen Planungen Klicken Sie auf **Assign**, um Planungen anzuzeigen und zum MTree zuzuweisen.

Tabelle 96 Detaillierte MTree-Informationen für einen ausgewählten MTree (Fortsetzung)

Element	Beschreibung

	• Name: Planungsname
	• Status: Aktiviert oder deaktiviert
	• Priority:
	  ▪ Normal: Sendet eine Messaufgabe an die Verarbeitungswarteschlange
	  ▪ Urgent: Sendet eine Messaufgabe an den Beginn der Verarbeitungswarteschlange.
	• Plan: Zeitpunkt der Aufgabenausführung
	• MTree Assignments: Anzahl der MTrees, denen die Planung zugewiesen ist

Submitted Measurements	Zeigt den Status der Postkomprimierung für den MTree an Klicken Sie auf **Measure Now**, um einen manuellen Postkomprimierungsjob für den MTree zu senden und eine Priorität für den Job zu wählen. • 0: kein Messjob gesendet • 1: 1 Messjob wird ausgeführt • 2: 2 Messjobs werden ausgeführt
Snapshots	Zeigt die folgenden Statistiken an: • Total Snapshots • Expired • Unexpired • Oldest Snapshot • Newest Snapshot • Next Scheduled • Assigned Snapshot Schedules Durch Klicken auf **Total Snapshots** gelangen Sie zur Ansicht **Data Management** > **Snapshots**. Klicken Sie auf **Assign Schedules**, um Snapshot-Planungen zu konfigurieren.

Anzeigen von Replikationsinformationen für einen MTree

Zeigen Sie die Replikationskonfiguration für einen MTree an.

Wenn der ausgewählte MTree für die Replikation konfiguriert ist, werden in diesem Bereich zusammengefasste Informationen über die Konfiguration angezeigt. Andernfalls wird in diesem Bereich `No Record Found` angezeigt.

- Klicken Sie auf den Link „Replication“, um zur Seite „Replication“ für die Konfiguration zu wechseln und weitere Details anzuzeigen.

Tabelle 97 MTree-Replikationsinformationen

Element	Beschreibung
Quelle	Pfadname des Quell-MTree
Ziel	Pfadname des Ziel-MTree
Status	Status des MTree-Replikationspaars. Die Optionen für den Status sind „Normal“, „Error“ oder „Warning“.
Synchonisierungszeitpunkt	Tag und Uhrzeit der letzten Synchronisierung des Replikationspaars

Anzeigen von Snapshot-Informationen für einen MTree

Wenn der ausgewählte MTree für Snapshots konfiguriert ist, wird eine Zusammenfassung der Snapshot-Konfiguration angezeigt.

- Klicken Sie auf den Link **Snapshots**, um zur Seite „Snapshots“ zu wechseln und die Konfiguration durchzuführen oder weitere Details anzuzeigen.
- Klicken Sie auf **Assign Snapshot Schedules**, um dem ausgewählten MTree eine Snapshot-Planung zuzuweisen. Aktivieren Sie das Kontrollkästchen der Planung und klicken Sie anschließend auf **OK** und **Close**. Um eine Snapshot-Planung zu erstellen, klicken Sie auf **Create Snapshot Schedule** (Anweisungen finden Sie im Abschnitt zur Erstellung einer Snapshot-Planung).

Tabelle 98 Snapshot-Informationen für einen MTree

Element	Beschreibung
Total Snapshots	Die Gesamtzahl der Snapshots, die für diesen MTree erstellt wurden. Insgesamt können für jeden MTree 750 Snapshots erstellt werden.
Expired	Die Anzahl der Snapshots in diesem MTree, die zur Löschung markiert wurden, jedoch noch nicht mithilfe eines Bereinigungsvorgangs entfernt wurden.
Unexpired	Die Anzahl der Snapshots in diesem MTree, die nicht zur Löschung markiert wurden.
Oldest Snapshot	Das Datum des ältesten Snapshot für diesen MTree.
Newest Snapshot	Das Datum des neuesten Snapshot für diesen MTree.
Next Scheduled	Das Datum des nächsten geplanten Snapshot.
Assigned Snapshot Schedules	Der Name der Snapshot-Planung, die diesem MTree zugewiesen wurde.

Anzeigen von Retention Lock-Informationen für MTrees

Wenn der ausgewählte MTree für eine der DD Retention Lock-Softwareoptionen konfiguriert ist, wird eine Übersicht über die DD Retention Lock-Konfiguration angezeigt.

Hinweis

Informationen zur Verwaltung von DD Retention Lock für MTree finden Sie im Abschnitt zur Arbeit mit DD Retention Lock.

Tabelle 99 DD Retention Lock-Informationen

Element	Beschreibung
Status	Gibt an, ob DD Retention Lock aktiviert oder deaktiviert ist.
Retention Period	Gibt die minimale und maximale Frist für DD Retention Lock an.
UUID	Zeigt eines der beiden an: • die eindeutige Identifizierungsnummer, die für einen MTree generiert wird, wenn der MTree für DD Retention Lock aktiviert ist • dass DD Retention Lock in einer Datei in einem MTree zurückgesetzt wurde

Aktivieren und Managen von DD Retention Lock-Einstellungen

Im Bereich „DD Retention Lock“ der GUI können Sie Aufbewahrungssperrfristen ändern.

Vorgehensweise

1. Wählen Sie **Data Management** > **MTree** > **Summary**.
2. Klicken Sie im Bereich „Retention Lock“ auf **Edit**.
3. Wählen Sie im Dialogfeld „Modify Retention Lock“ die Option **Enable**, um DD Retention Lock auf dem Data Domain-System zu aktivieren.
4. Ändern Sie im Fenster „Retention Period“ die minimale oder maximale Aufbewahrungsfrist (die Funktion muss zuerst aktiviert werden).
5. Wählen Sie ein Intervall aus (Minuten, Stunden, Tage, Jahre). Klicken Sie auf **Default**, um die Standardwerte zu zeigen.
6. Klicken Sie auf **OK**.

Ergebnisse

Nachdem Sie das Dialogfeld „Modify Retention Lock“ geschlossen haben, werden aktualisierte MTree-Informationen im DD Retention Lock-Zusammenfassungsbereich angezeigt.

Informationen über die Ansicht „Space Usage“ (MTrees)

Sie können eine visuelle Darstellung der Datennutzung eines MTree zu bestimmten Points-in-Time anzeigen.

Wählen Sie **Data Management** > **MTree** > **Space Usage**.

- Klicken Sie auf einen Punkt auf der Linie des Diagramms, um ein Feld mit den Daten für diesen Punkt anzuzeigen.
- Klicken Sie auf **Print** (unten im Diagramm), um das Standarddruckdialogfeld anzuzeigen.

- Klicken Sie auf **Show in new window**, um das Diagramm in einem neuen Browserfenster anzuzeigen.

Die Linien des Diagramms bezeichnen die Messungen für folgende Elemente:

- Pre-Comp Written: Die Gesamtdatenmenge der an den MTree vom Backupserver gesendeten Daten. Daten vor der Komprimierung auf einem MTree sind das, was der Backupserver als die Gesamtmenge unkomprimierter Daten erkennt, die in einem als Speichereinheit verwendeten MTree enthalten sind, wobei der Speicherplatz (links) auf der vertikalen Achse des Diagramms angezeigt wird.

Hinweis

Für die Ansicht „MTree Space Usage“ zeigt das System nur Informationen vor der Komprimierung an. Daten können von mehreren MTrees gemeinsam genutzt werden und daher kann für einen einzigen MTree keine komprimierte Nutzung bereitgestellt werden.

Überprüfen des Verlaufs der Speicherplatznutzung
Klicken Sie im Diagramm „Space Usage“ auf ein Intervall (d. h. 7 Tage, 30 Tage, 60 Tage oder 120 Tage) auf der Linie „Duration“ über der Grafik, um die Anzahl der Tage der in der Grafik angezeigten Daten zu ändern, von sieben bis 120 Tagen.

Um die Speicherplatznutzung für Intervalle von mehr als 120 Tagen anzuzeigen, führen Sie folgenden Befehl aus:

```
# filesys show compression [summary | daily | daily-detailed] {[last n
{hours | days | weeks | months}] | [start date [end date]]}
```

Informationen über die Ansicht „Daily Written“ (MTrees)

Zeigen Sie den Datenfluss der letzten 24 Stunden an. Die über einen bestimmten Zeitraum dargestellten Datenmengen beziehen sich auf vor- und nachkomprimierte Daten.

Außerdem stellt sie Gesamtwerte für die globale und lokale Komprimierungsmenge sowie für vor- und nachkomprimierte Datenmengen zur Verfügung.

- Klicken Sie auf einen Punkt auf der Linie des Diagramms, um das Fenster mit den Daten für diesen Punkt anzuzeigen
- Klicken Sie auf **Print** (unten im Diagramm), um das Standarddruckdialogfeld anzuzeigen.
- Klicken Sie auf **Show in new window**, um das Diagramm in einem neuen Browserfenster anzuzeigen.

Die Linien des Diagramms bezeichnen die Messungen für folgende Elemente:

- Pre-Comp Written – Die Gesamtmenge der Daten, die vom Backupserver in den MTree geschrieben wurde. Vorkomprimierte Daten in einem MTree werden einem Backupserver als die nicht komprimierten Gesamtdaten, die sich in einem als Speichereinheit fungierenden MTree befinden, angezeigt.
- Post-Comp Written – Die Gesamtmenge der Daten, die in den MTree geschrieben wurden, nachdem Komprimierung durchgeführt wurde, wie in GiB dargestellt.
- Total Comp Factor – Der Gesamtbetrag der Komprimierung, die das Data Domain-System mit den empfangenden Daten durchgeführt hat (Komprimierungsrate), angezeigt mit dem Gesamtkomprimierungsfaktor (rechts) als vertikale Achse der Grafik.

Prüfung von historischen geschriebenen Daten
In der Grafik „Daily Written“ ermöglicht das Klicken auf ein Intervall (d. h. 7d, 30d, 60d oder 120d) auf die Zeile „Duration“ über der Grafik die Änderung der Anzahl der Tage, die in der Grafik angezeigt werden, von 7 bis 120 Tagen.

Unter der Grafik „Daily Written“ werden die folgenden Summen für den aktuellen Dauerwert angezeigt:

- Pre-Comp Written
- Post-Comp Written
- Global-Comp Factor
- Local-Comp Factor
- Total-Comp Factor

Überwachen der MTree-Nutzung

Zeigen Sie die Speichernutzung und Trends zu geschriebenen Daten für einen MTree an.

Vorgehensweise

- Wählen Sie**Data Management** > **MTree** aus.

  Die MTree-Ansicht zeigt eine Liste der konfigurierten MTrees an. Wenn ein MTree in der Liste ausgewählt wird, werden Details dazu auf der Registerkarte „Summary“ angezeigt. Die Registerkarten „Space Usage“ und „Daily Written“ zeigen Diagramme an, die die Speicherplatznutzung und Trends zu geschriebenen Daten für einen ausgewählten MTree darstellen. Die Ansicht enthält außerdem Optionen, die die MTree-Konfiguration für CIFS, NFS und DD Boost ermöglichen, sowie Abschnitte zur Verwaltung von Snapshots und DD Retention Lock für MTree.

  Die MTree-Ansicht verfügt über ein MTree-Übersichtsfenster und drei Registerkarten, die in diesen Abschnitten ausführlich beschrieben werden.

  - Informationen über den MTree-Bereich auf Seite 221
  - Informationen über die Ansicht „Summary“ auf Seite 222
  - Informationen über die Ansicht „Space Usage“ (MTrees) auf Seite 226
  - Informationen über die Ansicht „Daily Written“ (MTrees) auf Seite 227

Hinweis

Die physische Kapazitätsmessung (Physical Capacity Measurement, PCM) bietet Speicherplatz-Nutzungsinformationen für MTrees. Weitere Informationen zu PCM finden Sie im Abschnitt zur Messung der physischen Kapazität.

Physische Kapazitätsmessung

Die physische Kapazitätsmessung (Physical Capacity Measurement, PCM) bietet Informationen zur Speicherplatznutzung für eine Untergruppe von Speicherplatz. Über den DD System Manager bietet PCM Informationen zur Speicherplatznutzung für MTrees. Über die Befehlszeilenschnittstelle können Sie Informationen zur Speicherplatznutzung für MTrees, Mandanten, Mandanteneinheiten und Pfadsätze anzeigen.

Sobald ein Pfad für PCM ausgewählt wurde, werden alle Pfade darunter automatisch einbezogen. Wählen Sie keinen untergeordneten Pfad, nachdem der übergeordnete

Pfad bereits ausgewählt wurde. Wenn beispielsweise `/data/col1/mtree3` ausgewählt wird, wählen Sie keine Unterverzeichnisse unter mtree3.

Weitere Informationen zur Verwendung von PCM in der Befehlszeile finden Sie im *Data Domain Operating System Command Reference Guide*.

Aktivieren, Deaktivieren und Anzeigen der physischen Kapazitätsmessung

Die physische Kapazitätsmessung bietet Speicherplatz-Nutzungsinformationen für einen MTree.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **File System**.

   Das System zeigt die Registerkarte "Summary" im Bereich "File System" an.
2. Klicken Sie auf **Enable** rechts neben **Physical Capacity Measurement Status**, um PCM zu aktivieren.
3. Klicken Sie auf **Details** rechts neben **Physical Capacity Measurement Status**, um aktuell ausgeführte PCM-Aufträge anzuzeigen.
   - **MTree**: MTree, den PCM misst.
   - **Priority**: Priorität ("normal" oder "urgent") für die Aufgabe.
   - **Submit Time**: Zeitpunkt, zu dem die Aufgabe angefordert wurde.
   - **Dauer**: PCM-Ausführungsdauer für die Aufgabe.
4. Klicken Sie auf **Disable** rechts neben **Physical Capacity Measurement Status**, um PCM zu deaktivieren und alle aktuell ausgeführten PCM-Jobs abzubrechen.

Initialisieren der physischen Kapazitätsmessung

Die Initialisierung der physischen Kapazitätsmessung (Physical Capacity Measurement, PCM) ist eine einmalige Aktion, die nur stattfinden kann, wenn PCM aktiviert ist und der Cache nicht initialisiert wurde. Sie bereinigt die Caches und verbessert die Messgeschwindigkeit. Sie können während des Initialisierungsprozesses PCM-Jobs weiterhin managen und ausführen.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Configuration**.
2. Klicken Sie auf **Initialize** unter "Physical Capacity Measurement" rechts neben "Cache".
3. Klicken Sie auf **Yes**.

Managen von Planungen für die physische Kapazitätsmessung

Erstellen, bearbeiten, löschen und zeigen Sie Planungen der physischen Kapazitätsmessung an. In diesem Dialogfeld werden nur Planungen für MTrees und Planungen angezeigt, die derzeit keine Zuweisungen aufweisen.

Vorgehensweise

1. Wählen Sie **Data Management** > **MTree** > **Manage Schedules**.
   - Klicken Sie auf **Add** (+), um eine Planung zu erstellen.
   - Wählen Sie eine Planung aus und klicken Sie auf **Modify**(Stift), um die Planung zu bearbeiten.
   - Wählen Sie eine Planung aus und klicken Sie auf **Delete** (X), um eine Planung zu löschen.

2. Klicken Sie optional auf die Überschriftennamen, um nach Planung zu sortieren: **Name**, **Status** (Enabled oder Disabled) **Priority** (Urgent oder Normal), **Schedule** (Planungstiming) und **MTree Assignments** (Anzahl der MTrees, denen die Planung zugewiesen ist).

Erstellen von Planungen für die physische Kapazitätsmessung

Erstellen Sie Planungen für die physische Kapazitätsmessung und weisen Sie sie MTrees zu.

Vorgehensweise

1. Wählen Sie **Data Management** > **MTree** > **Manage Schedules**.
2. Klicken Sie auf **Add** (+), um eine Planung zu erstellen.
3. Geben Sie den Namen für die Planung ein.
4. Wählen Sie den Status:
   - **Normal**: Sendet eine Messaufgabe an die Verarbeitungswarteschlange.
   - **Urgent**: Sendet eine Messaufgabe an den Anfang der Verarbeitungswarteschlange.
5. Wählen Sie, wie oft die Planung eine Messung auslöst: **Day**, **Week** oder **Month**.
   - Wählen Sie für **Day** die Uhrzeit aus.
   - Wählen Sie für **Week** die Uhrzeit und den Wochentag aus.
   - Wählen Sie für **Month** die Uhrzeit und Tage aus.
6. Wählen Sie die MTree-Zuweisungen für die Planung (MTrees, für die die Planung gilt):
7. Klicken Sie auf **Create**.
8. Klicken Sie optional auf die Überschriftennamen, um nach Planung zu sortieren: **Name**, **Status** (Enabled oder Disabled) **Priority** (Urgent oder Normal), **Schedule** (Planungstiming) und **MTree Assignments** (Anzahl der MTrees, denen die Planung zugewiesen ist).

Bearbeiten von Planungen für die physische Kapazitätsmessung

Bearbeiten Sie eine Planung für die physische Kapazitätsmessung.

Vorgehensweise

1. Wählen Sie **Data Management** > **MTree** > **Manage Schedules**.
2. Wählen Sie eine Planung aus und klicken Sie auf **Modify**(Stift).
3. Ändern Sie die Planung und klicken Sie auf **Save**.

   Planungsoptionen werden im Thema "Erstellen von Planungen für die physische Kapazitätsmessung" beschrieben.
4. Klicken Sie optional auf die Überschriftennamen, um nach Planung zu sortieren: **Name**, **Status** (Enabled oder Disabled) **Priority** (Urgent oder Normal), **Schedule** (Planungstiming) und **MTree Assignments** (Anzahl der MTrees, denen die Planung zugewiesen ist).

Zuweisen von Planungen für die physische Kapazitätsmessung zu einem MTree

Hängen Sie Planungen an einen MTree an.

Bevor Sie beginnen

Planungen für die physische Kapazitätsmessung (Physical Capacity Measurement, PCM) müssen erstellt werden.

Hinweis

Administratoren können bis zu drei PCM-Planungen zu einem MTree zuweisen.

Vorgehensweise

1. Wählen Sie **Data Management** > **MTree** > **Summary**.
2. Wählen Sie die MTrees, denen Planungen zugewiesen werden sollen.
3. Blättern Sie nach unten zum Bereich "Physical Capacity Measurements" und klicken Sie auf **Assign** rechts neben "Schedules".
4. Wählen Sie die Planungen, die dem MTree zugewiesen werden sollen, und klicken Sie auf **Assign**.

Sofortiges Starten der physischen Kapazitätsmessung

Starten Sie die Messung so bald wie möglich.

Vorgehensweise

1. Wählen Sie **Data Management** > **MTree** > **Summary**.
2. Blättern Sie zum Bereich "Physical Capacity Measurements" nach unten und klicken Sie auf **Measure Now** rechts neben "Submitted Measurements".
3. Wählen Sie **Normal** (sendet eine Messungsaufgabe an die Verarbeitungswarteschlange) oder **Urgent** (sendet eine Messungsaufgabe an den Beginn der Verarbeitungswarteschlange).
4. Klicken Sie auf **Senden**.

Festlegen der Drosselung der physischen Kapazitätsmessung

Legen Sie den Prozentsatz der Systemressourcen fest, die für die Messung der physischen Kapazität reserviert sind.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Configuration**.
2. Klicken Sie im Bereich "Physical Capacity Measurement" links von "Throttle" auf **Edit**.
3.

Option	Beschreibung
Click Default	Eingabe des Systemstandards von 20 %
Type throttle percent	Prozentsatz der Systemressourcen, die zur Messung der physischen Kapazität reserviert sind

4. Klicken Sie auf **Save**.

Managen von MTree-Vorgängen

In diesem Abschnitt werden das Erstellen und Konfigurieren von MTrees, das Aktivieren und Deaktivieren von MTree-Quotas usw. beschrieben.

Erstellen eines MTree

Ein MTree ist eine logische Partition des Dateisystems. Verwenden Sie MTrees für DD Boost-Speichereinheiten, DD VTL-Pools oder NFS-/CIFS-Shares.

MTrees werden im Bereich /data/col1/*mtree_name* erstellt.

Vorgehensweise

1. Wählen Sie**Data Management** > **MTree** aus.
2. Klicken Sie im MTree-Übersichtsbereich auf **Create**.
3. Geben Sie den Namen des MTrees im Textfeld „MTree Name“ ein. Namen für MTrees können bis zu 50 Zeichen enthalten. Die folgenden Zeichen sind zulässig:
   - Groß- und Kleinbuchstaben: A-Z, a-z
   - Nummern: 0-9
   - Leerzeichen
   - Komma (,)
   - Punkt (.), solange er nicht dem Namen vorangeht
   - Ausführungszeichen (!)
   - Doppelkreuz (#)
   - Dollarzeichen ($)
   - Prozentvorzeichen (%)
   - Pluszeichen (+)
   - At-Zeichen (@)
   - Gleichheitszeichen (=)
   - Kaufmännisches Und (&)
   - Semikolon (;)
   - Klammern [(und)]
   - Eckige Klammern ([und])
   - Geschweifte Klammern ({und})
   - Einschaltungszeichen (^)
   - Tilde (~)
   - Apostroph (gerades einzelnes Anführungszeichen)
   - Einzelnes schräges Anführungszeichen (‘)
4. Legen Sie die Speicherplatzbegrenzung für den MTree fest, um die Nutzung von überschüssigem Speicherplatz zu vermeiden. Geben Sie eine variable oder feste Quotabegrenzung oder beides ein. Bei einem variablen Grenzwert wird eine Warnmeldung ausgegeben, wenn die MTree-Größe das Limit überschreitet, aber Daten können dennoch in den MTree geschrieben werden. Daten können nicht in den MTree geschrieben werden, wenn der feste Grenzwert erreicht wurde.

Hinweis

Die Quota-Limits sind vorkomprimierte Werte.
Um ausgewählte Quota-Limits für den MTree festzulegen, wählen Sie **Set to Specific value** und geben Sie den Wert ein. Wählen Sie die Maßeinheit aus: MiB, GiB, TiB oder PiB.

Hinweis

Wenn variable und feste Grenzwerte festgelegt werden, kann die variable Grenze einer Quota die feste Grenze der Quota nicht übersteigen.

5. Klicken Sie auf **OK**.

   Der neue MTree wird in der MTree-Tabelle angezeigt.

Hinweis

Möglicherweise müssen Sie die Breite der Spalte „MTree-Name“ erweitern, um den gesamten Pfadnamen anzuzeigen.

Konfigurieren und Aktivieren/Deaktivieren von MTree-Quotas

Legen Sie die Speicherplatzbegrenzungen für einen MTree, eine Speichereinheit oder einen DD VTL-Pool fest.

Auf der Seite **Data Management** > **Quota** wird dem Administrator angezeigt, für wie viele MTrees keine weichen oder harten Quotas festgelegt sind. Bei MTrees, für die Quotas festgelegt sind, wird auf der Seite der Prozentsatz der verwendeten vorkomprimierten weichen und harten Limits angezeigt.

Beachten Sie beim Managen von Quotas folgende Informationen.

- MTree-Quotas werden auf Aufnahmevorgänge angewendet. Diese Quotas können auf DD VTL, DD Boost, CIFS und NFS sowie auf Daten auf Systemen mit DD Extended Retention-Software angewendet werden, unabhängig davon, auf welchem Tier sie sich befinden.
- Snapshots werden nicht berücksichtigt.
- Quotas können nicht für das Verzeichnis `/data/col1/backup` festgelegt werden.
- Der zulässige Höchstwert für eine Quota ist 4.096 PiB.

Konfigurieren von MTree-Quotas

Auf der Registerkarte „MTree“ oder der Registerkarte „Quota“ können Sie MTree-Quotas konfigurieren.

Vorgehensweise

1. Wählen Sie einen der folgenden Menüpfade aus:
   - Wählen Sie **Data Management** > **MTree**.
   - Wählen Sie **Data Management** > **Quota**.
2. Wählen Sie auf der Registerkarte „MTree“ nur einen MTree aus oder mehrere MTrees auf der Registerkarte „Quota“.

Hinweis

Quotas können nicht für das Verzeichnis `/data/col1/backup` festgelegt werden.

3. Klicken Sie auf der Registerkarte „MTree“ auf die Registerkarte **Summary** und klicken Sie dann auf die Schaltfläche **Configure** im Bereich „Quota“.
4. Klicken Sie auf der Registerkarte „Quota“ auf die Schaltfläche **Configure Quota**.

Konfigurieren von MTree-Quotas

Geben Sie Werte für harte und weiche Quotas ein und wählen Sie die Maßeinheit aus.

Vorgehensweise

1. Geben Sie im Dialogfeld „Configure Quota for MTrees“ Werte für harte und weiche Quotas ein und wählen Sie die Maßeinheit aus: MiB, GiB, TiB oder PiB.
2. **Klicken Sie auf OK**.

Löschen eines MTree

Der MTree wird aus der MTree-Tabelle entfernt. Die MTree-Daten werden bei der nächsten Bereinigung gelöscht.

Hinweis

Da der MTree und die zugehörigen Daten erst nach der Dateibereinigung entfernt werden, können Sie keinen neuen MTree mit dem Namen des gelöschten MTree erstellen, bis der gelöschte MTree mithilfe des Bereinigungsvorgangs vollständig aus dem Dateisystem entfernt wurde.

Vorgehensweise

1. Wählen Sie **Data Management** > **MTree** aus.
2. Wählen Sie einen MTree aus.
3. Klicken Sie in der MTree-Übersicht auf **Delete**.
4. Klicken Sie im Dialogfeld „Warning“ auf **OK**.
5. Klicken Sie im Statusdialogfeld „Delete MTree“ auf **Close**, nachdem Sie den Fortschritt angezeigt haben.

Wiederherstellen von MTree

Beim Wiederherstellen werden ein gelöschter MTree und seine Daten abgerufen und wieder in die MTree-Tabelle eingefügt.

Beim Wiederherstellen eines MTree werden ein gelöschter MTree und seine Daten abgerufen und wieder zurück in die MTree-Tabelle platziert.

Eine Wiederherstellung ist nur möglich, wenn keine Dateibereinigung ausgeführt wurde, nachdem der MTree zum Löschen markiert wurde.

Hinweis

Mit diesem Verfahren können Sie auch Speichereinheiten wiederherstellen.

Vorgehensweise

1. Wählen Sie **Data Management** > **MTree** > **More Tasks** > **Undelete**.
2. Aktivieren Sie die Kontrollkästchen der MTrees, die Sie wiederherstellen möchten und klicken Sie auf **OK**.
3. Klicken Sie im Dialogfeld „Undelete MTree Status“ auf **Close**, nachdem Sie den Fortschritt angezeigt haben.

   Der wiederhergestellte MTree wird in der MTree-Tabelle angezeigt.

Umbenennen eines MTree

Verwenden Sie die MTree-GUI von Data Management, um MTrees umzubenennen.

Vorgehensweise

1. Wählen Sie**Data Management** > **MTree** aus.
2. Wählen Sie in der Tabelle „MTree“ einen MTree aus.
3. Wählen Sie die Registerkarte Summary aus.
4. Klicken Sie im Übersichtsbereich „Detailed Information“ auf **Rename**.
5. Geben Sie den Namen des MTree in das Textfeld „New MTree Name“ ein.

   Weitere Informationen für eine Liste der zulässigen Zeichen finden Sie im Abschnitt über die Erstellung von MTrees.

6. Klicken Sie auf **OK**.

   Der umbenannte MTree wird in der Tabelle „MTree“ angezeigt.

KAPITEL 7

Snapshots

Inhalt dieses Kapitels:

Snapshots – Übersicht

In diesem Kapitel wird beschrieben, wie Sie die Snapshot-Funktion mit MTrees verwenden.

Snapshots speichern eine schreibgeschützte Kopie (einen so genannten *Snapshot*) von einem festgelegten MTree zu einem bestimmten Zeitpunkt. Sie können Snapshots als Wiederherstellungspunkt verwenden und MTree-Snapshots und Planungen managen sowie Informationen über den Status vorhandener Snapshots anzeigen.

Hinweis

Snapshots, die auf dem Data Domain-Quellsystem erstellt wurden, werden zum Ziel mit einer Sammel- und MTree-Replikation repliziert. Es ist nicht möglich, Snapshots auf einem Data Domain-System zu erstellen, das als ein Replikat für Sammelreplikationen fungiert. Es ist auch nicht möglich, einen Snapshot auf dem Ziel-MTree der MTree-Replikation zu erstellen. Bei der Verzeichnisreplikation werden Snapshots nicht repliziert und Sie müssen Snapshots auf dem Zielsystem separat erstellen.

Snapshots für den MTree namens `backup` werden im Systemverzeichnis `/data/col1/backup/.snapshot` erstellt. Jedes Verzeichnis unter `/data/col1/backup` enthält außerdem ein Verzeichnis `.snapshot` mit dem Namen der einzelnen Snapshots, die das Verzeichnis enthält. Jeder MTree weist denselben Strukturtyp auf. MTree „SantaClara“ verfügt also über das Systemverzeichnis `/data/col1/SantaClara/.snapshot` und jedes Unterverzeichnis unter `/data/col1/SantaClara` verfügt zudem über ein Verzeichnis `.snapshot`.

Hinweis

Das Verzeichnis `.snapshot` ist nicht sichtbar, wenn nur `/data` gemountet ist. Wenn der MTree selbst gemountet wurde, ist das Verzeichnis „.snapshot“ sichtbar.

Ein abgelaufener Snapshot bleibt bis zum nächsten Dateisystem-Bereinigungsvorgang verfügbar.

Die maximale Anzahl der pro MTree zugelassenen Snapshots ist 750. Warnungen werden gesendet, wenn die Anzahl von Snapshots pro MTree 90 % der maximal zulässigen Anzahl erreicht (von 675 bis 749 Snapshots) und eine Warnmeldung wird erzeugt, wenn die maximale Anzahl erreicht wird. Um die Warnmeldung zu löschen, lassen Sie die Snapshots ablaufen und führen Sie dann den Dateisystem-Bereinigungsvorgang aus.

Hinweis

Um einen MTree zu identifizieren, der sich der maximalen Anzahl von Snapshots annähert, aktivieren Sie den Bereich „Snapshots“ auf der Seite „MTree“, um die MTree-Snapshot-Informationen anzuzeigen.

Die Snapshot-Aufbewahrung für einen MTree nimmt keinen zusätzlichen Speicherplatz in Anspruch, aber wenn ein Snapshot vorhanden ist und die ursprüngliche Datei nicht mehr vorhanden ist, kann der Speicherplatz nicht zurückgewonnen werden.

Hinweis

Snapshots und CIFS-Protokoll: Ab DD OS 5.0 ist das Verzeichnis `.snapshot` nicht mehr in der Verzeichnisliste im Windows Explorer oder der DOS CMD-Shell sichtbar. Sie können auf das Verzeichnis `.snapshot` zugreifen, indem Sie den Namen in die Windows Explorer-Adresszeile oder in die DOS CMD-Shell eingeben. Beispiel: `\\dd\backup\.snapshot` oder `Z:\.snapshot`, wenn `Z:` als `\\dd\backup` zugeordnet ist.

Monitoring von Snapshots und ihren Planungen

Dieser Abschnitt bietet detaillierte und zusammenfassende Informationen über den Status von Snapshots und Snapshot-Planungen.

Informationen über die Snapshot-Ansicht

Die Themen in diesem Abschnitt beschreiben die Snapshot-Ansicht.

Snapshots – Übersichtsbereich

Sie können die Gesamtzahl der Snapshots, die Anzahl abgelaufener und nicht abgelaufener Snapshots sowie den Zeitpunkt der nächsten Bereinigung anzeigen.

Wählen Sie **Data Management** > **Snapshots**.

Tabelle 100 Informationen im Snapshot-Übersichtsbereich

Feld	Beschreibung
Total Snapshots (Across all MTrees)	Die Gesamtzahl der Snapshots, aktiv und abgelaufen, auf allen MTrees im System
Expired	Die Anzahl der Snapshots, die zum Löschen markiert wurden, jedoch noch nicht mit dem Bereinigungsvorgang entfernt wurden
Unexpired	Die Anzahl der Snapshots, die für die Aufbewahrung markiert sind
Next file system clean scheduled	Das Datum, an dem der nächste geplante Dateisystem-Bereinigungsvorgang durchgeführt wird

Ansicht „Snapshots“

Sie können Snapshot-Informationen nach Name, MTree, Erstellungszeit, Aktivitätsstatus und Ablaufzeitpunkt anzeigen.

In der Registerkarte „Snapshots“ wird eine Liste mit Snapshots und den folgenden Informationen angezeigt.

Tabelle 101 Snapshot-Informationen

Feld	Beschreibung
Selected Mtree	Eine Drop-down-Liste, über die der MTree ausgewählt wird, mit dem der Snapshot arbeitet.
Filtern nach	Elemente, nach denen in der Liste der angezeigten Snapshots gesucht werden soll. Optionen:

Tabelle 101 Snapshot-Informationen (Fortsetzung)

Feld	Beschreibung
	• **Name**: Name des Snapshot (Platzhalter zulässig). • **Year**: Drop-down-Liste zur Auswahl des Jahres.
Name	Der Name des Snapshot-Image.
Erstellungszeit	Das Datum, an dem der Snapshot erstellt wurde.
Läuft ab	Das Datum, an dem der Snapshot abläuft.
Status	Der Status des Snapshot, entweder „Expired“ oder leer, wenn der Snapshot aktiv ist.

Ansicht „Schedules“

Sie können Datum und Uhrzeit der Erstellung sowie Aufbewahrungsfristen und Benennungskonvention von Snapshots anzeigen.

Tabelle 102 Informationen zur Snapshot-Planung

Feld	Beschreibung
Name	Der Name der Snapshot-Planung
Tage	Die Tage, an denen die Snapshots erstellt werden
Uhrzeiten	Die Tageszeit, zu der die Snapshots erstellt werden
Retention Period	Die Zeitdauer, die der Snapshot aufbewahrt wird
Snapshot Name Pattern	Eine Zeichenfolge von Zeichen und Variablen, die in einem Snapshot-Namen übersetzt werden (z. B. `scheduled-%Y-%m-%d-%H-%M`, was in „scheduled-2010-04-12-17-33“ übersetzt wird).

1. Wählen Sie eine Planung auf der Registerkarte „Schedules“ aus. Der Bereich „Detailed Information“ wird mit einer Liste der MTrees angezeigt, die dieselbe Planung nutzen wie der ausgewählte MTree.
2. Klicken Sie auf die Schaltfläche **Add/Remove**, um MTrees zu der Liste „Schedules“ hinzuzufügen oder sie aus ihr zu entfernen.

Managen von Snapshots

In diesem Abschnitt wird das Management von Snapshots beschrieben.

Erstellen eines Snapshot

Erstellen Sie einen Snapshot, wenn ein nicht geplanter Snapshot erforderlich ist.

Vorgehensweise

1. Klicken Sie auf **Data Management** > **Snapshots**, um die Ansicht „Snapshots“ zu öffnen.
2. Klicken Sie im Dialogfeld „Snapshots“ auf **Create**.
3. Geben Sie im Feld „Name“ den Namen des Snapshot ein.

4. Aktivieren Sie im Bereich „MTree(s)“ das Kontrollkästchen für einen oder mehrere MTrees im Bereich „Available MTrees“ und klicken Sie auf **Add**.
5. Wählen Sie im Bereich „Expiration“ eine der folgenden Ablaufoptionen aus:
   a. **Never Expire**.
   b. Geben Sie eine Zahl in das Feld „In“ ein und wählen Sie **Days**, **Weeks**, **Month** oder **Years** aus der Drop-down-Liste aus. Der Snapshot wird bis zur selben Tageszeit aufbewahrt wie der, zu der er erstellt wurde.
   c. Geben Sie in das Textfeld „On“ ein Datum (im Format *mm/tt/jjjj*) ein oder klicken Sie auf **Calendar** und dann auf ein Datum. Der Snapshot wird bis Mitternacht (00:00, die erste Minute des Tages) des angegebenen Datums aufbewahrt.
6. Klicken Sie auf **OK** und **Close**.

Ändern des Ablaufdatums eines Snapshot

Ändern Sie das Ablaufdatum eines Snapshot, um ihn zu entfernen oder den Lebenszyklus zu Auditing- oder Compliancezwecken zu verlängern.

Vorgehensweise

1. Klicken Sie auf **Data Management**>**Snapshots**, um die Ansicht „Snapshots“ zu öffnen.
2. Klicken Sie auf das Kontrollkästchen des Snapshot-Eintrags in der Liste und dann auf **Modify Expiration Date**.

   Hinweis

   Sie können mehrere Snapshots gleichzeitig auswählen, indem Sie auf weitere Kontrollkästchen klicken.

3. Wählen Sie im Bereich „Expiration“ eine der folgenden Optionen für das Ablaufdatum aus:
   a. **Never Expire**.
   b. Geben Sie in das Textfeld „In“ eine Zahl ein und wählen Sie **Days**, **Weeks**, **Month** oder **Years** aus der Drop-down-Liste aus. Der Snapshot wird bis zur selben Tageszeit aufbewahrt wie der, zu der er erstellt wurde.
   c. Geben Sie in das Textfeld **On** ein Datum (im Format *mm/tt/jjjj*) ein oder klicken Sie auf **Calendar** und dann auf ein Datum. Der Snapshot wird bis Mitternacht (00:00, die erste Minute des Tages) des angegebenen Datums aufbewahrt.
4. Klicken Sie auf **OK**.

Umbenennen eines Snapshot

Auf der Registerkarte „Snapshot“ können Sie Snapshots umbenennen.

Vorgehensweise

1. Klicken Sie auf **Data Management** > **Snapshots**, um die Ansicht „Snapshots“ zu öffnen.
2. Aktivieren Sie das Kontrollkästchen des Snapshot-Eintrags in der Liste und klicken Sie auf **Rename**.

3. Geben Sie in das Feld „Name“ einen neuen Namen ein.
4. Klicken Sie auf **OK**.

Ablaufenlassen eines Snapshot

Snapshots können nicht gelöscht werden. Um Festplattenspeicherplatz freizugeben, können Sie Snapshots ablaufen lassen. Diese werden beim nächsten Bereinigungszyklus nach dem Ablaufdatum gelöscht.

Vorgehensweise

1. Wählen Sie **Data Management** > **Snapshots**, um die Ansicht „Snapshots“ zu öffnen.
2. Klicken Sie auf das Kontrollkästchen neben einem Snapshot-Eintrag in der Liste und klicken Sie auf **Expire**.

Hinweis

Es können mehrere Snapshots gleichzeitig ausgewählt werden, indem Sie zusätzliche Kontrollkästchen aktivieren.
Der Snapshot wird in der Spalte „Status“ als „Expired“ angezeigt und beim nächsten Bereinigungsvorgang gelöscht.

Managen von Snapshot-Planungen

Sie können eine Serie von Snapshots einrichten und managen, die automatisch in regelmäßigen Abständen erstellt werden (Snapshot-Planung).

Es können mehrere Snapshot-Planungen gleichzeitig aktiv sein.

Hinweis

Wenn mehrere Snapshots mit demselben Namen so geplant sind, dass sie zum selben Zeitpunkt erfolgen, wird nur einer beibehalten. Welcher beibehalten wird, ist unbestimmt, daher sollte nur einer der Snapshots mit diesem Namen für einen gegebenen Zeitraum geplant werden.

Erstellen einer Snapshot-Planung

Erstellen Sie über die Data Management-GUI eine wöchentliche oder monatliche Snapshot-Planung.

Vorgehensweise

1. Klicken Sie auf **Data Management** > **Snapshots** > **Schedules**, um die Ansicht „Schedules“ zu öffnen.
2. Klicken Sie auf **Create**.
3. Geben Sie im Textfeld **Name** den Namen der Planung ein.
4. Geben Sie im Textfeld **Snapshot Name Pattern** ein Namensmuster ein.

   Geben Sie eine Zeichenfolge aus Zeichen und Variablen ein, die einen Snapshot-Namen darstellt (z. B. ergibt `scheduled-%Y-%m-%d-%H-%m` den Namen „scheduled-2012-04-12-17-33“). Verwenden Sie Buchstaben, Ziffern, _, - und Variablen, die aktuelle Werte repräsentieren.

5. Klicken Sie auf **Validate Pattern & Update Sample**.
6. Klicken Sie auf **Next**.
7. Wählen Sie das Datum aus, ab dem die Planung ausgeführt werden soll.
   a. Weekly: Aktivieren Sie die Kontrollkästchen neben den Wochentagen oder wählen Sie **Every Day** aus.
   b. Monthly: Aktivieren Sie die Option **Selected Days** und klicken Sie auf die Daten im Kalender oder aktivieren Sie die Option **Last Day of the Month**.
   c. Klicken Sie auf **Next**.
8. Wählen Sie die Tageszeit aus, zu der die Planung ausgeführt werden soll.
   a. At Specific Times: Klicken Sie auf **Add** und geben Sie dann im sich öffnenden Dialogfeld „Time“ die Zeit im Format *hh:mm* ein und klicken Sie auf **OK**.
   b. In Intervals: Klicken Sie auf die Drop-down-Pfeile, um die Start- und Endzeit *hh:mm* und AM oder PM auszuwählen. Klicken Sie auf die Drop-down-Pfeile **Interval**, um eine Zahl und dann die Stunden oder Minuten des Intervalls auszuwählen.
   c. Klicken Sie auf **Next**.
9. Geben sie im Texteingabefeld „Retention Period“ eine Zahl ein und klicken Sie auf den Dropdown-Pfeil, um Tage, Monate oder Jahre auszuwählen. Klicken Sie dann auf **Next**.

   Planungen müssen eine Aufbewahrungszeit explizit angeben.
10. Überprüfen Sie die Parameter in der Planungszusammenfassung und klicken Sie auf **Finish**, um die Planung abzuschließen, bzw. auf **Zurück**, um Einträge zu ändern.
11. Wenn kein MTree mit der Planung verknüpft ist, werden Sie über ein Warndialogfeld gefragt, ob Sie der Planung einen MTree hinzufügen möchten. Klicken Sie zum Fortfahren auf **OK** oder zum Beenden auf **Cancel**.
12. Um der Planung einen MTree zuzuweisen, aktivieren Sie im Bereich „MTree“ das Kontrollkästchen für einen oder mehrere MTrees im Bildschirm „Available MTrees“ und klicken Sie auf **Add** und anschließend auf **OK**.

Benennungskonventionen für Snapshots, die von einer Planung erstellt wurden

Die Benennungskonvention für geplante Snapshots ist das Wort „scheduled“ gefolgt vom Datum, an dem der Snapshot aufgenommen wurde, im Format `scheduled-`*`jjjj-mm-tt-hh-mm.`* Beispielsweise `scheduled-2009-04-27-13-30`.

Der Name „mon_thurs“ ist der Name einer Snapshot-Planung. Snapshots, die von dieser Planung generiert werden, könnten die Namen `scheduled-2008-03-24-20-00`, `scheduled-2008-03-25-20-00` usw. haben.

Ändern einer Snapshot-Planung

Ändern Sie den Namen, das Datum und die Aufbewahrungsfrist einer Snapshot-Planung.

Vorgehensweise

1. Wählen Sie in der Liste „Schedule“ die Planung aus und klicken Sie auf **Modify**.
2. Geben Sie im Textfeld „Name“ den Namen der Planung ein und klicken Sie auf **Next**.

   Verwenden Sie alphanumerische Zeichen und die Zeichen „_“ und „-“.

3. Wählen Sie das Datum aus, an dem die Planung ausgeführt werden soll:
   a. Weekly: Aktivieren Sie die Kontrollkästchen neben den Wochentagen oder wählen Sie **Every Day** aus.
   b. Monthly: Aktivieren Sie die Option **Selected Days** und klicken Sie auf die Daten im Kalender oder aktivieren Sie die Option **Last Day of the Month**.
   c. Klicken Sie auf **Next**.
4. Wählen Sie die Tageszeit aus, zu der die Planung ausgeführt werden soll:
   a. At Specific Times: Klicken Sie auf das Kontrollkästchen der geplanten Zeit in der Liste „Times“ und dann auf **Edit**. Geben Sie im daraufhin angezeigten Dialogfeld „Times“ eine neue Zeit im Format *hh:mm* ein und klicken Sie auf **OK**. Oder klicken Sie auf **Delete**, um die geplante Zeit zu entfernen.
   b. In Intervals: Klicken Sie auf die Drop-down-Pfeile, um die Start- und Endzeit *hh:mm* und AM oder PM auszuwählen. Klicken Sie auf die Drop-down-Pfeile Interval, um eine Zahl und dann die Stunden oder Minuten des Intervalls auszuwählen.
   c. Klicken Sie auf **Next**.
5. Geben sie im Texteingabefeld „Retention Period“ eine Zahl ein und klicken Sie auf den Dropdown-Pfeil, um Tage, Monate oder Jahre auszuwählen. Klicken Sie dann auf **Next**.
6. Überprüfen Sie die Parameter in der Planungszusammenfassung und klicken Sie auf **Finish**, um die Planung abzuschließen, bzw. auf **Zurück**, um Einträge zu ändern.

Löschen einer Snapshot-Planung

Löschen Sie eine Snapshot-Planung aus der Planungsliste.

Vorgehensweise

1. Klicken Sie in der Planungsliste auf das Kontrollkästchen, um die Planung auswählen und klicken Sie auf **Delete**.
2. Klicken Sie Im Überprüfungsdialogfeld auf **OK** und anschließend auf **Close**.

Wiederherstellen von Daten aus einem Snapshot

Mit FastCopy-Vorgängen können Sie in Snapshots gespeicherte Daten abrufen. Weitere Informationen finden Sie im Abschnitt zu FastCopy-Vorgängen.

KAPITEL 8

CIFS

Inhalt dieses Kapitels:

Überblick über CIFS

CIFS-Clients (Common Internet File System) verfügen über Zugriff auf die Systemverzeichnisse auf dem Data Domain-System.

- Das Verzeichnis `/data/col1/backup` ist das Zielverzeichnis für komprimierte Backupserverdaten.
- Das Verzeichnis `/ddvar/core` enthält Data Domain-Core- und -Protokolldateien (löschen Sie alte Protokolle und Core-Dateien, um Speicherplatz in diesem Bereich freizugeben).

Hinweis

Sie können Core-Dateien auch aus dem Verzeichnis `/ddvar` oder dem Verzeichnis `/ddvar/ext` entfernen, wenn dieses vorhanden ist.

Clients, z. B. Backupserver, die Backup- und Wiederherstellungsvorgänge mit mindestens einem Data Domain-System durchführen, benötigen Zugriff auf das Verzeichnis `/data/col1/backup`. Clients, die über einen administrativen Zugriff verfügen, müssen auch in der Lage sein, auf das Verzeichnis `/ddvar/core` zuzugreifen, um Core- und Protokolldateien abzurufen.

Als Teil der ersten Data Domain-Systemkonfiguration wurden CIFS-Clients dafür konfiguriert, auf diese Bereiche zuzugreifen. In diesem Kapitel wird beschrieben, wie diese Einstellungen geändert werden und wie der Datenzugriff über den Data DD Manager und den Befehl`cifs` gemanagt wird.

Hinweis

- Auf der DD System Manager-Seite **Protocols** > **CIFS** können Sie wichtige CIFS-Vorgänge wie das Aktivieren und Deaktivieren von CIFS, das Festlegen der Authentifizierung, das Managen von Shares und das Anzeigen von Konfigurations- und Share-Informationen durchführen.
- Der Befehl `cifs` enthält alle Optionen für das Management von CIFS-Backups und -Wiederherstellungen zwischen Windows-Clients und Data Domain-Systemen und das Anzeigen von CIFS-Statistiken und -Status. Umfassende Informationen zum `cifs`-Befehl finden Sie im *Data Domain Operating System Command Reference Guide*.
- Informationen zur Erstkonfiguration des Systems finden Sie im *Data Domain Operating System Initial Configuration Guide*.
- Informationen zum Konfigurieren von Clients für die Verwendung des Data Domain-Systems als Server finden Sie im entsprechenden Tuningleitfaden wie dem *CIFS Tuning Guide*, der auf der support.emc.com-Website zur Verfügung steht. Suchen Sie über das Feld zum Durchsuchen nach dem vollständigen Namen des Dokuments.

Konfigurieren der SMB-Signatur

Sie können in einer DD OS-Version, die dies unterstützt, die SMB-Signaturfunktion mithilfe der CIFS-Option namens „Serversignatur“ konfigurieren.

Diese Funktion ist standardmäßig deaktiviert, da sie die Performance beeinträchtigt. Wenn diese Option aktiviert ist, kann die SMB-Signatur einen Abfall der Durchsatzperformance von 29 Prozent (Lesevorgänge) bis 50 Prozent (Schreibvorgänge) verursachen, wobei die jeweilige Systemperformance variiert. Es gibt drei mögliche Werte für SMB-Signaturen: disabled, auto und mandatory.

- Wenn SMB-Signaturen auf „disabled“ festgelegt sind, handelt es sich um den Standardwert.
- Wenn SMB-Signaturen auf „required“ festgelegt wurden, sind SMB-Signaturen erforderlich und müssen auf beiden Rechnern in der SMB-Verbindung aktiviert sein.

Befehlszeilenoberflächenbefehle für SMB-Signaturen

`cifs option set "server-signing" required`
Legt fest, dass eine Serversignatur erforderlich ist.

`cifs option reset "server-signing"`
Setzt die Serversignatur auf den Standardwert (disabled) zurück.

Als Best Practice sollten Sie bei jeder Änderung der SMB-Signaturoptionen den CIFS-Service mit dem folgenden Befehl der Befehlszeilenoberfläche deaktivieren und dann wieder aktivieren (neu starten):

```
cifs disable
cifs enable
```

Die DD System Manager-Oberfläche zeigt an, ob die SMB-Signaturoption auf „disabled“, „auto“ oder „mandatory“ eingestellt ist. Um diese Einstellung in der Schnittstelle anzuzeigen, navigieren Sie zu: **Protocols** > **CIFS** > **Registerkarte "Configuration"**. Im Bereich „Options“ lautet der Wert für die SMB-Signaturoption je nach über den Befehl festgelegtem Wert „disabled“, „auto“ oder „mandatory“.

Durchführen einer CIFS-Einrichtung

Dieser Abschnitt enthält Anweisungen zum Aktivieren von CIFS-Services, zum Benennen des CIFS-Servers usw.

HA-Systeme und CIFS

HA-Systeme sind kompatibel mit CIFS; wenn ein CIFS-Job jedoch während eines Failover durchgeführt wird, muss der Job manuell neu gestartet werden.

„/ddvar ist ein ext3-Dateisystem und kann nicht wie eine normale MTree-basierte Share freigegeben werden. Die Informationen in /ddvar sind veraltet, wenn ein Failover des aktiven Node auf den Stand-by-Node durchgeführt wird, da sich die Dateihandles auf den zwei Nodes unterscheiden. Wenn /ddvar gemountet wird, um auf Protokolldateien zuzugreifen oder das System zu aktualisieren, unmounten und remounten Sie /ddvar, wenn ein Failover seit dem letzten Mounten von /ddvar durchgeführt wurde.“

Vorbereiten von Clients für den Zugriff auf Data Domain-Systeme

Die entsprechende Dokumentation finden Sie online.

Vorgehensweise

1. Melden Sie sich auf der Onlinesupport-Website (support.emc.com) an.
2. Geben Sie den Namen des Dokuments, nach dem Sie suchen, in das Feld zum Durchsuchen ein.

3. Wählen Sie das entsprechende Dokument aus, z. B. *Technische Hinweise zu CIFS und Data Domain-Systemen*.
4. Befolgen Sie die Anweisungen im Dokument.

Aktivierung von CIFS-Services

Aktivieren Sie den Client, um über das CIFS-Protokoll auf das System zuzugreifen.

Nachdem ein Client für den Zugriff auf Data Domain-Systeme konfiguriert wurde, können Sie CIFS-Services aktivieren, die den Zugriff des Clients auf das System über das CIFS-Protokoll ermöglichen.

Vorgehensweise

1. Klicken Sie für das Data Domain-System, das in der DD System Manager-Navigationsstruktur ausgewählt ist, auf **Protocols** > **CIFS**.
2. Klicken Sie im Bereich „CIFS Status“ auf **Enable**.

Benennen des CIFS-Servers

Der Hostname für das Data Domain-System, das als CIFS-Server dient, wird bei der Erstkonfiguration des Systems festgelegt.

Um einen CIFS-Servernamen zu ändern, lesen Sie die Verfahren im Abschnitt zur Einstellung der Authentifizierungsparameter.

Der Hostname eines Data Domain-Systems sollte mit dem Namen in der DNS-Tabelle, der der IP-Adresse oder den IP-Adressen zugewiesen wird, übereinstimmen. Andernfalls kann die Authentifizierung sowie Versuche, einer Domäne beizutreten, fehlschlagen. Wenn Sie den Hostnamen des Data Domain-Systems ändern müssen, verwenden Sie den Befehl `net set hostname` und ändern Sie den Systemeintrag in der DNS-Tabelle.

Wenn das Data Domain-System als CIFS-Server dient, übernimmt es den Hostnamen des Systems. Aus Kompatibilitätsgründen erstellt es auch einen NetBIOS-Namen. Der NetBIOS-Name ist die erste Komponente des Hostnamens, komplett in Großbuchstaben. Beispiel: Der Hostname `jp9.oasis.local` wird in den NetBIOS-Namen `JP9` gekürzt. Der CIFS-Server antwortet beiden Namen.

Sie können den CIFS-Server auf unterschiedliche Namen auf NetBIOS-Ebene reagieren lassen, indem Sie den NetBIOS-Hostnamen ändern.

Ändern des NetBIOS-Hostnamens

Ändern Sie den NetBIOS-Hostnamen über die CLI.

Vorgehensweise

1. Zeigen Sie den aktuellen NetBIOS-Namen an, indem Sie Folgendes eingeben:

   ```
   # cifs show config
   ```

2. Verwenden Sie den Befehl
   `cifs set nb-hostname`*`nb-hostname`*`.`

Einrichten der Authentifizierungsparameter

Legen Sie die Data Domain-Authentifizierungsparameter für CIFS fest.

Klicken Sie auf der Registerkarte „Configuration“ links neben der Bezeichnung „Authentication“ auf den Link „Configure“. Das System navigiert zur Registerkarte

Administration > **Access** > **Authentication**, auf der Sie die Authentifizierung für Active Directory, Kerberos, Arbeitsgruppen und NIS konfigurieren können.

Festlegen von CIFS-Optionen

Sie können die CIFS-Konfiguration anzeigen und anonyme Verbindungen einschränken.

Vorgehensweise

1. Wählen Sie **Protocols** > **CIFS** > **Configuration**.
2. Klicken Sie im Bereich „Options“ auf **Configure Options**.
3. Um anonyme Verbindungen zu beschränken, klicken Sie auf das Kontrollkästchen der Option **Enable** im Bereich „Restrict Anonymous Connections“.
4. Klicken Sie im Bereich „Log-Level“ auf die Drop-down-Liste, um die Levelnummer auszuwählen.

   Das Level ist eine Ganzzahl von 1 (eins) bis 5 (fünf). Eins ist das Standardsystemlevel, das die am wenigsten detaillierten Protokollmeldungen im Zusammenhang mit CIFS sendet, fünf umfasst die meisten Details. Protokollmeldungen werden in der Datei `/ddvar/log/debug/cifs/cifs.log` gespeichert.

   Hinweis

   Ein Protokolllevel von 5 wirkt sich negativ auf die Systemperformance aus. Klicken Sie im Bereich „Log Level“ auf **Default**, nachdem Sie ein Problem beseitigt haben. Hierdurch wird das Level zurück auf 1 gesetzt.

5. Wählen Sie im Bereich "Server Signing" Folgendes:
   - **Enabled** zum Aktivieren der Serversignatur
   - **Disabled** zum Deaktivieren der Serversignatur
   - **Required**, wenn eine Serversignatur erforderlich ist

Deaktivieren von CIFS-Services

Verhindern Sie, dass Clients auf das Data Domain-System zugreifen.

Vorgehensweise

1. Wählen Sie **Protocols** > **CIFS**.
2. Klicken Sie im Bereich „Status“ auf **Disable**.
3. Klicken Sie auf **OK**.

   Auch nach der Deaktivierung des CIFS-Zugriffs werden CIFS-Authentifizierungsservices weiterhin auf dem Data Domain-System ausgeführt. Diese Fortsetzung ist erforderlich, um Active Directory-Domainbenutzer für den Managementzugriff zu authentifizieren.

Arbeiten mit Shares

Erstellen Sie Shares auf dem Data Domain-System, um Daten gemeinsam zu nutzen.

Shares werden auf dem Data Domain-System und den CIFS-Systemen verwaltet.

Erstellen von Shares auf dem Data Domain-System

Bei der Erstellung von Shares müssen Sie jedem Verzeichnis separat den Clientzugriff zuweisen und den Zugriff von jedem Verzeichnis separat entfernen. Zum Beispiel kann ein Client aus `/ddvar` entfernt werden und dennoch Zugriff auf `/data/col1/backup` haben.

Ein Data Domain-System unterstützt maximal 3000 CIFS-Shares.[1] 600 gleichzeitige Verbindungen sind zulässig. Allerdings ist die maximale Anzahl der unterstützten Verbindungen vom Systemspeicher abhängig. Im Abschnitt zum Festlegen der maximalen Anzahl geöffneter Dateien für eine Verbindung finden Sie weitere Informationen.

Hinweis

Wenn eine Replikation zu implementieren ist, kann ein einziges Data Domain-System Backups von CIFS-Clients und NFS-Clients empfangen, solange hierzu separate Verzeichnisse verwendet werden. CIFS- und NFS-Daten dürfen nicht im selben Verzeichnis abgelegt sein.

Vorgehensweise

1. Wählen Sie die Registerkarten **Protocols** > **CIFS**, um zur CIFS-Ansicht zu navigieren.
2. Stellen Sie sicher, dass die Authentifizierung konfiguriert wurde, wie im Abschnitt zum Festlegen von Authentifizierungsparametern beschrieben.
3. Legen Sie auf dem CIFS-Client gemeinsame Verzeichnisberechtigungen oder Sicherheitsoptionen fest.
4. Klicken Sie in der Ansicht „CIFS“ auf die Registerkarte „Shares“.
5. Klicken Sie auf **Create**.
6. Geben Sie im Dialogfeld „Create Shares“ die folgenden Informationen ein:

Tabelle 103 Informationen im Dialogfeld „Shares“

Element	Beschreibung
Share Name	ein beschreibender Name für die Share
Directory Path	Der Pfad zum Zielverzeichnis (z. B. `/data/col1/backup/dir1`). **Hinweis** col1 verwendet den Kleinbuchstaben L gefolgt von der Zahl 1.
Anmerkung	eine beschreibende Anmerkung über die Share

Hinweis

Der Share-Name darf maximal 80 Zeichen lang sein und darf die folgenden Zeichen nicht enthalten: \ / : * ? " < > | + [ ] ; , = oder erweiterte ASCII-Zeichen.

1. Kann von Hardwarebeschränkungen betroffen sein.

7. Fügen Sie durch Klicken auf „Add“ (**+**) im Bereich „Clients“ einen Client hinzu. Das Dialogfeld „Client“ wird angezeigt. Geben Sie den Namen des Clients im Textfeld „Client“ ein und klicken Sie auf **OK**.

   Beachten Sie beim Eingeben des Clientnamens Folgendes.

   - Es sind keine Leerzeichen oder Tabstopps (Leerstellen) zulässig.
   - Es wird nicht empfohlen, ein Sternchen (*) und einen einzelnen Clientnamen oder eine IP-Adresse für eine bestimmte Share zu verwenden. Wenn ein Sternchen (*) vorhanden ist, werden keine anderen Clienteinträge für diese Share verwendet.
   - Es ist nicht erforderlich, Clientname und IP-Adresse des Clients für denselben Client auf einer gegebenen Share zu verwenden. Verwenden Sie Clientnamen, wenn die Clientnamen in der DNS-Tabelle definiert sind.
   - Um Shares für alle Clients verfügbar zu machen, geben Sie ein Sternchen (*) als Client an. Alle Benutzer in der Liste der Clients können auf die Share zugreifen, es sei denn, eine oder mehrere Benutzernamen sind angegeben. In diesem Fall können nur die aufgeführten Namen auf die Share zugreifen.

   Wiederholen Sie diesen Schritt für jeden zu konfigurierenden Client.

8. Wählen Sie im Bereich „Max Connections“ das Textfeld aus und geben Sie die maximale Anzahl der Verbindungen mit der Share ein, die gleichzeitig zulässig sind. Der Standardwert null (kann auch über die Schaltfläche „Unlimited“ festgelegt werden) erzwingt, dass bei der Anzahl der Verbindungen kein Grenzwert gilt.
9. Klicken Sie auf **OK**.

   Die neu erstellte Share wird am Ende der Liste der Shares angezeigt, die sich in der Mitte des Bereichs „Shares“ befindet.

Ändern einer Share auf einem Data Domain-System

Ändern Sie die Informationen und Verbindungen einer Share.

Vorgehensweise

1. Wählen Sie **Protocols** > **CIFS** > **Shares**, um zur CIFS-Ansicht und zur Registerkarte "Shares" zu navigieren.
2. Aktivieren Sie das Kontrollkästchen neben der Share, die Sie in der Liste „Share Name“ ändern möchten.
3. Klicken Sie auf **Bearbeiten**.
4. Ändern von Share-Informationen:
   a. Geben Sie zum Ändern des Kommentars neuen Text in das Textfeld „Comment“ ein.
   b. Um einen Benutzer- oder Gruppennamen zu ändern, aktivieren Sie in der Liste „User/Group“ das Kontrollkästchen des Benutzers bzw. der Gruppe und klicken Sie auf **Edit** (Bleistift) oder **Delete** (X). Um einen Benutzer bzw. eine Gruppe hinzuzufügen, klicken Sie auf das Pluszeichen (**+**), wählen Sie im Dialogfeld „User/Group“ „Type“ für „User/Group“ aus und geben Sie den Benutzer- bzw. den Gruppennamen ein.
   c. Klicken Sie zum Ändern eines Clientnamens in der Liste „Client“ auf den Client und dann auf **Edit** (Bleistift) oder **Delete** (X). Klicken Sie zum Hinzufügen eines Clients auf die Schaltfläche zum Hinzufügen (**+**) und fügen Sie den Namen im Dialogfeld „Client“ hinzu.

Hinweis

Sie können die Share für alle Clients zur Verfügung stellen, indem Sie ein Sternchen (*) als Client angeben. Alle Benutzer in der Liste der Clients können auf die Share zugreifen, es sei denn, eine oder mehrere Benutzernamen sind angegeben. In diesem Fall können nur die aufgeführten Namen auf die Share zugreifen.

d. Klicken Sie auf **OK**.

5. Ändern Sie im Bereich „Max Connections“ im Textfeld die maximale Anzahl von Verbindungen mit der Share, die gleichzeitig zulässig sind. Oder wählen Sie „Unlimited“ aus, um keinen Grenzwert für die Anzahl von Verbindungen zu erzwingen.
6. Klicken Sie auf **OK**.

Erstellen einer Share aus einer vorhandenen Share

Erstellen Sie eine Share aus einer vorhandenen Share und ändern Sie die neue Share bei Bedarf.

Hinweis

Benutzerberechtigungen der vorhandenen Share werden auf die neue Share übertragen.

Vorgehensweise

1. Aktivieren Sie in der Registerkarte „CIFS Shares“ das Kontrollkästchen für die Share, die Sie als Quelle verwenden möchten.
2. Klicken Sie auf **Create From**.
3. Ändern Sie die Share-Informationen, wie im Abschnitt zur Änderung einer Share auf einem Data Domain-System beschrieben.

Deaktivieren einer Share auf einem Data Domain-System

Deaktivieren Sie eine oder mehrere Shares.

Vorgehensweise

1. Klicken Sie auf der Registerkarte „Shares“ auf das Kontrollkästchen für die Share, die Sie in der Liste „Share Name“ deaktivieren möchten.
2. Klicken Sie auf **Deaktivieren**.
3. Klicken Sie auf **Close**.

Aktivieren einer Share auf einem Data Domain-System

Aktivieren Sie eine oder mehrere Shares.

Vorgehensweise

1. Aktivieren Sie auf der Registerkarte „Shares“ das Kontrollkästchen der Shares, die Sie in der Liste der Share-Namen aktivieren möchten.
2. Klicken Sie auf **Aktivieren**.
3. Klicken Sie auf **Close**.

Löschen einer Share auf einem Data Domain-System

Löschen Sie eine oder mehrere Shares.

Vorgehensweise

1. Aktivieren Sie auf der Registerkarte „Shares“ das Kontrollkästchen der Shares, die Sie in der Liste der Share-Namen löschen möchten.
2. Klicken Sie auf **Delete**.

   Es wird ein Warndialogfeld angezeigt.
3. Klicken Sie auf **OK**.

   Die Shares werden entfernt.

Durchführen der MMC-Administration

Verwenden Sie die MMC (Microsoft Management Console) zur Administration.

DD OS unterstützt folgende MMC-Funktionen:

- Share-Management, außer dem Durchsuchen beim Hinzufügen einer Share oder dem Ändern der Offline-Standardeinstellungen, wobei es sich um ein manuelles Verfahren handelt.
- Sitzungsmanagement
- Offenes Dateimanagement, außer zum Löschen von Dateien.

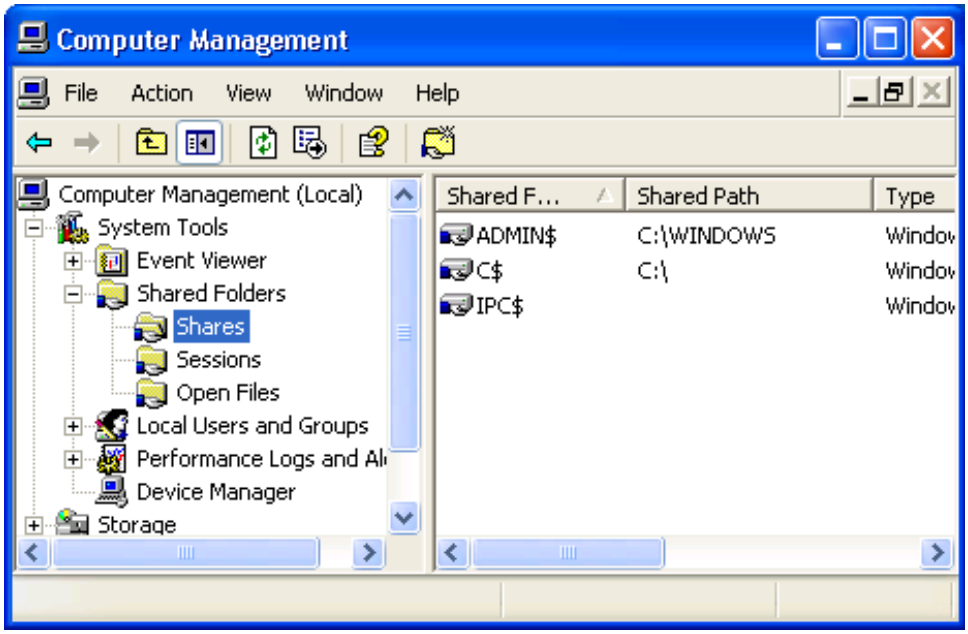
Verbinden mit einem Data Domain-System von einem CIFS-Client

Stellen Sie mithilfe von CIFS eine Verbindung zu einem Data Domain-System her und erstellen Sie einen schreibgeschützten Backupunterordner.

Vorgehensweise

1. Überprüfen Sie auf der CIFS-Seite des Data Domain-Systems, ob im CIFS-Status angezeigt wird, dass CIFS aktiviert ist und ausgeführt wird.
2. Öffnen Sie in der Systemsteuerung „Administrative Tools“ und wählen Sie **Computer Management** aus.
3. Klicken Sie im Dialogfeld „Computer Management“ mit der rechten Maustaste auf **Computer Management (Local)** und wählen Sie im Menü **Connect to another computer** aus.
4. Geben Sie im Dialogfeld „Select Computer“ **Another computer** aus und geben Sie den Namen oder die IP-Adresse für das Data Domain-System ein.
5. Erstellen Sie einen schreibgeschützten Unterordner `\backup`. Weitere Informationen finden Sie im Abschnitt zum Erstellen eines schreibgeschützten Unterordners /data/col1/backup.

Abbildung 6 Dialogfeld „Computer Management“



Erstellen eines schreibgeschützten Unterordners \data\col1\backup

Geben Sie einen Pfad und einen Sharenamen ein und wählen Sie Berechtigungen aus.

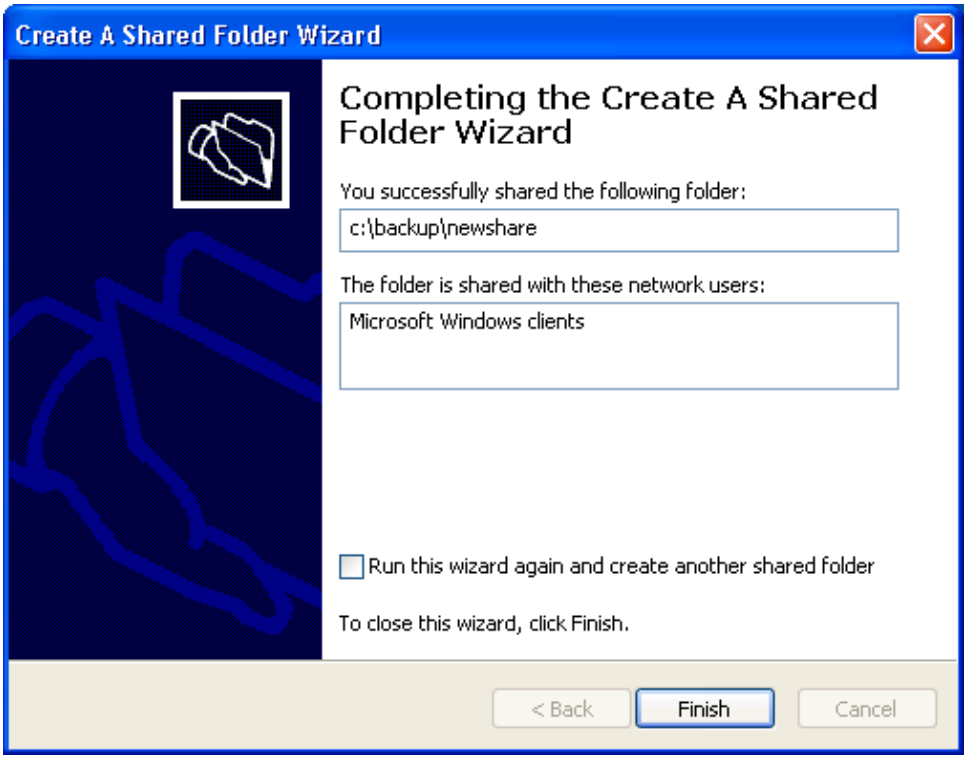
Vorgehensweise

1. Öffnen Sie in der Systemsteuerung „Administrative Tools“ und wählen Sie **Computer Management** aus.
2. Klicken Sie im Verzeichnis „Shared Folders“ mit der rechten Maustaste auf **Shares**.
3. Wählen Sie **New File Share** aus dem Menü aus.

   Der Assistent **Create a Shared Folder** wird geöffnet. Der Computername sollte der Name oder die IP-Adresse des Data Domain-Systems sein.

4. Geben Sie den Pfad für den freizugebenden Ordner ein, z. B. `C:\data\col1\backup\newshare`.
5. Geben Sie den Namen der Share ein, z. B. **`newshare`**. Klicken Sie auf **Next**.
6. Für die Berechtigungen für freigegebene Ordner haben ausgewählte Administratoren vollen Zugriff. Andere Benutzer verfügen nur über schreibgeschützten Zugriff. Klicken Sie auf **Next**.

Abbildung 7 Abschließen des Assistenten „Create a Shared Folder“



7. Im Dialogfeld „Completing“ sehen Sie, dass Sie den Ordner für alle Microsoft-Clients im Netzwerk erfolgreich freigegeben haben. Klicken Sie auf **Finish**.

   Der neu erstellte freigegebene Ordner wird im Dialogfeld „Computer Management“ aufgeführt.

Anzeigen von CIFS-Informationen

Sie können Informationen über freigegebene Ordner, Sitzungen und geöffnete Dateien anzeigen.

Vorgehensweise

1. Öffnen Sie in der Systemsteuerung „Administrative Tools“ und wählen Sie **Computer Management** aus.
2. Wählen Sie einen der „Shared Folders“ (**Shares**, **Sessions** oder **Open Files**) im Verzeichnis „System Tools“ aus.

   Informationen zu freigegebenen Ordnern, Sitzungen und offenen Dateien werden im rechten Bereich angezeigt.

Managen der Zugriffskontrolle

Sie können von einem Windows-Client auf Shares zugreifen, Administratorzugriff bereitstellen und den Zugriff durch Benutzer in vertrauenswürdigen Domains zulassen.

Zugriff auf Shares über einen Windows-Client

Verwenden Sie die Befehlszeile, um eine Share zuzuordnen.

Vorgehensweise

- Führen Sie auf dem Windows-Client diesen DOS-Befehl aus:
  `net use`*`drive`*`:`*`backup-location`*

Geben Sie beispielsweise Folgendes ein:

```
# \\dd02\backup /USER:dd02\backup22
```

Mit diesem Befehl wird die Backup-Share vom Data Domain-System dd02 dem Laufwerk H auf dem Windows-System zugeordnet und dem Benutzer „backup22“ Zugriff auf das Verzeichnis `\\DD_sys\backup` erteilt.

Bereitstellen des Administratorzugriffs für Domainbenutzer

Verwenden Sie die Befehlszeile, um CIFS hinzuzufügen und den Domainnamen in die SSH-Anweisung aufzunehmen.

Vorgehensweise

- Geben Sie Folgendes ein: **`adminaccess authentication add cifs`**

  Der SSH- oder Telnet- oder FTP-Befehl, der auf das Data Domain-System zugreift, muss in doppelte Anführungszeichen gesetzt den Domainnamen, einen umgekehrten Schrägstrich und den Benutzernamen umfassen. Beispiel:

  ```
  C:> ssh "domain2\djones" @dd22
  ```

Zulassen des Administratorzugriffs auf ein Data Domain-System für Domainbenutzer

Ordnen Sie über die Befehlszeile eine Standardgruppennummer des DD-Systems zu und aktivieren Sie anschließend den CIFS-Administratorzugriff.

Vorgehensweise

1. Um die Standardgruppennummer eines Data Domain-Systems einem Windows-Gruppennamen zuzuordnen, der vom Standardgruppennamen abweicht, verwenden Sie den Befehl
   `cifs option set "dd admin group2"["windows`*`grp-name`*`"].`

   Der Windows-Gruppenname ist eine Gruppe (basierend auf der Benutzerrolle „admin“, „user“ oder „backup-operator“), die auf einem Windows-Domain-Controller vorhanden ist. Sie können bis zu 50 Gruppen verwenden (dd admin group 1 bis dd admin group 50)

   Hinweis

   Eine Beschreibung der DD OS-Benutzerrollen und Windows-Gruppen finden Sie im Abschnitt über die Verwaltung von Data Domain-Systemen.

2. Geben Sie Folgendes ein, um den CIFS-Administratorzugriff zu aktivieren:

   `adminaccess authentication add cifs`

   - Die Data Domain-System-Standardgruppe „dd admin group1“ wird der Windows-Gruppe „Domain Admin“ zugeordnet.

- Sie können die Data Domain-System-Standardgruppe „dd admin group2“ einer Windows-Gruppe namens „Data Domain“ zuordnen, die Sie auf einem Windows-Domain-Controller erstellen.
- Zugriff ist über SSH, Telnet, FTP, HTTP und HTTPS verfügbar.
- Nachdem Sie den Administratorzugriff auf das Data Domain-System für die Windows-Gruppe `Data Domain` eingerichtet haben, müssen Sie mithilfe des Befehls `adminaccess` den CIFS-Administratorzugriff aktivieren.

Beschränken des Administratorzugriffs von Windows

Verwenden Sie die Befehlszeile, um den Zugriff für Benutzer ohne DD-Konto zu verweigern.

Vorgehensweise

- Geben Sie Folgendes ein: `adminaccess authentication del cifs`

  Dieser Befehl verweigert Windows-Benutzern den Zugriff auf das Data Domain-System, wenn sie nicht über ein Konto auf dem Data Domain-System verfügen.

Dateizugriff

Dieser Abschnitt enthält Informationen über ACLs, das Festlegen von DACL- und SACL-Berechtigungen über Windows Explorer usw.

NT-Zugriffskontrolllisten

Zugriffskontrolllisten (ACLs) sind standardmäßig auf dem Data Domain-System aktiviert.

⚠ ACHTUNG

Data Domain empfiehlt, NTFS-ACLs nicht zu deaktivieren, wenn sie einmal aktiviert wurden. Wenden Sie sich an den Data Domain-Support, bevor Sie NTFS-ACLs deaktivieren.

Standard-ACL-Berechtigungen

Die Standardberechtigungen, die neuen Objekten zugewiesen werden, die über das CIFS-Protokoll erstellt werden, wenn ACLs aktiviert sind, hängen von dem Status des übergeordneten Verzeichnisses ab. Es gibt drei verschiedene Möglichkeiten:

- Das übergeordnete Verzeichnis hat keine ACL, da es über das NFS-Protokoll erstellt wurde.
- Das übergeordnete Verzeichnis hat eine vererbbare ACL, da sie entweder über das CIFS-Protokoll erstellt wurde oder da die ACL explizit festgelegt wurde. Die übernommene ACL wird für neue Objekte festgelegt.
- Das übergeordnete Verzeichnis hat eine ACL, diese ist jedoch nicht vererbbar. Folgende Berechtigungen stehen zur Verfügung:

Tabelle 104 Berechtigungen

Typ	Name	Berechtigung	Anwenden auf
Allow	SYSTEM	Vollständige Kontrolle	Nur dieser Ordner

Tabelle 104 Berechtigungen (Fortsetzung)

Typ	Name	Berechtigung	Anwenden auf
Allow	CREATOR OWNER	Vollständige Kontrolle	Nur dieser Ordner

Hinweis

CREATOR OWNER wird von dem Benutzer ersetzt, der die Datei/den Ordner für normale Benutzer erstellt, und von den Administratoren für Administratorbenutzer.

Berechtigungen für ein neues Objekt, wenn das übergeordnete Verzeichnis keine ACL hat

Folgende Berechtigungen stehen zur Verfügung:

- BUILTIN\Administrators:(OI)(CI)F
- NT AUTHORITY\SYSTEM:(OI)(CI)F
- CREATOR OWNER:(OI)(CI)(IO)F
- BUILTIN\Users:(OI)(CI)R
- BUILTIN\Users:(CI)(special access:)FILE_APPEND_DATA
- BUILTIN\Users:(CI)(IO)(special access:)FILE_WRITE_DATA
- Everyone:(OI)(CI)R

Diese Berechtigungen werden im Folgenden ausführlicher beschrieben:

Tabelle 105 Berechtigungsdetail

Typ	Name	Berechtigung	Anwenden auf
Allow	Administratoren	Vollständige Kontrolle	Dieser Ordner, Unterordner und Dateien
Allow	SYSTEM	Vollständige Kontrolle	Dieser Ordner, Unterordner und Dateien
Allow	CREATOR OWNER	Vollständige Kontrolle	Nur Unterordner und Dateien
Allow	Benutzer	Lesen und Ausführen	Dieser Ordner, Unterordner und Dateien
Allow	Benutzer	Unterordner erstellen	Nur dieser Ordner und Unterordner
Allow	Benutzer	Dateien erstellen	Nur Unterordner
Allow	Jeder	Lesen und Ausführen	Dieser Ordner, Unterordner und Dateien

Festlegen von ACL-Berechtigungen und Sicherheit

Windows-basierte Backup- und Wiederherstellungstools wie NetBackup können dazu verwendet werden, DACL- und SACL-geschützte Dateien auf dem Data Domain-System zu sichern und sie vom Data Domain-System wiederherzustellen.

Granulare und komplexe Berechtigungen (DACL)

Sie können granulare und komplexe Berechtigungen (DACL) für jedes Datei- oder Ordnerobjekt innerhalb des Dateisystems festlegen, entweder über Windows-Befehle

wie `cacls`, `xcacls`, `xcopy` und `scopy` oder über das CIFS-Protokoll mithilfe der Windows Explorer-GUI.

Audit ACL (SACL)
Sie können Audit ACL (SACL) für jedes Objekt im Dateisystem entweder über Befehle oder über das CIFS-Protokoll mithilfe der Windows Explorer-GUI festlegen.

Festlegen der DACL-Berechtigungen mithilfe von Windows Explorer

Legen Sie die DACL-Berechtigungen in den Explorer-Eigenschaften fest.

Vorgehensweise

1. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner und wählen Sie **Properties**.
2. Klicken Sie im Dialogfeld „Properties“ auf die Registerkarte „Security“.
3. Wählen Sie den Gruppen- oder Benutzernamen, z. B. **Administrators** aus der Liste aus. Die Berechtigungen werden angezeigt, in diesem Fall `Administrators, Full Control`.
4. Klicken Sie auf die Schaltfläche **Advanced**, über die Sie spezielle Berechtigungen festlegen können.
5. Klicken Sie im Dialogfeld „Advanced Security Settings for ACL“ auf die Registerkarte „Permissions“.
6. Wählen Sie den Eintrag für die Berechtigung in der Liste aus.
7. Wählen Sie zum Anzeigen weiterer Informationen zu einem Berechtigungseintrag den entsprechenden Eintrag aus und klicken Sie auf **Edit**.
8. Wählen Sie die Option „Inherit from parent“ aus, damit Berechtigungen von übergeordneten Einträgen an ihre untergeordneten Einträge vererbt werden und klicken Sie auf **OK**.

Festlegen der SACL-Berechtigungen mithilfe von Windows Explorer

Legen Sie die SACL-Berechtigungen in den Explorer-Eigenschaften fest.

Vorgehensweise

1. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner und wählen Sie im Menü **Properties** aus.
2. Klicken Sie im Dialogfeld „Properties“ auf die Registerkarte „Security“.
3. Wählen Sie den Gruppen- oder Benutzernamen, z. B. **Administrators**, aus der Liste aus, um die Berechtigungen anzuzeigen, in diesem Fall `Full Control`.
4. Klicken Sie auf die Schaltfläche **Advanced**, die es Ihnen ermöglicht, spezielle Berechtigungen festzulegen.
5. Klicken Sie im Dialogfeld „Advanced Security Settings for ACL“ auf „Auditing“.
6. Wählen Sie den Überwachungseintrag aus der Liste aus.
7. Um weitere Informationen zu speziellen Überwachungseinträgen anzuzeigen, wählen Sie den Eintrag aus und klicken Sie auf **Edit**.
8. Aktivieren Sie das Kontrollkästchen „Inherit from parent“, um die Berechtigungen der übergeordneten Objekte von den untergeordneten Objekten zu übernehmen, und klicken Sie auf **OK**.

Anzeigen oder Ändern der aktuellen Eigentümer-SID (Sicherheits-ID)

Verwenden Sie das Dialogfeld „Advanced Security Settings for ACL“.

Vorgehensweise

1. Klicken Sie im Dialogfeld „Advanced Security Settings for ACL“ auf die Registerkarte „Owner“.
2. Um den Eigentümer zu ändern, wählen Sie einen Namen aus der Liste „Change owner“ aus und klicken Sie auf **OK**.

Steuern der ID-Kontozuordnung

Mit der CIFS-Option idmap-type wird die ID-Kontozuordnung gesteuert.

Für diese Option gibt es zwei mögliche Werte: rid (der Standardwert) und none. Wenn die Option auf rid festgelegt ist, wird die ID-Zuordnung intern durchgeführt. Wenn die Option auf none festgelegt ist, werden alle CIFS-Benutzer einem lokalen UNIX-Benutzer namens „cifsuser“ zugeordnet, der zu den lokalen UNIX-Gruppenbenutzern gehört.

Beachten Sie beim Managen dieser Option die folgenden Informationen.

- CIFS muss deaktiviert sein, damit diese Option festgelegt werden kann. Wenn CIFS ausgeführt wird, deaktivieren Sie die CIFS-Services.
- idmap-type kann nur dann auf „none“ festgelegt werden, wenn ACL-Unterstützung aktiviert ist.
- Wann immer idmap type geändert wird, ist möglicherweise eine Konvertierung der Metadaten des Dateisystems für einen korrekten Dateizugriff erforderlich. Ohne eine Konvertierung können Benutzer möglicherweise nicht auf die Daten zugreifen. Um Metadaten zu konvertieren, wenden Sie sich an Ihren Supportanbieter.

Monitoring des CIFS-Betriebs

Themen zum Monitoring des CIFS-Betriebs

Anzeigen des CIFS-Status

Sie können den CIFS-Status anzeigen und aktivieren/deaktivieren.

Vorgehensweise

1. Wählen Sie im DD System Manager **Protocols** > **CIFS**.
   - Der Status ist entweder aktiviert und in Betrieb oder deaktiviert, aber die CIFS-Authentifizierung wird ausgeführt.
     Informationen dazu, wie Sie CIFS aktivieren, finden Sie im Abschnitt zum Aktivieren von CIFS-Services. Informationen dazu, wie Sie CIFS zu deaktivieren, finden Sie im Abschnitt zum Deaktivieren von CIFS-Services.
   - **Connections** enthält die Auszählung der offenen Verbindungen und offenen Dateien.

Tabelle 106 Connections Details-Informationen

Element	Beschreibung
Open Connections	Offene CIFS-Verbindungen
Connection Limit	Maximal zulässige Verbindungen
Open Files	Aktuelle geöffnete Dateien

Tabelle 106 Connections Details-Informationen (Fortsetzung)

Element	Beschreibung
Max Open Files	Maximale Anzahl an geöffneten Dateien auf einem Data Domain-System

2. Klicken Sie auf **Connection Details**, um weitere Verbindungsinformationen anzuzeigen.

Tabelle 107 Connections Details-Informationen

Element	Beschreibung
Sessions	Aktive CIFS-Sitzungen
Computer	IP-Adresse oder Computername (für die Sitzung mit DDR verbunden)
User	Benutzer, die den Computer verwenden, der mit DDR verbunden ist
Open Files	Anzahl der geöffneten Dateien für jede Sitzung
Connection Time	Dauer der Verbindung in Minuten
User	Domainname des Computers
Mode	Dateiberechtigungen
Locks	Anzahl der Sperren für die Datei
Files	Speicherort der Datei

Anzeigen der CIFS-Konfiguration

In diesem Abschnitt wird die CIFS-Konfiguration angezeigt.

Authentifizierungskonfiguration

Die im Bereich „Authentication“ angezeigten Informationen hängen vom Typ der konfigurierten Authentifizierung ab.

Klicken Sie auf der Registerkarte „Configuration“ links neben der Bezeichnung „Authentication“ auf den Link „Configure“. Das System navigiert zur Seite **Administration** > **Access** > **Authentication**, wo Sie die Authentifizierung für Active Directory, Kerberos, Arbeitsgruppen und NIS konfigurieren können.

Active Directory-Konfiguration

Tabelle 108 Informationen zur Active Directory-Konfiguration

Element	Beschreibung
Mode	Es wird der Active Directory-Modus angezeigt.
Bereich	Es wird der konfigurierte Bereich angezeigt.
DDNS	Es wird der Status des DDNS-Servers angezeigt: „Enabled“ oder „Disabled“.

Tabelle 108 Informationen zur Active Directory-Konfiguration (Fortsetzung)

Element	Beschreibung
Domain Controllers	Es wird der Name der konfigurierten Domain Controller oder ein „*“ angezeigt, wenn alle Controller zulässig sind.
Organisationseinheit	Es wird der Name der konfigurierten Organisationseinheiten angezeigt.
CIFS Server Name	Es wird der Name der konfigurierten CIFS-Server angezeigt.
WINS Server Name	Es wird der Name der konfigurierten WINS-Server angezeigt.
Short Domain Name	Es wird der kurze Domainname angezeigt.

Workgroup Configuration

Tabelle 109 Authentifizierungsinformationen zur Arbeitsgruppenkonfiguration

Element	Beschreibung
Mode	Es wird der Arbeitsgruppenmodus angezeigt.
Workgroup Name	Es wird der Name der konfigurierten Arbeitsgruppe angezeigt.
DDNS	Es wird der Status des DDNS-Servers angezeigt: „Enabled“ oder „Disabled“.
CIFS Server Name	Es wird der Name der konfigurierten CIFS-Server angezeigt.
WINS Server Name	Es wird der Name der konfigurierten WINS-Server angezeigt.

Anzeigen von Informationen über Shares

In diesem Abschnitt werden Informationen über Shares angezeigt.

Anzeigen konfigurierter Shares

Zeigen Sie die Liste der konfigurierten Shares an.

Tabelle 110 Informationen über konfigurierte Shares

Element	Beschreibung
Freigabename	Der Name der Share (z. B. share1).
Share Status	Der Status der Share: entweder aktiviert oder deaktiviert
Verzeichnispfad	Der Verzeichnispfad zur Share (z. B. `/data/col1/backup/dir1`). **Hinweis** col1 verwendet den Kleinbuchstaben L, gefolgt von der Zahl 1.
Directory Path Status	Der Status des Verzeichnispfads.

- Um Informationen über eine bestimmte Share aufzulisten, geben Sie den Share-Namen in das Textfeld „Filter by Share Name“ ein und klicken Sie auf **Update**.

- Klicken Sie auf **Update**, um zur Standardliste zurückzukehren.
- Um die Liste der Shares zu durchblättern, klicken Sie auf die Pfeile **<** und **>** unten rechts in der Ansicht, um vor- oder zurückzublättern. Um zum Anfang der Liste zu springen, klicken Sie auf **|<**, und um zum Ende zu springen, klicken Sie auf **>|**.
- Klicken Sie auf den Drop-down-Pfeil **Items per Page**, um die Anzahl der Share-Einträge zu ändern, die auf einer Seite aufgeführt sind. Die Möglichkeiten sind 15, 30 oder 45 Einträge.

Anzeigen detaillierter Shareinformationen

Zeigen Sie detaillierte Informationen zu einer Share an, indem Sie in der Shareliste auf den Sharenamen klicken.

Tabelle 111 Shareinformationen

Element	Beschreibung
Share Name	Der Name der Share (z. B. share1).
Directory Path	Der Verzeichnispfad zur Share (z. B. `/data/col1/backup/dir1`). **Hinweis** col1 verwendet den Kleinbuchstaben L gefolgt von der Zahl 1.
Directory Path Status	Gibt an, ob der konfigurierte Verzeichnispfad auf dem DDR vorhanden ist. Mögliche Werte sind "Path Exists" oder "Path Does Not Exist". (Letzteres gibt eine falsche oder unvollständige CIFS-Konfiguration an.)
Max. Verbindungen	Die zulässige Höchstzahl gleichzeitiger Verbindungen zur Share. Der Standardwert ist "Unlimited".
Anmerkung	Der Kommentar, der konfiguriert wurde, als die Share erstellt wurde.
Share Status	Der Status der Share: entweder „enabled“ oder „disabled“.

- Der Bereich „Clients“ listet die Clients auf, die für den Zugriff auf die Share konfiguriert sind, zusammen mit einer Clientzählung unter der Liste.
- Der Bereich „User/Groups“ listet die Namen und den Typ der Benutzer oder Gruppen auf, die für den Zugriff auf die Share konfiguriert wurden, zusammen mit einer Benutzer- oder Gruppenzählung unter der Liste.
- Der Bereich „Optionen“ listet den Namen und den Wert der konfigurierten Optionen auf.

Anzeigen von CIFS-Statistiken

Verwenden Sie die Befehlszeile, um CIFS-Statistiken anzuzeigen.

Vorgehensweise

- Geben Sie Folgendes ein: `cifs show detailed-stats`

  Die Ausgabe zeigt die Anzahl der verschiedenen empfangenen SMB-Anforderungen und die benötigte Zeit, um sie zu verarbeiten.

Durchführen eines CIFS-Troubleshooting

Dieser Abschnitt enthält grundlegende Verfahren zum Troubleshooting.

Hinweis

Die `cifs troubleshooting`-Befehle bieten detaillierte Informationen über CIFS-Benutzer und -Gruppen.

Anzeigen der aktuellen Aktivität von Clients

Verwenden Sie die Befehlszeile, um CIFS-Sitzungen anzuzeigen und Datei-Informationen zu öffnen.

Vorgehensweise

- Geben Sie Folgendes ein: **`cifs show active`**

Ergebnisse

Tabelle 112 Sitzungen

Computer	Benutzer	Geöffnete Dateien	Verbindungszeit (Sek.)	Leerlauf (Sek.)
::ffff: 10.25.132.84	ddve-25179109\sysadmin	1	92	0

Tabelle 113 Geöffnete Dateien

Benutzer	Mode	Sperren	Datei
Ddve-25179109\sysadmin	1	0	C:\data\col1\backup

Festlegen der maximalen Anzahl offener Dateien in einer Verbindung

Verwenden Sie die Befehlszeile, um die maximale Anzahl von Dateien festzulegen, die gleichzeitig geöffnet sein können.

Vorgehensweise

- Geben Sie Folgendes ein: **`cifs option set max-global-open-files`***value*.

  Der *value* für die maximale Anzahl an global geöffneten Dateien kann zwischen 1 und der Obergrenze für geöffnete Dateien liegen. Die Obergrenze basiert auf dem DDR-Systemspeicher. Für Systeme mit mehr als 12 GB liegt die maximale Anzahl geöffneter Dateien bei 30.000. Bei Systemen mit weniger als oder gleich 12 GB liegt die maximale Anzahl geöffneter Dateien bei 10.000.

  Tabelle 114 Verbindung und maximale Anzahl geöffneter Dateien

DDR-Modelle	Speicher	Verbindungslimit	Maximale Anzahl geöffneter Dateien
DD620, DD630, DD640	8 GB	300	10.000

Tabelle 114 Verbindung und maximale Anzahl geöffneter Dateien (Fortsetzung)

DDR-Modelle	Speicher	Verbindungslimit	Maximale Anzahl geöffneter Dateien
DD640	16 GB	600	30.000
DD640	20 GB	600	30.000
DD860	36 GB	600	30.000
DD860, DD860ArT	72 GB	600	30.000
	96 GB	600	30.000
	128 GB	600	30.000
	256 GB	600	30.000

Hinweis

Das System hat eine maximale Grenze von 600 CIFS-Verbindungen und 10.000 offenen Dateien. Wenn das System keine offenen Dateien mehr übrig hat, kann die Anzahl der Dateien vergrößert werden.

Hinweis

Dateizugriffslatenzen werden durch die Anzahl der Dateien in einem Verzeichnis beeinträchtigt. Es wird empfohlen, soweit wie möglich, Verzeichnisgrößen von weniger als 250.000 einzuhalten. Bei größeren Verzeichnisgrößen kommt es evtl. zu langsameren Antworten auf Metadatenvorgänge wie das Auflisten der Dateien im Verzeichnis und das Öffnen oder Erstellen einer Datei.

Data Domain-Systemuhr

Wenn Sie den Active Directory-Modus für den CIFS-Zugriff verwenden, darf die Data Domain-Systemuhrzeit maximal fünf Minuten von der des Domain Controllers abweichen.

Die DD System Manager-Registerkarte **Administration** > **Settings** > **Time and Date Settings** synchronisiert die Uhr mit einem Zeitserver.

Da der Windows-Domänencontroller die Uhrzeit von einer externen Quelle bezieht, muss NTP konfiguriert werden. Anweisungen zur Konfiguration von NTP für die Windows-Betriebssystemversion oder das Service Pack auf dem Domain Controller finden Sie in der Microsoft-Dokumentation .

Im Active Directory-Authentifizierungsmodus synchronisiert das Data Domain-System die Uhr regelmäßig mit einem Active Directory-Domänencontroller.

Synchronisieren von einem Windows-Domaincontroller

Verwenden Sie die Befehlszeile auf einem Windows-Domaincontroller für die Synchronisation mit einem NTP-Server.

Hinweis

Dieses Beispiel gilt für Windows 2003 SP1. Ersetzen Sie den Namen des NTP-Servers (*ntpservername*) durch Ihren Domain-Server.

Vorgehensweise

1. Geben Sie auf dem Windows-System Befehle wie den folgenden ein:

   ```
   C:\>w32tm /config /syncfromflags:manual /manualpeerlist: ntp-server-name C:\>w32tm /config /update C:\>w32tm /resync
   ```

2. Nachdem NTP auf dem Domain Controller konfiguriert wurde, konfigurieren Sie die Zeitserversynchronisation, wie im Abschnitt zur Arbeit mit Zeit- und Datumseinstellungen beschrieben.

Synchronisieren von einem NTP-Server

Konfigurieren Sie die Zeitserversynchronisation, wie im Abschnitt zur Arbeit mit Zeit- und Datumseinstellungen beschrieben.

KAPITEL 9

NFS

Inhalt dieses Kapitels:

Überblick über NFS

NFS-Clients können auf Systemverzeichnisse oder MTrees auf dem Data Domain-System zugreifen.

- Das Verzeichnis `/backup` ist das Standardzielverzeichnis für komprimierte Nicht-MTree-Backupserverdaten.
- Der Pfad `/data/col1/backup` ist das Root-Ziel bei der Verwendung von MTrees für komprimierte Backupserverdaten.
- Das Verzeichnis `/ddvar/core` enthält Data Domain-Core- und -Protokolldateien (löschen Sie alte Protokolle und Core-Dateien, um Speicherplatz in diesem Bereich freizugeben).

Hinweis

Auf Data Domain-Systemen befindet sich `/ddvar/core` auf einer separaten Partition. Wenn Sie nur `/ddvar` mounten, können Sie nicht zu `/ddvar/core` vom `/ddvar`-Mount-Punkt navigieren.

Clients, z. B. Backupserver, die Backup- und Wiederherstellungsvorgänge mit mindestens einem Data Domain-System durchführen, benötigen Zugriff auf den Bereich `/backup` oder `/data/col1/backup`. Clients, die über einen administrativen Zugriff verfügen, müssen auch in der Lage sein, auf das Verzeichnis `/ddvar/core` zuzugreifen, um Core- und Protokolldateien abzurufen.

Als Teil der ersten Data Domain-Systemkonfiguration wurden NFS-Clients dafür konfiguriert, auf diese Bereiche zuzugreifen. In diesem Kapitel wird erläutert, wie Sie diese Einstellungen ändern und den Datenzugriff managen.

Hinweis

- Informationen zur Erstkonfiguration des Systems finden Sie im *Data Domain Operating System Initial Configuration Guide*.
- Der Befehl `nfs` managt Backups und Wiederherstellungen zwischen NFS-Clients und Data Domain-Systemen und zeigt NFS-Statistiken und den Status an. Umfassende Informationen zum Befehl `nfs` finden Sie im *Data Domain Operating System Command Reference Guide*.
- Informationen zum Einrichten von Drittanbieterclients zur Verwendung des Data Domain-Systems als Server finden Sie im entsprechenden Tuning-Leitfaden, z. B. in *Solaris System Tuning*, der auf der Data Domain-Support-Website verfügbar ist. Wählen Sie auf der Seite „Documentation >Integration Documentation“ den Hersteller aus der Liste aus und klicken Sie auf **OK**. Wählen Sie den gewünschten Tuning-Leitfaden aus der Liste aus.

HA-Systeme und NFS

HA-Systeme sind mit NFS kompatibel. Wenn ein NFS-Job während eines Failover durchgeführt wird, muss der Job **nicht** neu gestartet werden.

Hinweis

„/ddvar“ ist ein ext3-Dateisystem und kann nicht wie eine normale MTree-basierte Share freigegeben werden. Die Informationen in /ddvar sind veraltet, wenn ein Failover des aktiven Node auf den Stand-by-Node durchgeführt wird, da sich die Dateihandles auf den zwei Nodes unterscheiden. Wenn „/ddvar“ gemountet wird, um auf Protokolldateien zuzugreifen oder das System zu aktualisieren, unmounten und remounten Sie „/ddvar“, wenn ein Failover seit dem letzten Mounten von „/ddvar“ durchgeführt wurde.

Um gültige NFS-Exporte zu erstellen, die zu einem Failover mit HA führen, muss der Export aus dem aktiven HA-Node erstellt und in der Regel über die Failover-Netzwerkschnittstellen freigegeben werden.

Verwalten des NFC-Clientzugriffs auf das Data Domain-System

Die Themen in diesem Abschnitt beschreiben, wie Sie den NFS-Clientzugriff auf ein Data Domain-System verwalten.

Aktivieren von NFS-Services

Aktivieren Sie NFS-Services, um den Clientzugriff auf das System mithilfe das NFS-Protokolls zu ermöglichen.

Vorgehensweise

1. Wählen Sie **Protocols** > **NFS**.

   Die NFS-Ansicht zeigt die Registerkarte "Exports" an.

2. Klicken Sie auf **Aktivieren**.

Deaktivieren von NFS-Services

Deaktivieren Sie NFS-Services, um den Clientzugriff auf das System mithilfe des NFS-Protokolls zu verhindern.

Vorgehensweise

1. Wählen Sie die Registerkarten **Protocols** > **NFS**.

   Die NFS-Ansicht zeigt die Registerkarte "Exports" an.

2. Klicken Sie auf **Deaktivieren**.

Erstellen eines Exports

Mithilfe der Schaltfläche „Create“ in Data Domain System Manager in der Ansicht „NFS“ oder dem Konfigurationsassistenten können Sie die NFS-Clients angeben, die auf die Bereiche `/backup`, `/data/col1/backup`,`/ddvar` und `/ddvar/core` oder den Bereich `/ddvar/ext` zugreifen können, falls dieser vorhanden ist.

Ein Data Domain-System unterstützt maximal 2048 Exporte[2], wobei die Anzahl der Verbindungen je nach Systemarbeitsspeicher skaliert werden kann.

2. Kann von Hardware-Einschränkungen betroffen sein.

Hinweis

Sie müssen den Clientzugriff separat zu jedem Export zuweisen und den Zugriff separat von jedem Export entfernen. Beispielsweise kann ein Client von `/ddvar` entfernt werden und weiterhin Zugriff auf `/data/col1/backup` haben.

⚠ ACHTUNG

Wenn eine Replikation implementiert werden soll, kann ein einziges Data Domain-Zielsystem Backups von CIFS-Clients und NFS-Clients empfangen, solange hierzu separate Verzeichnisse oder MTrees verwendet werden. CIFS- und NFS-Daten dürfen nicht im selben Bereich gemischt werden.

Vorgehensweise

1. Wählen Sie **Protocols > NFS**.

   Die NFS-Ansicht öffnet die Registerkarte „Exports“.

2. Klicken Sie auf **Create**.
3. Geben Sie den Pfadnamen in das Textfeld „Directory Path“ ein (z. B. `/data/col1/backup/dir1`).

   Hinweis

   `col1` verwendet den kleinen Buchstaben L, gefolgt von der Zahl 1.

4. Wählen Sie im Bereich „Clients“ einen vorhandenen Client aus oder klicken Sie auf das **+**-Symbol, um einen Client zu erstellen.

   Das Dialogfeld „Client“ wird angezeigt.

   a. Geben Sie einen Servernamen in das Textfeld ein.

   Geben Sie einen vollständig qualifizierten Domainnamen, Hostnamen oder IP-Adressen ein. Ein einzelner Stern (`*`) als Platzhaltersymbol zeigt an, dass alle Backupserver als Clients verwendet werden können.

   Hinweis

   Clients mit Zugriff auf das Verzeichnis `/data/col1/backup` haben Zugriff auf das gesamte Verzeichnis. Ein Client mit Zugriff auf ein Unterverzeichnis von `/data/col1/backup` kann nur auf dieses Unterverzeichnis zugreifen.

   - Ein Client kann ein vollständig qualifizierter Domainhostname, eine IPv4- oder IPv6-Adresse, eine IPv4-Adresse mit einer Netzmaske oder Präfixlänge, eine IPv6-Adresse mit Präfixlänge, ein NIS-Netzgruppenname mit dem Präfix `@` oder ein Sternchen-Platzhalter `(*)` mit einem Domainnamen wie `*.yourcompany.com` sein.
   - Ein Client, der einem Unterverzeichnis unter `/data/col1/backup` hinzugefügt wird, hat nur auf dieses Unterverzeichnis Zugriff.
   - Geben Sie ein Sternchen (`*`) als Clientliste ein, um Zugriff auf alle Clients im Netzwerk zu gewähren.

   b. Aktivieren Sie die Kontrollkästchen der NFS-Optionen für den Client.

   Allgemein:

- Read-only permission (ro)
- Allow connections from ports below 1024 (secure) (Standardwert).

Anonymous UID/GID:

- Map requests from UID (user identifier) or GID (group identifier) 0 to the anonymous UID/GID (root _squash).
- Map all user requests to the anonymous UID/GID (all _squash).
- Use Default Anonymous UID/GID.

Allowed Kerberos Authentication Modes:

- Unauthenticated connections (sec=sys). Wählen Sie diese Option aus, um keine Authentifizierung zu verwenden.
- Authenticated Connections (sec=krb5).

Hinweis

Integrität und Datenschutz werden unterstützt, obwohl sie die Leistung erheblich verlangsamen können.

c. Klicken Sie auf **OK**.

5. Klicken Sie auf **OK**, um den Export zu erstellen.

Ändern eines Exports

Ändern Sie über die GUI den Verzeichnispfad, den Domainnamen und andere Optionen.

Vorgehensweise

1. Wählen Sie **Protocols** > **NFS**.

   Die NFS-Ansicht öffnet die Registerkarte „Exports“.

2. Aktivieren Sie das Kontrollkästchen eines Exports in der Tabelle „NFS Exports“.
3. Klicken Sie auf **Bearbeiten**.
4. Ändern Sie den Pfadnamen im Textfeld „Directory Path“.
5. Wählen Sie im Bereich „Clients“ einen anderen Client aus und klicken Sie auf das Stiftsymbol (Modify) oder auf **+**, um einen Client zu erstellen

   a. Geben Sie einen Servernamen in das Textfeld „Client“ ein.

   Geben Sie einen vollständig qualifizierten Domainnamen, Hostnamen oder IP-Adressen ein. Ein einzelner Stern (*) als Platzhaltersymbol zeigt an, dass alle Backupserver als Clients verwendet werden können.

   Hinweis

   Clients mit Zugriff auf das Verzeichnis `/data/col1/backup` haben Zugriff auf das gesamte Verzeichnis. Ein Client mit Zugriff auf ein Unterverzeichnis von `/data/col1/backup` kann nur auf dieses Unterverzeichnis zugreifen.

   - Ein Client kann ein vollqualifizierter Domainhostname, eine IPv4- oder IPv6-Adresse, eine IPv4-Adresse mit einer Netzmaske bzw. Präfixlänge, eine IPv6-Adresse mit Präfixlänge, ein NIS-Netzgruppenname mit dem

Präfix `@` oder ein Sternchen-Platzhalter (`*`) mit einem Domainnamen sein, zum Beispiel `*.yourcompany.com`.
Ein Client, der einem Unterverzeichnis unter `/data/col1/backup` hinzugefügt wird, hat nur auf dieses Unterverzeichnis Zugriff.

- Geben Sie ein Sternchen (`*`) als Clientliste ein, um Zugriff auf alle Clients im Netzwerk zu gewähren.

b. Aktivieren Sie die Kontrollkästchen der NFS-Optionen für den Client.

Allgemein:

- Read-only permission (ro)
- Allow connections from ports below 1024 (secure) (Standardwert).

Anonymous UID/GID:

- Map requests from UID (user identifier) or GID (group identifier) 0 to the anonymous UID/GID (root _squash).
- Map all user requests to the anonymous UID/GID (all _squash).
- Use Default Anonymous UID/GID.

Allowed Kerberos Authentication Modes:

- Unauthenticated connections (sec=sys). Wählen Sie diese Option aus, um keine Authentifizierung zu verwenden.
- Authenticated Connections (sec=krb5).

Hinweis

Integrität und Datenschutz werden nicht unterstützt.

c. Klicken Sie auf **OK**.

6. Klicken Sie auf **OK**, um den Export zu ändern.

Erstellen eines Exports aus einem vorhandenen Export

Erstellen Sie einen Export aus einem vorhandenen Export und ändern Sie ihn dann nach Bedarf.

Vorgehensweise

1. Klicken Sie in der Registerkarte „NFS Exports“ auf das Kontrollkästchen des Exports, den Sie als Quelle verwenden möchten.
2. Klicken Sie auf **Create From**.
3. Ändern Sie die Exportinformationen, wie im Abschnitt zur Änderung eines Exports beschrieben.

Löschen von Exporten

Löschen Sie einen Export in der Registerkarte „NFS Exports“.

Vorgehensweise

1. Aktivieren Sie in der Registerkarte „NFS Exports“ das Kontrollkästchen des Exports, den Sie löschen möchten.

2. Klicken Sie auf **Delete**.
3. Klicken Sie auf **OK** und **Close**, um den Export zu löschen.

Anzeigen von NFS-Informationen

Die Themen in diesem Abschnitt beschreiben, wie Sie DD System Manager dazu verwenden, den NFS-Clientstatus und die NFS-Konfiguration zu überwachen.

Anzeigen des NFS-Status

Zeigen Sie an, ob NFS aktiv und ob Kerberos aktiviert ist.

Vorgehensweise

- Klicken Sie auf **Protocols** > **NFS**.

  Im oberen Fenster wird der Betriebsstatus von NFS angezeigt, z. B., ob NFS derzeit aktiv und in Betrieb ist und ob der Kerberos-Modus aktiviert ist.

  Hinweis

  Klicken Sie auf "Configure", um die Registerkarte **Administration** > **Access** > **Authentication** anzuzeigen, auf der Sie die Kerberos-Authentifizierung konfigurieren können.

Anzeigen von NFS-Exporten

Zeigen Sie die Liste der Clients an, die auf das Data Domain-System zugreifen dürfen.

Vorgehensweise

1. Klicken Sie auf **Protocols** > **NFS**.

   In der Ansicht „Exports“ wird eine Tabelle mit NFS-Exporten angezeigt, die für das Data Domain-System konfiguriert sind. Außerdem werden der Mount-Pfad, der Status und die NFS-Optionen für jeden Export angezeigt.

2. Klicken Sie auf einen Export in der Tabelle, um den Bereich mit detaillierten Informationen unter der Tabelle „Exports“ zu füllen.

   Neben dem Verzeichnispfad des Exports, den konfigurierten Optionen und dem Status zeigt das System auch eine Liste der Clients an.

   Verwenden Sie das Textfeld „Filter By“, um nach Mountpfad zu sortieren.

   Klicken Sie für das System auf **Update**, um die Tabelle zu aktualisieren und die angegebenen Filter anzuwenden.

   Klicken Sie für das System auf **Reset**, um die Pfad- und Clientfilter zu löschen.

Anzeigen der aktiven NFS-Clients

Zeigen Sie alle Clients, die in den letzten 15 Minuten verbunden wurden, mit ihrem Mount-Pfad an.

Vorgehensweise

- Wählen Sie die Registerkarte **Protocols** > **NFS** > **Active Clients**.

Die Ansicht „Active Clients“ wird geöffnet und zeigt alle Clients, die in den letzten 15 Minuten verbunden wurden, mit ihrem Mount-Pfad an.

Verwenden Sie die Textfelder „Filter By“, um nach Mount-Pfad und Clientname zu sortieren.

Klicken Sie für das System auf **Update**, um die Tabelle zu aktualisieren und die angegebenen Filter anzuwenden.

Klicken Sie für das System auf **Reset**, um die Pfad- und Clientfilter zu löschen.

Integrieren eines DDR in eine Kerberos-Domain

Legen Sie den Domainnamen, den Hostnamen und den DNS-Server für den DDR fest.

Ermöglichen Sie es dem DDR, den Authentifizierungsserver als Key Distribution Center (für UNIX) bzw. als Distribution Center (für Windows Active Directory) zu verwenden.

⚠ ACHTUNG

Die Beispiele in dieser Beschreibung sind spezifisch für das Betriebssystem-(OS), das verwendet wurde, um diese Übung zu entwickeln. Sie müssen die Befehle verwenden, die für Ihr Betriebssystem spezifisch sind.

Hinweis

Für den UNIX Kerberos-Modus muss eine keytab-Datei vom KDC-Server (Key Distribution Center), in dem sie erzeugt wird, zum DDR übertragen werden. Wenn Sie mehr als einen DDR verwenden, erfordert jeder DDR eine separate keytab-Datei. Die keytab-Datei enthält den freigegebenen Schlüssel zwischen dem KDC-Server und dem DDR.

Hinweis

Bei Verwendung eines UNIX-KDC muss der DNS-Server nicht der KDC-Server sein, er kann auch ein separater Server sein.

Vorgehensweise

1. Legen Sie den Hostnamen und den Domainnamen für den DDR mit DDR-Befehlen fest.

   ```
   net set hostname <host>
   ```

   ```
   net set {domainname <local-domain-name>}
   ```

   Hinweis

   Der Hostname ist der Name des DDR.

2. Konfigurieren Sie den NFS-Prinzipal (Node) für den DDR auf dem Key Distribution Center (KDC).

   Beispiel:

   ```
   addprinc nfs/hostname@realm
   ```

   Hinweis

   Hostname ist der Name für den DDR.

3. Überprüfen Sie, ob NFS-Einträge als Prinzipale auf dem KDC hinzugefügt werden.

   Beispiel:
   listprincs
   ```
   nfs/hostname@realm
   ```

4. Fügen Sie den DDR-Prinzipal in eine keytab-Datei hinzu.

   Beispiel:
   ktadd <keytab_file> nfs/hostname@realm

5. Überprüfen Sie, ob eine NFS-keytab-Datei auf dem KDC konfiguriert ist.

   Beispiel:
   klist -k <keytab_file>

   Hinweis

   <keytab_file> ist die keytab-Datei, die in einem vorherigen Schritt verwendet wurde, um Schlüssel zu konfigurieren.

6. Kopieren Sie die keytab-Datei vom Speicherort, an dem die Schlüssel für NFS DDR erzeugt werden, zum DDR im Verzeichnis /ddvar/.

   Tabelle 115 Keytab-Ziel

Kopieren Sie die Datei von:	Kopieren Sie die Datei in:
<keytab_file> (die keytab-Datei, die in einem vorherigen Schritt konfiguriert wurde)	/ddvar/

7. Legen Sie den Bereich auf dem DDR mit dem folgenden DDR-Befehl fest:

   authentication kerberos set realm <home realm> kdc-type <unix, windows.> kdcs <IP address of server>

8. Wenn der kdc-type UNIX ist, importieren Sie die keytab-Datei aus /ddvar/ in /ddr/etc/, wo die Kerberos-Konfigurationsdatei erwartet wird. Verwenden Sie den folgenden DDR-Befehl, um die Datei zu kopieren:

   authentication kerberos keytab import

   HINWEIS

   Dieser Schritt ist nur erforderlich, wenn UNIX der kdc-type ist.

   Die Kerberos-Einrichtung ist nun abgeschlossen.

9. Um einen NFS-Mount-Punkt hinzuzufügen und so Kerberos verwenden zu können, verwenden Sie den Befehl „nfs add“.

   Weitere Informationen finden Sie im *Data Domain Operating System Command Reference Guide*.

10. Fügen Sie Host, NFS und relevante Benutzerprinzipale für jeden NFS-Client auf dem Key Distribution Center (KDC) hinzu.

    Beispiel: **listprincs**

```
host/hostname@realm
nfs/hostname@realm
root/hostname@realm
```

11. Importieren Sie für jeden NFS-Client alle seine Prinzipale in eine keytab-Datei auf dem Client.

    Beispiel:
    ktadd -k <keytab_file> host/hostname@realm

    ktadd -k <keytab_file> nfs/hostname@realm

Hinzufügen und Löschen von KDC-Servern nach der Erstkonfiguration

Nachdem Sie einen DDR in eine Kerberos-Domain integriert und dadurch den DDR dafür aktiviert haben, den Authentifizierungsserver als Key Distribution Center (für UNIX) und als Distribution Center (für Windows Active Directory) zu verwenden, können Sie mit dem folgenden Verfahren KDC-Server hinzufügen oder entfernen.

Vorgehensweise

1. Verbinden Sie den DDR mit einem AD-Server (Active Directory) oder einem UNIX Key Distribution Center (KDC).

   authentication kerberos set realm <home-realm> kdc-type {windows [kdcs <kdc-list>] | unix kdcs <kdc-list>}

   Beispiel: **authentication kerberos set realm krb5.test kdc-type unix kdcs nfskrb-kdc.krb5.test**

   Dieser Befehl verbindet das System mit dem Bereich krb5.test und aktiviert die Kerberos-Authentifizierung für NFS-Clients.

   Hinweis

   Ein keytab, das auf diesem KDC erzeugt wird, muss auf dem DDR vorhanden sein, um die Kerberos-Authentifizierung verwenden zu können.

2. Überprüfen Sie die Kerberos-Authentifizierungskonfiguration.

   authentication kerberos show config

   ```
   Home Realm:          krb5.test
   KDC List:            nfskrb-kdc.krb5.test
   KDC Type:            unix
   ```

3. Fügen Sie einen zweiten KDC-Server hinzu.

   authentication kerberos set realm <home-realm> kdc-type {windows [kdcs <kdc-list>] | unix kdcs <kdc-list>}

   Beispiel: **authentication kerberos set realm krb5.test kdc-type unix kdcs ostqa-sparc2.krb5.test nfskrb-kdc.krb5.test**

   Hinweis

   Ein keytab, das auf diesem KDC erzeugt wird, muss auf dem DDR vorhanden sein, um die Kerberos-Authentifizierung verwenden zu können.

4. Überprüfen Sie, ob zwei KDC-Server hinzugefügt wurden.

   authentication kerberos show config

```
Home Realm:           krb5.test
KDC List:             ostqa-sparc2.krb5.test, nfskrb-
kdc.krb5.test
KDC Type:             unix
```

5. Zeigen Sie den Wert für den Kerberos-Konfigurationsschlüssel an.

   reg show config.keberos

```
config.kerberos.home_realm = krb5.test
config.kerberos.home_realm.kdc1 = ostqa-sparc2.krb5.test
config.kerberos.home_realm.kdc2 = nfskrb-kdc.krb5.test
config.kerberos.kdc_count = 2
config.kerberos.kdc_type = unix
```

6. Löschen Sie einen KDC-Server.

   Löschen Sie einen KDC-Server, indem Sie den Befehl **authentication kerberos set realm <home-realm> kdc-type {windows [kdcs <kdc-list>] | unix kdcs <kdc-list>}** verwenden, ohne den KDC-Server aufzulisten, den Sie löschen möchten. Wenn beispielsweise die vorhandenen KDC-Server kdc1, kdc2 und kdc3 sind und Sie kdc2 aus dem Bereich entfernen möchten, können Sie das folgende Beispiel verwenden:

   authentication kerberos set realm <realm-name> kdc-type <kdc_type> kdcs kdc1,kdc3

KAPITEL 10

NFSv4

Inhalt dieses Kapitels:

Einführung in NFSv4

Da NFS-Clients zunehmend NFSv4.x als NFS-Standardprotokollebene verwenden, können Data Domain-Systeme nun NFSv4 einsetzen. Der Client muss dann nicht in einem Abwärtskompatibilitätsmodus arbeiten.

In Data Domain-Systemen können Clients in gemischten Umgebungen arbeiten, in denen NFSv4 und NFSv3 auf dieselben NFS-Exporte zugreifen können sollten.

Der Data Domain-NFS-Server kann so konfiguriert werden, dass NFSv4 und NFSv3 unterstützt werden (je nach den Anforderungen vor Ort). Sie können jeden NFS-Export nur NFSv4-Clients, nur NFSv3-Clients oder beiden zur Verfügung stellen.

Verschiedene Faktoren beeinflussen, ob Sie NFSv4 oder NFSv3 wählen:

- NFS-Clientunterstützung
  Einige NFS-Clients unterstützen evtl. nur NFSv3 oder NFSv4 oder funktionieren besser mit einer Version.
- Vorgangsanforderungen
  In einem Unternehmen gibt es evtl. strenge Standards in Bezug auf die NFS-Verwendung (entweder NFSv4 oder NFSv3).
- Sicherheit
  Wenn Sie mehr Sicherheit benötigen, ist NFSv4 besser geeignet als NFSv3, einschließlich ACL und erweiterte Eigentümer- und Gruppenkonfiguration.
- Funktionsanforderungen
  Wenn eine Bytebereichssperre oder UTF-8-Dateien erforderlich sind, sollten Sie NFSv4 wählen.
- NFSv3-Submounts
  Wenn die vorhandene Konfiguration NFSv3-Submounts verwendet, ist möglicherweise NFSv3 die richtige Wahl.

NFSv4 im Vergleich zu NFSv3 auf Data Domain-Systemen

NFSv4 bietet mehr Funktionalität und Funktionen im Vergleich zu NFSv3.

Die folgende Tabelle vergleicht NFSv3-Funktionen mit NFSv4-Funktionen.

Funktion	NFSv3	NFSv4
Standardbasiertes Netzwerk-Dateisystem	Ja	Ja
Kerberos-Unterstützung	Ja	Ja
Kerberos mit LDAP	Ja	Ja
Quotenreporting	Ja	Ja
Mehrere Exporte mit clientbasierten Zugriffslisten	Ja	Ja
ID-Zuordnung	Ja	Ja
Unterstützung für UTF-8	Nein	Ja
Datei-/Verzeichnisbasierte Zugriffskontrolllisten (ACLs)	Nein	Ja
Eigentümer/Gruppe erweitert (OWNER@)	Nein	Ja
Sperrung von Dateifreigaben	Nein	Ja
Sperrung des Bytebereichs	Nein	Ja

Funktion	NFSv3	NFSv4
DD-CIFS-Integration (Sperre, ACL, AD)	Nein	Ja
Öffnung und Recovery von zustandsorientierter Datei	Nein	Ja
Globaler Namespace und pseudoFS	Nein	Ja
Multi-System-Namespace mit Referrals	Nein	Ja

NFSv4-Ports

Sie können NFSv4 und NFSv3 unabhängig aktivieren oder deaktivieren. Darüber hinaus können Sie NFS-Versionen auf unterschiedliche Ports verschieben; beide Versionen müssen sich nicht auf demselben Port befinden.

Für NFSv4 müssen Sie nicht das Data Domain-Datei-System neu starten, wenn Sie Ports ändern. In solchen Fällen ist nur ein NFS-Neustart erforderlich.

Wie NFSv3 wird NFSv4 auf Port 2049 als Standard ausgeführt (bei Aktivierung).

NFSv4 verwendet nicht Portmapper (Port 111) oder mountd (Port 2052).

ID-Zuordnung – Übersicht

NFSv4 identifiziert Eigentümer und Gruppen durch ein gemeinsames externes Format, wie `joe@example.com`. Diese gängigen Formate werden als Kennungen oder IDs bezeichnet.

Kennungen werden auf einem NFS-Server gespeichert und verwenden interne Darstellungen wie ID 12345 oder ID S-123-33-667-2. Die Konvertierung zwischen internen und externen Kennungen wird als ID-Zuordnung bezeichnet.

Kennungen sind verbunden mit:

- Eigentümern von Dateien und Verzeichnissen
- Eigentümergruppen von Dateien und Verzeichnissen
- Einträgen in Zugriffskontrolllisten (Access Control Lists, ACLs)

Data Domain-Systeme verwenden ein gemeinsames internes Format für NFS- und CIFS/SMB-Protokolle, das die gemeinsame Verwendung von Dateien und Verzeichnissen durch NFS und CIFS/SMB ermöglicht. Jedes Protokoll konvertiert das interne Format in ein eigenes externes Format mit eigener ID-Zuordnung.

Externe Formate

Das externe Format für NFSv4-Kennungen folgt NFSv4-Standards (z. B. RFC-7530 für NFSv4.0). Darüber hinaus werden zusätzliche Formate für Interoperabilität unterstützt.

Standardmäßige Kennungsformate

Standardmäßige externe Kennungen für NFSv4 haben das Format *`identifier@domain`*. Diese Kennung wird für NFSv4-Eigentümer, -Eigentümergruppen, und -Zugriffskontrolleinträge (ACEs) verwendet. Die Domäne muss mit der konfigurierten NFSv4-Domain übereinstimmen, die mit dem Befehl `nfs option` festgelegt wurde.

Das folgende CLI-Beispiel legt die NFSv4-Domain auf `mycorp.com` für den Data Domain-NFS-Server:

```
nfs option set nfsv4-domain myCorp.com
```

Informieren Sie sich in der clientspezifischen Dokumentation über das Festlegen der Client-NFS-Domain. Je nach Betriebssystem müssen Sie eine Konfigurationsdatei aktualisieren (z. B. `/etc/idmapd.conf`) oder ein Clientverwaltungstool verwenden.

Hinweis

Wenn Sie nicht den Standardwert festlegen, folgt sie dem DNS-Namen für das Data Domain-System.

Hinweis

Das Dateisystem muss nach dem Ändern der DNS-Domain neu gestartet werden, damit nfs4-domain automatisch aktualisiert wird.

Erweiterte ACE-Kennungen

Für ACL-ACE-Einträge unterstützt Data Domain-NFS-Server auch folgende standardmäßige erweiterte NFSv4-ACE-Kennungen (definiert durch NFSv4-RFC):

- OWNER@, der Eigentümer der Datei oder des Verzeichnisses
- GROUP@, die aktuelle Eigentümergruppe der Datei oder des Verzeichnisses
- spezielle Kennungen: INTERACTIVE@, NETWORK@, DIALUP@, BATCH@, ANONYMOUS@, AUTHENTICATED@, SERVICE@

Alternative Formate

Um Interoperabilität zu ermöglichen, unterstützen NFSv4-Server auf Data Domain-Systemen einige alternative Kennungsformate für Eingabe und Ausgabe.

- Numerische Kennungen; zum Beispiel „12345“.
- Windows-kompatible Sicherheitskennungen (SIDs) ausgedrückt als „S-NNN-NNN-...“

In den Abschnitten zur Eingabe- und Ausgabezuordnung finden Sie weitere Informationen zu Einschränkungen in Bezug auf diese Formate.

Interne Kennungsformate

Das Data Domain-Dateisystem speichert Kennungen mit jedem Objekt (Datei oder Verzeichnis) im Dateisystem. Alle Objekte haben eine numerische Benutzer-ID (UID) und Gruppen-ID (GID). Diese, zusammen mit einer Reihe von Mode Bits, ermöglichen traditionelle UNIX/Linux-Identifizierung und Zugriffskontrollen.

Objekte, die mit dem CIFS/SMB-Protokoll oder dem NFSv4-Protokoll (NFSv4-ACLs aktiviert) erstellt werden, haben auch eine erweiterte Sicherheitsbeschreibung (Security Descriptor, SD). Jede SD enthält Folgendes:

- Eigentümersicherheitskennung (SID)
- Eigentümergruppen-SID
- Beliebige Zugriffskontrollliste (DACL)
- (Optional) System-ACL (SACL)

Jede SID enthält eine relative ID (RID) und eine andere Domain in einer ähnlichen Weise wie Windows-SIDs. Im Abschnitt zu NFSv4- und CIFS-Interoperabilität finden Sie weitere Informationen zu SIDs und der Zuordnung von SIDs.

ID-Zuordnung

Der Data Domain-NFSv4-Server führt eine Zuordnung unter den folgenden Umständen durch:

- Eingangszuordnung
  Der Data Domain-NFS-Server erhält eine Kennung von einem NFSv4-Client. Siehe Eingangszuordnung auf Seite 283.
- Ausgangszuordnung:
  Eine Kennung wird vom Data Domain-NFS-Server an den NFSv4-Client gesendet. Siehe Ausgangszuordnung auf Seite 283.
- Zuordnung von Anmeldedaten
  Die Anmeldedaten des RPC-Clients werden einer internen Identität für Zugriffskontrolle und andere Vorgänge zugeordnet. Siehe Zuordnung von Anmeldedaten auf Seite 284.

Eingangszuordnung

Eine Eingangszuordnung tritt auf, wenn ein NFSv4-Client eine Kennung an den Data Domain-NFSv4-Server sendet, beispielsweise beim Festlegen des Eigentümers oder der Eigentümergruppe einer Datei. Die Eingabezuordnung unterscheidet sich von der Anmeldedatenzuordnung. Weitere Informationen zur Anmeldedatenzuordnung finden Sie unter xxxx.

Standardformatkennungen wie `joe@mycorp.com` werden in eine interne UID/GID konvertiert, basierend auf den konfigurierten Konvertierungsregeln. Wenn NFSv4-ACLs aktiviert sind, wird auch eine SID generiert, basierend auf den konfigurierten Konvertierungsregeln.

Die numerischen Kennungen (beispielsweise 12345) werden direkt in entsprechende UID/GIDs konvertiert, wenn der Client keine Kerberos-Authentifizierung verwendet. Wenn Kerberos verwendet wird, wird ein Fehler generiert, wie durch den NFSv4-Standard empfohlen. Wenn NFSv4-ACLs aktiviert sind, wird eine SID basierend auf den Konvertierungsregeln generiert.

Windows-SIDs (z. B. „S-NNN-NNN-...“) werden validiert und direkt in die entsprechenden SIDs konvertiert. Eine UID/GID wird basierend auf den Konvertierungsregeln generiert.

Ausgangszuordnung

Eine Ausgangszuordnung tritt auf, wenn der NFSv4-Server eine Kennung an den NFSv4-Client sendet, beispielsweise wenn der Server den Eigentümer oder die Eigentümergruppe einer Datei zurückgibt.

1. Bei Konfiguration kann die Ausgabe die numerische ID sein.
   Dies kann nützlich für NFSv4-Clients sein, die nicht für die ID-Zuordnung konfiguriert sind (z. B. einige Linux-Clients).
2. Es wird versucht, die Zuordnung mit den konfigurierten Zuordnungsservices (z. B. NIS oder Active Directory) durchzuführen.
3. Die Ausgabe ist eine numerische ID- oder SID-Zeichenfolge, wenn die Zuordnung fehlschlägt und die Konfiguration zulässig ist.

4. Ansonsten wird „nobody“ zurückgegeben.

nfs option *nfs4-idmap-out-numeric* konfiguriert die Zuordnung bei der Ausgabe:

- Wenn **nfs option *nfs4-idmap-out-numeric*** auf **map-first** festgelegt ist, wird versucht, eine Zuordnung durchzuführen. Bei einem Fehler wird eine numerische Zeichenfolge ausgegeben, falls zulässig. Dies ist die Standardeinstellung.
- Wenn **nfs option *nfs4-idmap-out-numeric*** auf **always**festgelegt wird, ist die Ausgabe immer eine numerische Zeichenfolge, falls zulässig.
- Wenn **nfs option *nfs4-idmap-out-numeric*** auf **never** festgelegt wird, wird versucht, eine Zuordnung durchzuführen. Bei einem Fehler lautet die Ausgabe: **nobody@nfs4-domain**.
  Wenn die RPC-Verbindung GSS/Kerberos verwendet, ist eine numerische Zeichenfolge nie zulässig und **nobody@nfs4-domain** ist die Ausgabe.

Im folgenden Beispiel wird der Data Domain-NFS-Server so konfiguriert, dass er immer versucht, eine numerische Zeichenfolge auszugeben. Für Kerberos wird der Name „nobody“ zurückgegeben:

```
nfs option set nfs4-idmap-out-numeric always
```

Zuordnung von Anmeldedaten

Der NFSv4-Server stellt Anmeldedaten für den NFSv4-Client bereit.

Diese Anmeldedaten haben die folgenden Funktionen:

- Bestimmen der Zugriffs-Policy für den Vorgang; beispielsweise Fähigkeit, eine Datei zu lesen.
- Bestimmen des Standardeigentümers und der Standardeigentümergruppe für neue Dateien und Verzeichnisse

Vom Client gesendete Anmeldedaten sind evtl. `john_doe@mycorp.com` oder Systemanmeldedaten wie `UID=1000, GID=2000`. Systemanmeldedaten geben eine UID/GID zusammen mit Hilfsgruppen-IDs an.

Wenn NFSv4-ACLs deaktiviert sind, werden die UID/GID und die Hilfsgruppen-IDs für die Anmeldedaten verwendet.

Wenn NFSv4-ACLs aktiviert sind, werden die konfigurierten Zuordnungsservices verwendet, um eine erweiterte Sicherheitsbeschreibung für die Anmeldedaten zu erstellen:

- SIDs für Eigentümer, Eigentümergruppe und Hilfsgruppe werden zugeordnet und zur Sicherheitsbeschreibung (Security Descriptor, SD) hinzugefügt.
- Anmeldedatenberechtigungen werden (falls vorhanden) zur SD hinzugefügt.

NFSv4- und CIFS/SMB-Interoperabilität

Die Sicherheitsbeschreibungen, die von NFSv4 und CIFS verwendet werden, ähneln sich aus Sicht der ID-Zuordnung. Es gibt jedoch Unterschiede.

Für optimale Interoperabilität sollten Sie Folgendes beachten:

- Active Directory sollte für CIFS und NFSv4 konfiguriert sein und der NFS ID Mapper sollte so konfiguriert werden, dass Active Directory für die ID-Zuordnung verwendet wird.
- Wenn Sie oft CIFS-ACLs verwenden, können Sie die Kompatibilität in der Regel verbessern, indem Sie auch NFSv4-ACLs aktivieren.

  - Durch das Aktivieren von NFSv4-ACLs können NFSv4-Anmeldedaten bei der Evaluierung des DACL-Zugriffs der entsprechenden SID zugeordnet werden.
- Der CIFS-Server erhält Anmeldedaten vom CIFS-Client, einschließlich Standard-ACL und Benutzerberechtigungen.
  - Im Gegensatz dazu erhält der NFSv4-Server einen begrenzteren Satz von Anmeldedaten und erstellt Anmeldedaten zur Laufzeit mit seinem ID Mapper. Aus diesem Grund sieht das Dateisystem evtl. unterschiedliche Anmeldedaten.

CIFS/SMB – Active Directory-Integration

Der Data Domain-NFSv4-Server kann so konfiguriert werden, dass er die Windows Active Directory-Konfiguration verwendet, die mit dem Data Domain-CIFS-Server festgelegt ist.

Das Data Domain-System wird zugeordnet, um Active Directory zu verwenden, wenn möglich. Diese Funktion ist standardmäßig deaktiviert, aber Sie können sie mit dem folgenden Befehl aktivieren:

```
nfs option set nfs4-idmap-active-directory enabled
```

Standard-DACL für NFSv4

NFSv4 legt eine andere Standard-DACL (beliebige Zugriffskontrollliste) als die von CIFS bereitgestellte Standard-DACL fest.

Nur OWNER@, GROUP@ und EVERYONE@ werden in der standardmäßigen NFSv4-DACL definiert. Mit ACL-Vererbung können Sie standardmäßig automatisch CIFS-relevante ACEs hinzufügen (falls angemessen).

Systemstandard-SIDs

Dateien und Verzeichnisse, die von NFSv3 und NFSv4 ohne ACLs erstellt werden, verwenden die standardmäßige Systemdomain, die manchmal als UNIX-Standarddomain bezeichnet wird:

- Benutzer-SIDs in der Systemdomain haben das Format `S-1-22-1-N`, wobei N die UID ist.
- Gruppen-SIDs in der Systemdomain haben das Format `S-1-22-2-N`, wobei N die GID ist.
  Beispielsweise hat ein Benutzer mit `UID 1234` die Eigentümer-SID `S-1-22-1-1234`.

Gemeinsame Kennungen in NFSv4-ACLs und -SIDs

Die Kennung EVERYONE@ und andere spezielle Kennungen (wie beispielsweise BATCH@) in NFSv4-ACLs verwenden die äquivalenten CIFS-SIDs und sind kompatibel.

Die Kennungen OWNER@ und GROUP@ kommunizieren in CIFS nicht direkt; sie werden als aktueller Eigentümer und aktuelle Eigentümergruppe der Datei oder des Verzeichnisses angezeigt.

NFS-Referrals

Die Referral-Funktion ermöglicht einem NFSv4-Client den Zugriff auf einen Export (oder ein Dateisystem) an einem oder mehreren Speicherorten. Speicherorte können sich auf demselben NFS-Server oder auf verschiedenen NFS-Servern befinden und

entweder denselben oder einen anderen Pfad verwenden, um auf den Export zuzugreifen.

Da Referrals eine NFSv4-Funktion sind, gelten sie nur für NFSv4-Mounts.

Referrals können zu jedem beliebigen Server erfolgen, der NFSv4 oder höher verwendet, einschließlich:

- Data Domain-System mit NFS mit NFSv4
- Andere Server, die NFSv4 unterstützen (einschließlich Linux-Servern, NAS-Appliances und VNX-Systemen)

Ein Referral kann einen NFS-Exportpunkt mit oder ohne aktuellen zugrunde liegenden Pfad im Data Domain-Dateisystem verwenden.

NFS-Exporte mit Referrals können über NFSv3 gemountet werden, aber NFSv3-Clients werden nicht umgeleitet, da Referrals eine NFSv4-Funktion sind. Dieses Merkmal ist nützlich in Scale-out-Systemen, um Exporte auf Dateimanagementebene umleiten zu können.

Referral-Speicherorte

NFSv4-Referrals weisen immer einen oder mehrere Standorte auf.

Diese Speicherorte umfassen Folgendes:

- Pfad auf einem Remote-NFS-Server zum entsprechenden Dateisystem.
- Eine oder mehrere Server-Netzwerkadressen, mit denen der Client den Remote-NFS-Server erreichen kann

Wenn mehrere Serveradressen mit demselben Speicherort verknüpft sind, befinden sich diese Adressen in der Regel auf demselben NFS-Server.

Referral-Speicherortnamen

Sie können jeden Referral-Speicherort in einem NFS-Export benennen. Sie können den Namen verwenden, um auf das Referral zuzugreifen und es zu ändern oder zu löschen.

Eine Referral-Name kann maximal 80 Zeichen aus den folgenden Zeichensätzen enthalten:

- a-z
- A-Z
- 0-9
- "."
- ","
- "_"
- "-"

Hinweis

Sie können Leerzeichen verwenden, solange die Leerzeichen in den Namen eingebettet sind. Wenn Sie eingebettete Leerzeichen verwenden, müssen Sie den vollständigen Namen in doppelte Anführungszeichen setzen.

Namen, die mit "." beginnen, sind reserviert für die automatische Erstellung durch das Data Domain-System. Sie können diese Namen löschen, aber Sie können sie nicht

mithilfe der Befehlszeilenschnittstelle (CLI) oder System Management Services (SMS) erstellen oder ändern.

Referrals und Scale-out-Systeme

NFSv4-Referrals und -Speicherorte können besser Zugriff gewähren, wenn Sie ein Scale-out für Ihre Data Domain-Systeme durchführen.

Da Ihr Data Domain-System evtl. noch keinen globalen Namespace enthält, beschreiben die folgenden beiden Szenarios, wie Sie NFSv4-Referrals verwenden können:

- Ihr Data Domain-System enthält keinen globalen Namespace.
  - Mit NFSv4-Referrals können Sie diesen globalen Namespace erstellen. Systemadministratoren können diese globalen Namespaces erstellen oder Sie können nach Bedarf den intelligenten System Manager (SM) verwenden, um Referrals zu erstellen.
- Ihr Data Domain-System hat bereits einen globalen Namespace.
  - Wenn Ihr System einen globalen Namespace mit MTrees in bestimmten Nodes aufweist, können NFS-Referrals erstellt werden, um den Zugriff auf diese MTrees auf die Nodes umzuleiten, die zum Scale-out-System hinzugefügt wurden. Sie können diese Referrals erstellen oder automatisch in NFS ausführen, wenn die erforderlichen SM- oder File Manager(FM)-Informationen verfügbar sind.
    Weitere Informationen zur MTrees finden Sie im *Data Domain Operating System Administration Guide*.

NFSv4 und hohe Verfügbarkeit

Mit NFSv4 werden Protokollexporte (beispielsweise `/data/col1/<mtree>`) in einem High Availability(HA)-Setup gespiegelt. Jedoch werden Konfigurationsexporte wie `/ddvar` nicht gespiegelt.

Das `/ddvar`-Dateisystem ist einzigartig für jeden Node eines HA-Paars. Infolgedessen werden `/ddvar`-Exporte und die verbundenen Clientzugriffslisten nicht auf den Standby-Node in einer HA-Umgebung gespiegelt.

Die Informationen in `/ddvar` sind veraltet, wenn ein Failover vom aktiven Node zum Standby-Node stattfindet. Alle Clientberechtigungen, die `/ddvar` auf dem ursprünglichen aktiven Node gewährt werden, müssen nach dem Failover auf dem neuen aktiven Node neu erstellt werden.

Sie müssen ferner alle zusätzlichen /ddvar-Exporte und ihre Clients (beispielsweise `/ddvar/core`), die auf dem ursprünglichen aktiven Node erstellt wurden, nach einem Failover zum neuen aktiven Node hinzufügen.

Schließlich müssen Sie nach einem Failover alle gewünschten `/ddvar`-Exporte vom Client unmounten und dann wieder mounten.

Globale NFSv4-Namespaces

Der NFSv4-Server stellt einen virtuellen Verzeichnisbaum mit der Bezeichnung PseudoFS bereit, um NFS-Exporte in einer durchsuchbaren Gruppe von Pfaden zu verbinden.

Die Verwendung von PseudoFS unterscheidet NFSv4 von NFSv3, das das MOUNTD-Hilfsprotokoll verwendet.

In den meisten Konfigurationen ist die Änderung von NFSv3 MOUNTD zum globalen NFSv4-Namespace transparent und wird automatisch vom NFSv4-Client und -Server durchgeführt.

Globale NFSv4-Namespaces und NFSv3-Submounts

Wenn Sie NFSv3-Export-Submounts verwenden, verhindern globale Namespaces von NFSv4 evtl., dass Submounts auf dem NFSv4-Mount sichtbar sind.

Beispiel 1 NFSv3-Hauptexporte und Submount-Exporte

Wenn NFSv3 einen Hauptexport und einen Submount-Export aufweist, verwenden diese Exporte evtl. dieselben NFSv3-Clients, jedoch unterschiedliche Zugriffsebenen:

Export	Pfad	Client	Optionen
MT1	`/data/col1/mt1`	client1.example.com	ro
Mt1-sub	`/data/col1/mt1/subdir`	client1.example.com	rw

In der vorherigen Tabelle gilt für NFSv3 Folgendes:

- Wenn client1.example.com /data/col1/mt1 mountet, erhält der Client Lesezugriff.
- Wenn client1.example.com /data/col1/mt1/subdir mountet, erhält der Client Lese-/Schreibzugriff.

NFSv4 funktioniert auf dieselbe Weise in Bezug auf Exportpfade auf oberster Ebene. Für NFSv4 navigiert client1.example.com durch das NFSv4-PseudoFS, bis er den Exportpfad auf oberster Ebene erreicht: `/data/col1/mt1`. Dort erhält er Lesezugriff.

Da der Export jedoch ausgewählt wurde, ist der Submount-Export (Mt1-sub) nicht Teil des PseudoFS für den Client und es wird kein Lese-/Schreibzugriff gewährt.

Best Practice
Wenn Ihr System NFSv3-Export-Submounts verwendet, um dem Client Lese-/Schreibzugriff basierend auf dem Mount-Pfad zu gewähren, müssen Sie dies vor der Verwendung von NFSv4 mit diesen Submount-Exporten berücksichtigen.

Mit NFSv4 hat jeder Kunde ein individuelles PseudoFS.

Export	Pfad	Client	Optionen
Mt1	`/data/col1/mt1`	client1.example.com	ro
MT1-sub	`/data/col1/mt1/subdir`	client2.example.com	rw

NFSv4-Konfiguration

Die Standardkonfiguration für das Data Domain-System aktiviert nur NFSv3. Wenn Sie NFSv4 verwenden möchten, müssen Sie zuerst den NFSv4-Server aktivieren.

Aktivieren des NFSv4-Servers

Vorgehensweise

1. Geben Sie `nfs enable version 4` ein, um NFSv4 zu aktivieren:

```
# nfs enable version 4
NFS server version(s) 3:4 enabled.
```

2. (Optional) Wenn Sie NFSv3 deaktivieren möchten, geben Sie `nfs disable version 3` ein.

```
# nfs disable version 3
NFS server version(s) 3 disabled.
NFS server version(s) 4 enabled.
```

Weitere Erfordernisse

Nachdem der NFSv4-Server aktiviert wurde, müssen Sie ggf. zusätzliche NFS-Konfigurationsaufgaben speziell für Ihren Standort durchführen. Zu diesen Aufgaben können die folgenden Aktionen auf dem Data Domain-System gehören:

- Festlegen der NFSv4-Domain
- Konfigurieren der NFSv4-ID-Zuordnung
- Konfigurieren von ACLs (Zugriffskontrolllisten, Access Control Lists)

Festlegen des Standardservers zum Einschließen von NFSv4

Die Data Domain-NFS-Befehlsoption **`default-server-version`** steuert, welche NFS-Version aktiviert wird, wenn Sie den Befehl `nfs enable` ohne Angabe einer Version eingeben.

Vorgehensweise

1. Geben Sie den Befehl `nfs option set default-server-version 3:4` ein:

```
# nfs option set default-server-version 3:4
NFS option 'default-server-version' set to '3:4'.
```

Aktualisieren bestehender Exporte

Sie können vorhandene Exporte aktualisieren, um die NFS-Version zu ändern, die von Ihrem Data Domain-System verwendet wird.

Vorgehensweise

1. Geben Sie den Befehl `nfs export modify all` ein:

```
# nfs export modify all clients all options
version=Versionsnummer
```

Um sicherzustellen, dass alle Bestandskunden entweder Version 3, 4 oder beide verwenden, können Sie die NFS-Version in die entsprechende Zeichenfolge ändern. Das folgende Beispiel zeigt, dass NFS nun die Versionen 3 und 4 enthält:

```
#nfs export modify all clients all options version=3:4
```

Weitere Informationen zum Befehl `nfs export` finden Sie im *Data Domain Operating System Command Reference Guide*.

Kerberos und NFSv4

NFSv4 und NFSv3 verwenden den Kerberos-Authentifizierungsmechanismus, um Benutzeranmeldedaten zu sichern.

Kerberos verhindert, dass Anmeldedaten in NFS-Paketen gefälscht werden und schützt sie vor Manipulationen auf dem Weg zum Data Domain-System.

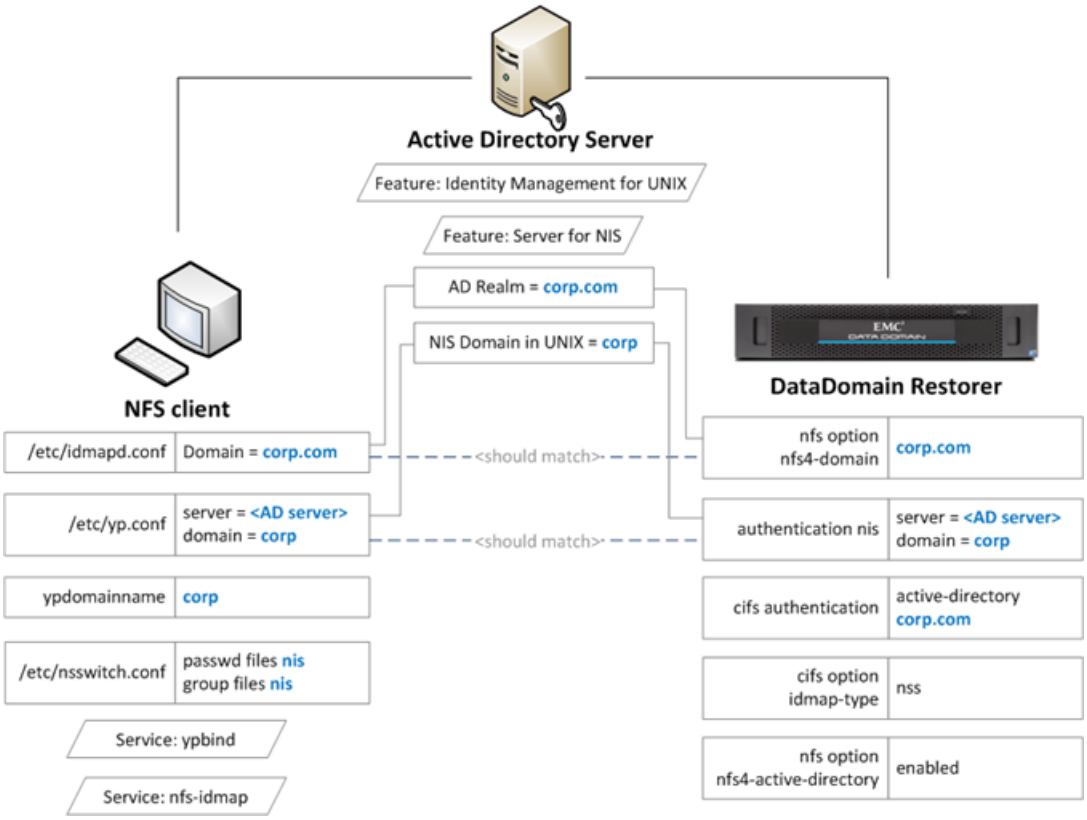
Es gibt verschiedene Arten von Kerberos über NFS:

- Kerberos 5 (`sec krb5 =`)
  Verwenden Sie Kerberos für Benutzeranmeldedaten.
- Kerberos 5 mit Integrität (`SEK = krb5i`)
  Verwenden Sie Kerberos und überprüfen Sie die Integrität der NFS-Nutzlast über eine verschlüsselte Prüfsumme.
- Kerberos 5 mit Sicherheit (`SEK = krb5p`)
  Verwenden Sie Kerberos 5 mit Integrität und verschlüsseln Sie die gesamte NFS-Nutzlast.

Hinweis

`krb5i` und `krb5p` können beide Leistungseinbußen durch Computingoverhead auf dem NFS-Client und dem Data Domain-System verursachen.

Abbildung 8 Active Directory-Konfiguration



Sie verwenden vorhandene NFSv3-Befehle, wenn Sie Ihr System für Kerberos konfigurieren. Im Kapitel zu NFSv3 des *Data Domain Command Reference Guide* finden Sie weitere Informationen.

Konfigurieren von Kerberos mit einem Linux-basierten KDC

Bevor Sie beginnen

Sie sollten sicherstellen, dass alle Systeme auf das Key Distribution Center (KDC) zugreifen können.

Wenn die Systeme das KDC nicht erreichen können, prüfen Sie die Domain Name System(DNS)-Einstellungen.

Die folgenden Schritte ermöglichen Ihnen das Erstellen von keytab-Dateien für den Client und das Data Domain-System:

- In den Schritten 1-3 erstellen Sie die keytab-Datei für das Data Domain-System.
- In den Schritten 4-5 erstellen Sie die keytab-Datei für den Client.

Vorgehensweise

1. Erstellen Sie den Serviceprinzipal **nfs/<ddr_dns_name>@<realm>**.

   ```
   kadmin.local: addprinc -randkey nfs/ddr12345.<domain-
   name>@<domain-name>
   ```

2. Exportieren Sie **nfs/<ddr_dns_name>@<realm>** in eine keytab-Datei.

   ```
   kadmin.local: ktadd -k /tmp/ddr.keytab nfs/
   ddr12345.corp.com@CORP.COM
   ```

3. Kopieren Sie die keytab-Datei auf das Data Domain-System am folgenden Speicherort:

   ```
   /ddr/var/krb5.keytab
   ```

4. Erstellen Sie einen der folgenden Prinzipale für den Client und exportieren Sie diesen Prinzipal in die keytab-Datei:

   ```
   nfs/<client_dns_name>@<REALM>
   root/<client_dns_name>@<REALM>
   ```

5. Kopieren Sie die keytab-Datei auf den Client am folgenden Speicherort:

   ```
   /etc/krb5.keytab
   ```

Hinweis

Es wird empfohlen, dass Sie einen NTP-Server verwenden, damit die Zeit auf allen Entitäten synchron bleibt.

Konfigurieren des Data Domain-Systems für Verwendung mit Kerberos-Authentifizierung

Vorgehensweise

1. Konfigurieren Sie den KDC- und Kerberos-Bereich auf dem Data Domain-System mit dem Befehl `authentication`:

   ```
   # authentication kerberos set realm <Bereich> kdc-type unix
   kdcs <kdc-server>
   ```

2. Importieren Sie die keytab-Datei:

   ```
   # authentication kerberos keytab import
   ```

3. (Optional) Konfigurieren Sie den NIS-Server, indem Sie die folgenden Befehle eingeben:

   ```
   # authentication nis servers add <server>
   # authentication nis domain set <domain-name>
   # authentication nis enable
   # filesys restart
   ```

4. (Optional) Legen Sie für **`nfs4-domain`** den Kerberos-Bereich mit dem Befehl `nfs option` fest:

   ```
   nfs option set nfs4-domain <kerberos-realm>
   ```

5. Fügen Sie einen Client zu einem vorhandenen Export hinzu, indem Sie **`sec=krb5`** zum Befehl `nfs export add` hinzufügen:

   ```
   nfs export add <export-name> clients * options
   version=4,sec=krb5
   ```

Konfigurieren von Clients

Vorgehensweise

1. Konfigurieren Sie den DNS-Server und überprüfen Sie, dass Vorwärts- und Rückwärtssuchen funktionieren.
2. Konfigurieren Sie den KDC- und Kerberos-Bereich durch Bearbeiten der Konfigurationsdatei `/etc/krb5.conf`.

   Sie müssen möglicherweise diesen Schritt basierend auf dem Client-Betriebssystem durchführen, das Sie verwenden.
3. Konfigurieren Sie NIS oder einen anderen externen Namenszuordungsservice.
4. (Optional) Bearbeiten Sie die Datei `/etc/idmapd.conf`, um sicherzustellen, dass sie dem Kerberos-Bereich entspricht.

   Sie müssen möglicherweise diesen Schritt basierend auf dem Client-Betriebssystem durchführen, das Sie verwenden.
5. Überprüfen Sie, ob die keytab-Datei **`/etc/krb5.keytab`** einen Eintrag für den Serviceprinzipal **`nfs/`** oder den Prinzipal **`root/`** enthält.

   ```
   [root@fc22 ~]# klist -k
   Keytab name: FILE:/etc/krb5.keytab
   KVNO Principal
   ----
   ---------------------------------------------------------------
   ```

```
----------
3 nfs/fc22.domain-name@domain-name
```

6. Mounten Sie den Export mit der Option **sec=krb5**.

```
[root@fc22 ~]# mount ddr12345.<domain-name>:/data/col1/
mtree1 /mnt/nfs4 -o sec=krb5,vers=4
```

Aktivieren von Active Directory

Durch Konfigurieren der Active Directory-Authentifizierung wird das Data Domain-System zu einem Teil eines Windows Active Directory-Bereichs. CIFS-Clients und NFS-Clients verwenden die Kerberos-Authentifizierung.

Vorgehensweise

1. Treten Sie einem Active Directory-Bereich mit dem Befehl `cifs set` bei:

```
# cifs set authentication active-directory <Bereich>
```

   Kerberos wird automatisch auf dem Data Domain-System eingerichtet. Das erforderliche NFS/Der erforderliche Serviceprinzipal wird automatisch auf dem KDC erstellt.

2. Konfigurieren Sie NIS mit dem Befehl `authentication nis`:

```
# authentication nis servers add <windows-ad-server>
# authentication nis domain set <ad-realm>
# authentication nis enable
```

3. Konfigurieren Sie CIFS für die Verwendung von NSS für die ID-Zuordnung mit den `cifs`-Befehlen:

```
# cifs disable
# cifs option set idmap-type nss
# cifs enable
# filesys restart
```

4. Legen Sie für **nfs4-domain** den Active Directory-Bereich fest:

```
# nfs option set nfs4-domain <ad-realm>
```

5. Aktivieren Sie Active Directory für die NFSv4-ID-Zuordnung mit dem Befehl `nfs`:

```
# nfs option set nfs4-idmap-active-directory enabled
```

Konfigurieren von Active Directory

Vorgehensweise

1. Installieren Sie die Active Directory Domain Service(AD DS)-Rolle auf dem Windows-Server.
2. Installieren Sie das Identitätsmanagement für UNIX-Komponenten.

```
C:\Windows\system32>Dism.exe /online /enable-feature /
featurename:adminui /all
C:\Windows\system32>Dism.exe /online /enable-feature /
featurename:nis /all
```

3. Überprüfen Sie, ob die NIS-Domäne auf dem Server konfiguriert ist.

```
C:\Windows\system32>nisadmin
The following are the settings on localhost
```

```
Push Interval : 1 days
Logging Mode  : Normal

NIS Domains
NIS Domain in AD  Master server  NIS Domain in UNIX
----------------  -------------  ----------------
corp              win-ad-server  corp
```

4. Weisen Sie AD-Benutzer und -Gruppen UNIX-UID/GIDs für den NFSv4-Server zu.
   a. Gehen Sie zu **Server Manager** > **Tools** > **Active Directory**.
   b. Öffnen Sie über **Properties** die Eigenschaften für einen AD-Benutzer oder eine AD-Gruppe.
   c. Geben Sie auf der Registerkarte „UNIX Atributes“ Werte in die Felder „NIS domain“, „UID“ und „Primary GID“ ein.

Konfigurieren von Clients in Active Directory

Vorgehensweise

1. Erstellen Sie einen neuen AD-Benutzer auf dem AD-Server, um den Serviceprinzipal des NFS-Clients darzustellen.
2. Erstellen Sie das NFS/den Serviceprinzipal für den NFS-Client.

```
> ktpass -princ nfs/<client_dns_name>@<REALM> -mapuser nfsuser -
pass **** -out nfsclient.keytab
/crytp rc4-hmac-nt /ptype KRB5_NT_PRINCIPAL
```

3. (Optional) Kopieren Sie die keytab-Datei in `/etc/krb5.keytab` auf dem Client.

   Ob dieser Schritt ausgeführt werden muss, hängt davon ab, welches Client-Betriebssystem Sie verwenden.

LDAP und NFSv4

Die Aktivierung von LDAP ermöglicht die Verwendung eines vorhandenen OpenLDAP-Servers oder die Bereitstellung mit DDR für NFSv4-ID-Zuordnung, NFSv3 Kerberos mit LDAP oder NFSv4 Kerberos mit LDAP.

LDAP-Server konfigurieren

Sie können einen oder mehrere LDAP-Server gleichzeitig konfigurieren.

Hinweis

LDAP muss deaktiviert sein, wenn Sie Änderungen an der Konfiguration vornehmen.

Geben Sie den LDAP-Server in einem der folgenden Formate an:

- IPv4-Adresse: `10.26.16.250`
- IPv4-Adresse mit Portnummer: `10.26.16.251:400`
- IPv6-Adresse: `[::ffff:9.53.96.21]`
- IPv6-Adresse mit Portnummer: `[::ffff:9.53.96.21]:400`
- Hostname: `myldapserver`

- Hostname mit Portnummer: **myldapserver:400**

Wenn Sie mehrere Server konfigurieren:

- Trennen Sie jeden Server durch ein Leerzeichen.
- Der erste aufgeführte Server bei Verwendung des `authentication ldap servers add`-Befehls wird der primäre Server.
- Wenn einer der Server nicht konfiguriert werden kann, schlägt der Befehl für alle aufgeführten Server fehl.

Vorgehensweise

1. Fügen Sie einen oder mehrere LDAP-Server mithilfe des Befehls `authentication ldap servers add` hinzu:

```
# authentication ldap servers add 10.26.16.250 10.26.16.251:400
LDAP server(s) added
LDAP Server(s):        2
#     IP Address/Hostname
---   --------------------
1.    10.26.16.250 (primary)
2.    10.26.16.251:400
---   --------------------
```

2. Entfernen Sie einen oder mehrere LDAP-Server mithilfe des Befehls `authentication ldap servers del`:

```
# authentication ldap servers del 10.26.16.251:400
LDAP server(s) deleted.
LDAP Servers: 1
#   Server
-   ------------   ---------
1   10.26.16.250   (primary)
-   ------------   ---------
```

3. Entfernen Sie alle LDAP-Server mithilfe des Befehls `authentication ldap servers reset`:

```
# authentication ldap servers reset
LDAP server list reset to empty.
```

Konfigurieren des LDAP-Basissuffix

Das Basissuffix ist der Basis-DN für die Suche. Hier beginnt das LDAP-Verzeichnis zu suchen.

Vorgehensweise

1. Festlegen des LDAP-Basissuffix mithilfe des Befehls `authentication ldap base set`:

```
# authentication ldap base set "dc=anvil,dc=team"
LDAP base-suffix set to "dc=anvil,dc=team".
```

2. Setzen Sie das LDAP-Basissuffix mithilfe des Befehls `authentication ldap base reset` zurück:

```
# authentication ldap base reset
LDAP base-suffix reset to empty.
```

Konfigurieren der LDAP-Clientauthentifizierung

Konfigurieren Sie das Konto (Bind DN) und Passwort (Bind PW) für die Authentifizierung beim LDAP-Server und für Abfragen.

Sie sollten immer Bind DN und Passwort konfigurieren. LDAP-Server erfordern in der Regel standardmäßig einen authentifizierten Bind. Wenn `client-auth` nicht festgelegt ist, wird anonymer Zugriff angefordert (ohne Name oder Passwort). Die Ausgabe von `authentication ldap show` ist wie folgt:

```
# authentication ldap show
LDAP configuration
        Enabled:          yes (*)
        Base-suffix:      dc=u2,dc=team
        Binddn:           (anonymous)
        Server(s):        1
#   Server
-   -------------   ---------
1   10.207.86.160   (primary)
-   -------------   ---------

Secure LDAP configuration
        SSL Enabled:      no
        SSL Method:       off
        tls_reqcert:      demand

(*) Requires a filesystem restart for the configuration to take
effect.
```

Wenn binddn mit der `client-auth`-CLI festgelegt, aber bindpw nicht bereitgestellt wird, wird nicht authentifizierter Zugriff angefordert.

```
# authentication ldap client-auth set binddn
"cn=Manager,dc=u2,dc=team"
Enter bindpw:
** Bindpw is not provided. Unauthenticated access would be requested.
LDAP client authentication binddn set to "cn=Manager,dc=u2,dc=team".
```

Vorgehensweise

1. Legen Sie Bind DN und Passwort mithilfe des Befehls `authentication ldap client-auth set binddn` fest:

   ```
   # authentication ldap client-auth set binddn
   "cn=Administrator,cn=Users,dc=anvil,dc=team"
       Enter bindpw:
       LDAP client authentication binddn set to
   "cn=Administrator,cn=Users,dc=anvil,dc=team".
   ```

2. Setzen Sie Bind DN und Passwort mithilfe des Befehls `authentication ldap client-auth reset` zurück:

   ```
   # authentication ldap client-auth reset
   LDAP client authentication configuration reset to empty.
   ```

Aktivieren von LDAP

Bevor Sie beginnen

Eine LDAP-Konfiguration muss vor der Aktivierung von LDAP vorhanden sein. Darüber hinaus müssen Sie NIS deaktivieren, sicherstellen, dass der LDAP-Server erreichbar ist und in der Lage sein, die Stamm-DSE des LDAP-Servers abzufragen.

Vorgehensweise

1. Aktivieren Sie LDAP mithilfe des Befehls `authentication ldap enable`:

   ```
   # authentication ldap enable
   ```

   Die Details der LDAP-Konfiguration werden zum Bestätigen angezeigt, bevor Sie fortfahren. Um fortzufahren, geben Sie **yes** ein und starten Sie das Dateisystem für die LDAP-Konfiguration neu, damit es wirksam wird.

2. Zeigen Sie die aktuelle LDAP-Konfiguration an, indem Sie den Befehl `authentication ldap show` verwenden:

   ```
   # authentication ldap show
   LDAP configuration
           Enabled:          no
           Base-suffix:      dc=anvil,dc=team
           Binddn:
   cn=Administrator,cn=Users,dc=anvil,dc=team
           Server(s):        2
   #   Server
   -   ----------------   ---------
   1   10.26.16.250       (primary)
   2   10.26.16.251:400
   -   ----------------   ---------

   Secure LDAP configuration
           SSL Enabled:      no
           SSL Method:       off
           tls_reqcert:      demand
   ```

   Konfigurationsdetails zu Basis-LDAP und sicherem LDAP werden angezeigt.

3. Zeigen Sie den aktuellen LDAP-Status mithilfe des Befehls `authentication ldap status` an:

   ```
   # authentication ldap status
   ```

   Der LDAP-Status wird angezeigt. Wenn der LDAP-Status nicht `good` ist, wird das Problem in der Ausgabe identifiziert. Beispiel:

   ```
   # authentication ldap status
   Status: invalid credentials
   ```

   oder

   ```
   # authentication ldap status
   Status: invalid DN syntax
   ```

4. Deaktivieren Sie LDAP mithilfe des Befehls `authentication ldap disable`:

   ```
   # authentication ldap disable
   LDAP is disabled.
   ```

Aktivieren von sicherem LDAP

Sie können DDR konfigurieren, um sicheres LDAP zu verwenden (durch Aktivieren von SSL).

Bevor Sie beginnen

Wenn es kein LDAP-CA-Zertifikat gibt und `tls_reqcert` auf `demand` festgelegt wird, schlägt der Vorgang fehl. Importieren Sie ein LDAP-CA-Zertifikat und versuchen Sie es erneut.

Wenn `tls_reqcert` auf `never` festgelegt ist, ist kein LDAP-CA-Zertifikat erforderlich. Weitere Informationen finden Sie unter Konfigurieren der LDAP-Server-Zertifikatsüberprüfung mit importierten CA-Zertifikaten auf Seite 298.

Vorgehensweise

1. Aktivieren Sie SSL mithilfe des Befehls `authentication ldap ssl enable`:

   ```
   # authentication ldap ssl enable
   Secure LDAP is enabled with 'ldaps' method.
   ```

   Die Standardmethode ist sicheres LDAP oder *ldaps*. Sie können andere Methoden angeben, z. B. TLS:

   ```
   # authentication ldap ssl enable method start_tls
   Secure LDAP is enabled with 'start_tls' method.
   ```

2. Deaktivieren Sie SSL mithilfe des Befehls `authentication ldap ssl disable`:

   ```
   # authentication ldap ssl disable
   Secure LDAP is disabled.
   ```

Konfigurieren der LDAP-Server-Zertifikatsüberprüfung mit importierten CA-Zertifikaten

Sie können das Zertifikatverhalten für die TLS-Anfrage ändern.

Vorgehensweise

1. Ändern Sie das Zertifikatverhalten für die TLS-Anfrage mithilfe des Befehls `authentication ldap ssl set tls_reqcert`.

   Überprüfen Sie das Zertifikat nicht:

   ```
   # authentication ldap ssl set tls_reqcert never
   "tls_reqcert" set to "never". LDAP server certificate will not
   be verified.
   ```

   Überprüfen Sie das Zertifikat:

   ```
   # authentication ldap ssl set tls_reqcert demand
   "tls_reqcert" set to "demand". LDAP server certificate will be
   verified.
   ```

2. Setzen Sie das Zertifikatverhalten für die TLS-Anfrage mithilfe des Befehls `authentication ldap ssl reset tls_reqcert` zurück. Das Standardverhalten ist `demand`:

   ```
   # authentication ldap ssl reset tls_reqcert
   tls_reqcert has been set to "demand". LDAP Server certificate
   will be verified with imported CA certificate.Use "adminaccess"
   CLI to import the CA certificate.
   ```

Managen von CA-Zertifikaten für LDAP

Sie können Zertifikate importieren oder löschen und aktuelle Zertifikatinformationen anzeigen.

Vorgehensweise

1. Importieren Sie ein CA-Zertifikat für die LDAP-Server-Zertifikatsüberprüfung mithilfe des Befehls `adminaccess certificate import`.

   Geben Sie `ldap` für `ca application` an:

```
# adminaccess certificate import{host application {all | aws-
federal | ddboost | https| keysecure | rkm | <application-
list>}| ca application { ldap }} [file <file-name>] Import host
or ca certificate
```

2. Löschen Sie ein CA-Zertifikat für die Zertifikatsüberprüfung für LDAP-Server mithilfe des Befehls `adminaccess certificate delete`.

   Geben Sie `ldap` für `application` an:

   ```
   # adminaccess certificate delete
   { subject <subject-name> | fingerprint <fingerprint>}
   [application { ldap }]
   ```

   Geben Sie `ldap` für `imported-ca application` an:

   ```
   # adminaccess certificate delete
   { imported-host application { all | aws-federal | ddboost |
   https
   | keysecure | rkm | <application-list>}
   | imported-ca application { ldap }}
   ```

3. Zeigen Sie aktuelle Informationen für CA-Zertifikate für die LDAP-Server-Zertifikatsüberprüfung mithilfe des Befehls `adminaccess certificate show` an:

   ```
   # adminaccess certificate show imported-ca ldap
   ```

KAPITEL 11

Speichermigration

Inhalt dieses Kapitels:

Speichermigration im Überblick

Die Speichermigration unterstützt den Austausch der vorhandenen Speichergehäuse durch neue Gehäuse, die höhere Performance, höhere Kapazität und geringeren Platzbedarf bieten können.

Nach der Installation neuer Gehäuse können Sie die Daten aus älteren Gehäusen zu neuen Gehäusen migrieren, während das System weiterhin andere Prozesse unterstützt, wie Zugriff auf Daten, Erweiterung, Bereinigung und Replikation. Die Speichermigration erfordert Systemressourcen, aber Sie können dies mit Drosselungseinstellungen steuern, mit denen der Migration eine relativ höhere oder niedrigere Priorität gegeben wird. Sie können eine Migration auch anhalten, um mehr Ressourcen für andere Prozesse zur Verfügung zu stellen, und dann die Migration wieder aufnehmen, wenn der Ressourcenbedarf geringer ist.

Während der Migration verwendet das System Daten auf den Quell- und Zielgehäusen. Neue Daten werden auf neue Gehäuse geschrieben. Nicht migrierte Daten werden auf den Quellgehäusen und Migrationsdaten werden auf den Zielgehäusen aktualisiert. Wenn die Migration unterbrochen wird, kann die Migration Blöcke im Migrationsprozess wieder aufnehmen, die nicht als migriert gekennzeichnet wurden.

Während der Migration wird jeder Block von Daten kopiert und überprüft, der Quellblock freigegeben und als migriert markiert und der Systemindex aktualisiert, um den neuen Standort zu verwenden. Neue Daten, die für den Quellblock gedacht waren, werden jetzt auf den Zielblock umgeleitet. Alle neuen Datenblockzuweisungen, die von der Quelle zugewiesen wurden, werden vom Ziel zugewiesen.

Der Migrationskopierprozess erfolgt auf Einschubebene, nicht auf logischer Datenebene, sodass auf alle Festplattensektoren im Quelleinschub Zugriff erfolgt und Kopien erstellt werden, unabhängig davon, ob Daten vorhanden sind. Aus diesem Grund kann das Storage Migration Utility nicht verwendet werden, um einen logischen Daten-Footprint zu reduzieren.

Hinweis

Da die Datenmenge während der Migration zwischen den Quell- und Zielgehäusen aufgeteilt wird, können Sie eine Migration nicht anhalten und nur die Quellgehäuse wieder aufnehmen. Nach dem Starten muss die Migration abgeschlossen werden. Wenn ein Fehler auftritt, z. B. ein fehlerhaftes Festplattenlaufwerk, und die Migration unterbrochen wird, beheben Sie das Problem und nehmen Sie die Migration wieder auf.

Abhängig von der Menge der zu migrierenden Daten und der ausgewählten Drosselungseinstellungen kann eine Speichermigration mehrere Tage oder Wochen dauern. Wenn alle Daten migriert wurden, startet der Finalisierungsprozess, der manuell mit dem Befehl `storage migration finalize` initiiert werden muss, das Dateisystem neu. Während des Neustarts werden die Quellgehäuse aus der Systemkonfiguration entfernt und die Zielgehäuse werden Teil des Dateisystems. Wenn der Finalisierungsprozess abgeschlossen ist, können die Quellgehäuse aus dem System entfernt werden.

Nach einer Speichermigration werden die Nummern der Festplatteneinschübe, die von DD OS gemeldet werden, möglicherweise nicht sequenziell angezeigt. Dies geschieht, da die Einschubnummerierung an die Seriennummer jedes einzelnen Festplatteneinschubs gekoppelt ist. KB-Artikel 499019, *Data Domain: Storage enclosure numbering is not sequential*, verfügbar auf https://support.emc.com, bietet weitere Details. In DD OS-Version 5.7.3.0 und höher erfordert der im Wissensdatenbankartikel

beschriebene Befehl `enclosure show persistent-id` Administratorzugriff und keinen SE-Zugriff.

Überlegungen zur Migrationsplanung

Beachten Sie die folgenden Richtlinien vor dem Starten einer Speichermigration.

- Die Speichermigration erfordert eine Single-Use-Lizenz und basiert auf Systemmodellen, die von DD OS-Version 5.7 oder höher unterstützt werden.

  Hinweis

  Für mehrere Speichermigrationsvorgänge sind mehrere Lizenzen erforderlich. Mehrere Quellgehäuse können jedoch während eines einzigen Vorgangs zu mehreren Zielgehäusen migriert werden.

- Die Speichermigration basiert auf Kapazität, nicht der Gehäuseanzahl. Es gilt:
  - Ein Quellgehäuse kann zu einem Zielgehäuse migriert werden.
  - Ein Quellgehäuse kann zu mehreren Zielgehäusen migriert werden.
  - Mehrere Quellgehäuse können zu einem Zielgehäuse migriert werden.
  - Mehrere Quellgehäuse können zu mehreren Zielgehäusen migriert werden.
- Die Zielgehäuse müssen:
  - neu, nicht zugewiesen und nicht lizenziert sein.
  - auf dem DD-Systemmodell unterstützt werden.
  - mindestens so viel nutzbare Kapazität wie die Gehäuse aufweisen, die sie ersetzen.

    Hinweis

    Es ist nicht möglich, die Auslastung der Quelleinschübe zu bestimmen. Das Data Domain-System führt alle Berechnungen auf Basis der Kapazität des Einschubs aus.
- Das DD-Systemmodell muss über ausreichend Arbeitsspeicher verfügen, um die Speicherkapazität der neuen Gehäuse des aktiven Tier zu unterstützen.
- Datenmigration wird für Festplatten im System-Controller nicht unterstützt.
- **⚠ ACHTUNG**

  Aktualisieren Sie DD OS nicht, bis die laufende Speichermigration abgeschlossen ist.
- Die Speichermigration kann nicht gestartet werden, wenn das Dateisystem deaktiviert ist oder während ein DD OS-Upgrade, ein anderer Migrationsprozess oder eine RAID-Rekonstruktion ausgeführt wird.

  Hinweis

  Wenn eine Speichermigration ausgeführt wird, ist eine neue Speichermigrationslizenz erforderlich, um einen neuen Speichermigrationsvorgang nach Abschluss der laufenden Migration zu starten. Als Teil der Vorabprüfung des Upgrades wird berichtet, ob eine Speichermigrationslizenz vorhanden oder nicht vorhanden ist.

- Alle angegebenen Quellgehäuse müssen sich in derselben Tier befinden (aktive oder Archiv).
- Es kann nur eine Gruppe von Festplatten in jedem Quellgehäuse geben und alle Festplatten in der Festplattengruppe müssen im selben Gehäuse eingebaut werden.
- Alle Festplatten in jedem Zielgehäuse müssen denselben Typ aufweisen (z. B. alle SATA oder alle SAS).
- Nach dem Start der Migration können die Zielgehäuse nicht entfernt werden.
- Quellgehäuse können erst entfernt werden, wenn die Migration abgeschlossen und finalisiert ist.
- Die Speichermigrationsdauer hängt von den Systemressourcen (unterschiedlich für verschiedene Systemmodelle), der Verfügbarkeit von Systemressourcen und der zu migrierenden Datenmenge ab. Die Speichermigration kann Tage oder Wochen dauern.

Überlegungen zu DS60-Einschüben

Der kompakte DS60-Einschub bietet ausreichend Platz für 60 Festplatten, damit der Kunde das gesamte Potenzial des Racks ausschöpfen kann. Die Laufwerke sind oben am Gehäuse durch das Ausziehen des Einschubs aus dem Schrank zugänglich. Lesen Sie aufgrund des Gewichts der Einschübe von etwa 102 kg bei vollständiger Beladung diesen Abschnitt vor dem Fortfahren mit einer Speichermigration auf DS60-Einschübe.

Beachten Sie die folgenden Hinweise bei der Arbeit mit dem DS60-Einschub:

⚠ ACHTUNG

- **Beim Laden der Einschübe oben am Rack besteht Kippgefahr.**
- **Überprüfen Sie, ob der Boden das Gesamtgewicht der DS60-Einschübe trägt.**
- **Überprüfen Sie, ob die Racks eine ausreichende Stromversorgung der DS60-Einschübe gewährleisten.**
- **Wenn Sie mehr als fünf DS60s im ersten Rack oder mehr als sechs DS60s im zweiten Rack hinzufügen, sind Stabilisatoren und eine Leiter zur Wartung der DS60-Einschübe erforderlich.**

Anzeigen des Migrationsstatus

DD System Manager bietet zwei Möglichkeiten zum Anzeigen des Speichermigrationsstatus.

Vorgehensweise

1. Wählen Sie **Hardware** > **Storage** aus.

   Überprüfen Sie im Bereich "Storage" die Zeile "Storage Migration Status". Wenn der Status "Not Licensed" ist, müssen Sie eine Lizenz hinzufügen, bevor Sie Speichermigrationsfunktionen verwenden können. Wenn die Speichermigrationslizenz installiert ist, kann der Status einer der folgenden sein: None, Starting, Migrating, Paused by User, Paused by System, Copy Completed - Pending Finalization, Finalizing, Failed during Copy oder Failed during Finalize.

2. Wenn eine Speichermigration ausgeführt wird, klicken Sie auf **View Storage Migration**, um die Fortschrittsdialogfelder anzuzeigen.

   Hinweis

   Der Status der Migration zeigt den Prozentsatz der übertragenen Blöcke. In einem System mit vielen freien Blöcken werden die freien Blöcke nicht migriert, sie sind jedoch in der Fortschrittsanzeige enthalten. In diesem Szenario ist der Fortschritt schnell und dann langsam, wenn die Datenmigration gestartet wird.

3. Wenn eine Speichermigration ausgeführt wird, können Sie auch den Status durch Auswahl von **Health** > **Jobs** anzeigen.

Evaluieren der Migrationsbereitschaft

Sie können mit dem System die Speichermigrationsbereitschaft evaluieren, ohne die Migration zu starten.

Vorgehensweise

1. Installieren Sie die Zielgehäuse mithilfe der Anweisungen in den Produktinstallationshandbüchern.
2. Wählen Sie **Administration** > **Licenses** und prüfen Sie, ob die Speichermigrationslizenz installiert ist.
3. Wenn die Speichermigrationslizenz nicht installiert ist, klicken Sie auf**Add Licenses** und fügen Sie die Lizenz hinzu.
4. Wählen Sie **Hardware** > **Storage** und klicken Sie dann auf **Migrate Data**.
5. Wählen Sie im Dialogfeld "Select a Task" die Option **Estimate** und klicken Sie dann auf **Next**.
6. Verwenden Sie im Dialogfeld "Select Existing Enclosures" die Kontrollkästchen, um jedes der Quellgehäuse für die Speichermigration auszuwählen, und klicken Sie dann auf **Next**.
7. Verwenden Sie im Dialogfeld "Select New Enclosures" die Kontrollkästchen, um jedes der Zielgehäuse für die Speichermigration auszuwählen, und klicken Sie dann auf **Next**.

   Die Schaltfläche "Add Licenses" ermöglicht es Ihnen, bei Bedarf ohne Unterbrechung der aktuellen Aufgabe Speicherlizenzen für die neuen Gehäuse hinzufügen.

8. Überprüfen Sie im Dialogfeld "Review Migration Plan" die voraussichtliche Migrationsplanung und klicken Sie dann auf **Next**.
9. Überprüfen Sie die Ergebnisse der Vorabprüfung im Dialogfeld "Verify Migration Preconditions" und klicken Sie dann auf "Close".

Ergebnisse

Wenn eine der Vorabprüfungen fehlschlägt, beheben Sie das Problem vor der Migration.

Migrieren von Speicher mithilfe von DD System Manager

Der Speichermigrationsprozess evaluiert die Systembereitschaft, fodert Sie auf, zu bestätigen, dass Sie die Migration starten möchten, migriert die Daten und fordert Sie dann auf, den Prozess zu finalisieren.

Vorgehensweise

1. Installieren Sie die Zielgehäuse mithilfe der Anweisungen in den Produktinstallationshandbüchern.
2. Wählen Sie **Administration** > **Licenses** und überprüfen Sie, ob die Speichermigrationslizenz installiert ist.
3. Wenn die Speichermigrationslizenz nicht installiert ist, klicken Sie auf **Add Licenses** und fügen Sie die Lizenz hinzu.
4. Wählen Sie **Hardware** > **Storage** und dann **Migrate Data**.
5. Wählen Sie im Dialogfeld "Select a Task" die Option **Migrate** und dann **Next**.
6. Verwenden Sie im Dialogfeld "Select Existing Enclosures" die Kontrollkästchen, um jedes der Quellgehäuse für die Speichermigration auszuwählen, und klicken Sie dann auf **Next**.
7. Verwenden Sie im Dialogfeld "Select New Enclosures" die Kontrollkästchen, um jedes der Zielgehäuse für die Speichermigration auszuwählen, und klicken Sie dann auf **Next**.

   Die Schaltfläche "Add Licenses" ermöglicht es Ihnen, Speicherlizenzen für die neuen Gehäuse nach Bedarf hinzuzufügen, ohne die aktuelle Aufgabe zu unterbrechen.
8. Prüfen Sie im Dialogfeld "Review Migration Plan" die voraussichtliche Migrationsplanung und klicken Sie dann auf **Start**.
9. Klicken Sie im Dialogfeld "Start Migration" auf **Start**.

   Das Dialogfeld "Migrate" wird angezeigt und während der drei Migrationsphasen aktualisiert: Starting Migration, Migration in Progress und Copy Complete.
10. Wenn "Copy Complete" der Titel des Dialogfelds "Migrate" ist und ein Neustart des Dateisystems möglich ist, klicken Sie auf **Finalize**.

    Hinweis

    Diese Aufgabe startet das Dateisystem neu und dauert in der Regel 10 bis 15 Minuten. Das System ist währenddessen nicht verfügbar.

Ergebnisse

Wenn die Migration abgeschlossen wurde, verwendet das System die Zielgehäuse und die Quellgehäuse können entfernt werden.

Beschreibungen zur Speichermigration in Dialogfeldern

Die Beschreibungen im DD System Manager-Dialogfeld bieten zusätzliche Informationen zur Speichermigration. Diese Informationen sind auch durch Klicken auf das Hilfesymbol in den Dialogfeldern verfügbar.

Dialogfeld "Select a Task"

Die Konfiguration in diesem Dialogfeld bestimmt, ob das System die Bereitschaft für die Speichermigration evaluiert und stoppt oder die Bereitschaft evaluiert und mit der Speichermigration beginnt.

Wählen Sie **Estimate**, um die Systembereitschaft zu evaluieren und zu stoppen.

Wählen Sie **Migrate**, um die Migration nach der Systemevaluierung zu starten. Zwischen der Systemevaluierung und dem Start der Migration fordert ein Dialogfeld Sie auf, die Speichermigration zu bestätigen oder abzubrechen.

Dialogfeld "Select Existing Enclosures"

Die Konfiguration in diesem Dialogfeld wählt entweder die aktive Ebene oder die Aufbewahrungsebene und die Quellgehäuse für die Migration.

Wenn die DD Extended Retention-Funktion installiert ist, verwenden Sie das Listenfeld, um **Active Tier** oder **Retention Tier** auszuwählen. Das Listenfeld wird nicht angezeigt, wenn DD Extended Retention nicht installiert ist.

Die Liste "Existing Enclosures" zeigt die Gehäuse, die für die Speichermigration geeignet sind. Aktivieren Sie das Kontrollkästchen für jedes zu migrierende Gehäuse. Klicken Sie auf **Next**, sobald Sie fortfahren möchten.

Dialogfeld "Select New Enclosures"

Die Konfiguration in diesem Dialogfeld wählt die Zielgehäuse für die Migration aus. In diesem Dialogfeld werden auch der Speicherlizenzstatus und die Schaltfläche **Add Licenses** angezeigt.

Die Liste der verfügbaren Gehäuse zeigt die Gehäuse, die qualifizierte Ziele für die Speichermigration sind. Aktivieren Sie das Kontrollkästchen für jedes der gewünschten Zielgehäuse.

Die Lizenz-Statusleiste repräsentiert alle Speicherlizenzen, die auf dem System installiert sind. Der grüne Bereich repräsentiert Lizenzen, die verwendet werden. Der transparente Bereich repräsentiert die lizenzierte verfügbare Speicherkapazität für Zielgehäuse. Wenn Sie weitere Lizenzen zur Unterstützung der ausgewählten Zielcontroller installieren müssen, klicken Sie auf **Add Licenses**.

Klicken Sie auf **Next**, sobald Sie fortfahren möchten.

Dialogfeld „Review Migration Plan“

Dieses Dialogfeld bietet eine Schätzung der Speichermigrationsdauer, organisiert nach den drei Phasen der Speichermigration.

Phase 1 der Speichermigration führt eine Reihe von Tests aus, um zu überprüfen, ob das System für die Migration bereit ist. Die Testergebnisse werden im Dialogfeld „Verify Migration Preconditions“ angezeigt.

Während Phase 2 werden die Daten von den Quellgehäusen zu den Zielgehäusen kopiert. Wenn eine große Menge an Daten vorhanden ist, kann das Kopieren Tage oder Wochen in Anspruch nehmen, da der Vorgang im Hintergrund ausgeführt wird, während das System weiterhin Backupclients bedient. Eine Einstellung im Dialogfeld „Migration in Progress“ ermöglicht Ihnen das Ändern der Migrationspriorität, wodurch die Migration beschleunigt oder verlangsamt werden kann.

Phase 3, die manuell aus dem Dialogfeld „Copy Complete“ initiiert wird, aktualisiert die Systemkonfiguration, um die Zielgehäuse zu verwenden, und entfernt die Konfiguration für die Quellcontroller. In dieser Phase wird das Dateisystem neu gestartet und das System steht für Backupclients nicht zur Verfügung.

Dialogfeld "Verify Migration Preconditions"

In diesem Dialogfeld werden die Ergebnisse der Tests angezeigt, die Sie vor Beginn der Migration ausführen.

Die folgende Liste zeigt die Abfolge der Tests und bietet weitere Informationen zu jedem der Tests.

P1. Diese Systemplattform wird unterstützt.

Ältere DD-Systemmodelle unterstützen die Speichermigration nicht.

P2. Es ist eine Speichermigrationslizenz verfügbar.

Es ist eine Speichermigrationslizenz erforderlich.

P3. Es wird derzeit keine andere Migration ausgeführt.

Eine vorherige Speichermigration muss abgeschlossen werden, bevor Sie eine andere starten können.

P4. Die aktuelle Anforderung für die Migration ist identisch mit der unterbrochenen Migrationsanforderung.

Setzen Sie die unterbrochene Migration fort und schließen Sie sie ab.

P5. Prüfen Sie das Layout der Festplattengruppe für die vorhandenen Gehäuse.

Die Speichermigration erfordert, dass jedes Quellgehäuse nur eine Gruppe von Festplatten umfasst, und alle Festplatten in der Gruppe müssen sich in diesem Gehäuse befinden.

P6. Überprüfen Sie die endgültige Kapazität des Systems.

Die Kapazität des gesamten Systems nach der Migration und das Entfernen der Quellgehäuse dürfen die Kapazität, die das DD-Systemmodell unterstützt, nicht überschreiten.

P7. Überprüfen Sie die Kapazität der Ersatzgehäuse.

Die nutzbare Kapazität der Zielgehäuse muss größer als die der Quellgehäuse sein.

P8. Quellgehäuse befinden sich in der gleichen aktiven Tier oder Aufbewahrungseinheit.

Das System unterstützt die Speichermigration von der aktiven Tier oder der Aufbewahrungs-Tier. Die Migration von Daten über beide Tiers zur gleichen Zeit wird nicht unterstützt.

P9. Quellgehäuse sind nicht Teil der Haupteinheit.

Obwohl der Systemcontroller als ein Gehäuse in der CLI angegeben ist, unterstützt die Speichermigration keine Migration von Festplatten, die im Systemcontroller installiert sind.

P10. Ersatzgehäuse können zum Speicher hinzugefügt werden.

Alle Festplatten in jedem Zielgehäuse müssen denselben Typ aufweisen (z. B. alle SATA oder alle SAS).

P11. In den Quellcontrollern wird keine RAID-Rekonstruktion durchgeführt.

Die Speichermigration kann nicht gestartet werden, während eine RAID-Rekonstruktion ausgeführt wird.

P12. Quelleinschub gehört zu einem unterstützten Tier.

Das Quellfestplattengehäuse muss Teil eines auf dem Migrationsziel unterstützten Tier sein.

Dialogfelder zum Migrationsfortschritt

Diese Serie von Dialogfeldern zeigt den Speichermigrationsstatus und die Steuerelemente, die in jeder Phase gelten.

Migrate - Starting Migration
Während der ersten Phase wird der Fortschritt in der Statusleiste angezeigt. Es stehen keine Steuerlemente zur Verfügung.

Migrate - Migration in Progress
In der zweiten Phase werden Daten aus den Quellgehäusen in die Zielgehäuse kopiert und der Fortschritt wird in der Statusleiste angezeigt. Da die Datenkopie Tage oder Wochen dauern kann, werden Steuerelemente bereitgestellt, sodass Sie die während der Migration verwendeten Ressourcen managen und die Migration unterbrechen können, wenn Ressourcen für andere Prozesse erforderlich sind.

Klicken Sie auf **Pause**, um die Migration anzuhalten, und später auf **Resume**, um mit der Migration fortzufahren.

Die Schaltflächen **Low**, **Medium** und **High** definieren Drosselungseinstellungen für Anforderungen im Hinblick auf Speichermigrationsressourcen. Eine niedrige Drosselungseinstellung gibt der Speichermigration eine niedrigere Ressourcenpriorität, was zu einer langsameren Migration führt und weniger Systemressourcen erfordert. Im Gegenzug gibt eine hohe Drosselungseinstellung der Speichermigration eine höhere Ressourcenpriorität, was zu einer schnelleren Migration führt und mehr Systemressourcen erfordert. Die mittlere Einstellung wählt eine mittlere Priorität.

Sie müssen dieses Dialogfeld während der Migration nicht geöffnet lassen. Um den Status der Migration nach dem Schließen dieses Dialogfelds zu prüfen, wählen Sie**Hardware** > **Storage**und zeigen Sie den Migrationsstatus an. Um von der Seite „Hardware/Storage“ zu diesem Dialogfeld zurückzukehren, klicken Sie auf **Manage Migration**. Der Migrationsfortschritt kann auch durch Auswahl von **Health** > **Jobs** angezeigt werden.

Migrate - Copy Complete
Wenn die Kopie abgeschlossen ist, wartet der Migrationsprozess darauf, dass Sie auf **Finalize** klicken. In dieser letzten Phase, die 10 bis 15 Minuten dauert, wird das Dateisystem neu gestartet und das System ist nicht verfügbar. Es wird empfohlen, diese Phase während eines Wartungsfensters oder einem Zeitraum mit geringer Systemaktivität zu starten.

Migrieren von Speicher mithilfe der CLI

Bei einer Migration werden einfach alle zugewiesenen Blöcke aus den Blocksätzen, die über Quell-DGs (wie Quellblocksätze) formatiert sind, auf die Blocksätze verschoben,

die über Ziel-DGs formatiert sind (wie Zielblocksätze). Sobald alle zugewiesenen Blöcke aus den Quellblocksätzen verschoben wurden, können diese Blocksätze aus dem Dateisystem, ihre Festplatten aus ihrem Speicher-Tier und die physischen Festplatten und Gehäuse aus dem DDR entfernt werden.

Hinweis

Die Vorbereitung der neuen Gehäuse für die Speichermigration wird vom Speichermigrationsprozess verwaltet. Bereiten Sie Zielgehäuse nicht wie beim Hinzufügen von Gehäusen vor. Beispielsweise ist die Verwendung des Befehls `filesys expand` für das Hinzufügen eines Gehäuses angemessen, aber dieser Befehl verhindert, dass Gehäuse als Speichermigrationsziele verwendet werden.

Ein DS60-Festplatteneinschub enthält vier Spindeln mit jeweils 15 Festplatten. Wenn ein DS60-Einschub Migrationsziel oder -quelle ist, werden die Spindeln als ***enclosure*:*pack*** referenziert. In diesem Beispiel ist die Quelle Gehäuse 7, Spindel 2 (7:2) und das Ziel ist Gehäuse 7, Spindel 4 (7:4).

Vorgehensweise

1. Installieren Sie die Zielgehäuse mithilfe der Anweisungen in den Produktinstallationshandbüchern.
2. Prüfen Sie, ob die Speichermigrationslizenz installiert ist.

   ```
   # elicense show
   ```
3. Wenn die Lizenz nicht installiert ist, aktualisieren Sie die elektronische Lizenz, um die Speichermigrationslizenz hinzuzufügen.

   ```
   # elicense update
   ```
4. Zeigen Sie den Festplattenstatus für die Quell- und Zielfestplatten an.

   ```
   # disk show state
   ```

   Die Quellfestplatten sollten sich im Status "Active" befinden und die Zielfestplatten im Status "Unknown".
5. Führen Sie den Befehl "storage migration precheck" aus, um zu ermitteln, ob das System bereit für die Migration ist.

   ```
   # storage migration precheck source-enclosures 7:2 destination-
   enclosures 7:4
   ```
6. Zeigen Sie die Migrationsdrosselungseinstellung an.

   ```
   storage migration option show throttle
   ```
7. Wenn das System bereit ist, starten Sie die Speichermigration.

   ```
   # storage migration start source-enclosures 7:2 destination-
   enclosures 7:4
   ```
8. Zeigen Sie optional den Festplattenstatus für die Quell- und Zielfestplatten während der Migration an.

   ```
   # disk show state
   ```

   Während der Migration sollten die Quellfestplatten den Status "Migrating" und die Zielfestplatten den Status "Destination" aufweisen.
9. Überprüfen Sie den Migrationsstatus nach Bedarf.

   ```
   # storage migration status
   ```
10. Zeigen Sie den Festplattenstatus für die Quell- und Zielfestplatten an.

```
# disk show state
```

Während der Migration sollten die Quellfestplatten den Status "Migrating" und die Zielfestplatten den Status "Destination" aufweisen.

11. Wenn die Migration abgeschlossen ist, aktualisieren Sie die Konfiguration, um die Zielgehäuse zu verwenden.

Hinweis

Diese Aufgabe startet das Dateisystem neu und dauert in der Regel 10 bis 15 Minuten. Das System ist während dieser Zeit nicht verfügbar.

```
storage migration finalize
```

12. Wenn Sie alle Daten aus den Quellgehäusen entfernen möchten, entfernen Sie die Daten jetzt.

```
storage sanitize start enclosure <enclosure-id>[:<pack-id>]
```

Hinweis

Der Befehl "storage sanitize" führt nicht zu einer zertifizierten Datenlöschung. Data Domain bietet eine zertifizierte Datenlöschung als Service. Weitere Informationen erhalten Sie bei Ihrem Data Domain-Vertriebsmitarbeiter.

13. Zeigen Sie den Festplattenstatus für die Quell- und Zielfestplatten an.

```
# disk show state
```

Nach der Migration sollten die Quellfestplatten den Status "Unkown" und die Zielfestplatten den Status "Active" aufweisen.

Ergebnisse

Nach der Migrationsfinalisierung verwendet das System den Zielspeicher und der Quellspeicher kann entfernt werden.

Beispiel für die CLI-Speichermigration

elicense show

```
# elicense show
Feature licenses:
## Feature     Count Mode            Expiration Date
-- ----------- ----- --------------- ---------------
1  REPLICATION 1     permanent (int) n/a
2  VTL         1     permanent (int) n/a
-- ----------- ----- --------------- ---------------
```

elicense update

```
# elicense update mylicense.lic
New licenses: Storage Migration
Feature licenses:
## Feature          Count   Mode             Expiration Date
-- -----------       -----  ---------------  ---------------
1  REPLICATION       1      permanent (int)  n/a
2  VTL               1      permanent (int)  n/a
3  Storage Migration 1      permanent (int)
-- -----------       -----  ---------------  ---------------
** This will replace all existing Data Domain licenses on the system with the above EMC ELMS
licenses.
Do you want to proceed? (yes|no) [yes]: yes
eLicense(s) updated.
```

disk show state

```
# disk show state
Enclosure        Disk
  Row(disk-id)    1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
--------------   ---------------------------------------------
1                 .  .  .  .
2                 U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3                 U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
4                 U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
5                 v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6                 U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
7                |--------|--------|--------|--------|
                  | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
      E(49-60)    |U  U  U |.  .  s |U  U  U |U  U  U |
      D(37-48)    |U  U  U |.  .  . |U  U  U |U  U  U |
      C(25-36)    |U  U  U |.  .  . |U  U  U |U  U  U |
      B(13-24)    |U  U  U |.  .  . |U  U  U |U  U  U |
      A( 1-12)    |U  U  U |.  .  . |U  U  U |U  U  U |
                  |--------|--------|--------|--------|
--------------   ---------------------------------------------

Legend   State            Count
------   ---------------  -----
.        In Use Disks     18
s        Spare Disks      1
v        Available Disks  15
U        Unknown Disks    105
------   ---------------  -----
```

storage migration precheck

```
#storage migration precheck  source-enclosures 2  destination-enclosures 11

  Source enclosures:
  Disks      Count   Disk    Disk         Enclosure   Enclosure
                     Group   Size         Model       Serial No.
  --------   -----   -----   ----------   ---------   --------------
  2.1-2.15   15      dg1     1.81 TiB     ES30        APM00111103820
  --------   -----   -----   ----------   ---------   --------------
  Total source disk size: 27.29 TiB

  Destination enclosures:
  Disks        Count   Disk      Disk       Enclosure   Enclosure
                       Group     Size       Model       Serial No.
  ----------   -----   -------   --------   ---------   --------------
  11.1-11.15   15      unknown   931.51 GiB ES30        APM00111103840
  ----------   -----   -------   --------   ---------   --------------
  Total destination disk size: 13.64 TiB

      1 "Verifying platform support.....................................PASS"
      2 "Verifying valid storage migration license exists...............PASS"
      3 "Verifying no other migration is running........................PASS"
      4 "Verifying request matches interrupted migration................PASS"
      5 "Verifying data layout on the source shelves....................PASS"
      6 "Verifying final system capacity................................PASS"
      7 "Verifying destination capacity.................................PASS"
      8 "Verifying source shelves belong to same tier...................PASS"
      9 "Verifying enclosure 1 is not used as source....................PASS"
     10 "Verifying destination shelves are addable to storage...........PASS"
     11 "Verifying no RAID reconstruction is going on in source shelves.....PASS"
Migration pre-check PASSED

Expected time to migrate data: 8 hrs 33 min
```

storage migration show history

```
# storage migration show history
Id   Source        Source Enclosure   Dest          Dest Enclosure    Status      Start Time                 End Time
     Enclosure*    Serial No.         Enclosure*    Serial No.
--   ----------    ----------------   ----------    --------------    ---------   ------------------------   ------------------------
2    9:0           SHU952400106A23    7:0           SHU9524084G055B   Finalized   Sat Aug  8 11:59:37 2015   Mon Aug 10 11:10:11 2015
1    9:0           SHU952400106A23    7:0           SHU9524084G055B   Finalized   Thu Aug  6 16:39:55 2015   Fri Aug  7 10:28:07 2015
                                      8:0           SHU9524084G04LR
--   ----------    ----------------   ----------    --------------    ---------   ------------------------   ------------------------
(*) Enclosure ids at migration start time.
```

storage migration start

```
#storage migration start  source-enclosures 2  destination-enclosures 11

  Source enclosures:
  Disks      Count   Disk    Disk         Enclosure   Enclosure
                     Group   Size         Model       Serial No.
  --------   -----   -----   ----------   ---------   --------------
  2.1-2.15   15      dg1     1.81 TiB     ES30        APM00111103820
  --------   -----   -----   ----------   ---------   --------------
  Total source disk size: 27.29 TiB

  Destination enclosures:
  Disks        Count   Disk      Disk       Enclosure   Enclosure
                       Group     Size       Model       Serial No.
  ----------   -----   -------   --------   ---------   --------------
  11.1-11.15   15      unknown   931.51 GiB ES30        APM00111103840
  ----------   -----   -------   --------   ---------   --------------
  Total destination disk size: 13.64 TiB

  Expected time to migrate data: 84 hrs 40 min

**   Storage migration once started cannot be aborted.
     Existing data on the destination shelves will be overwritten.
        Do you want to continue with the migration? (yes|no) [no]: yes

Performing migration pre-check:
      1 Verifying platform support.....................................................PASS
      2 Verifying valid storage migration license exists...............................PASS
      3 Verifying no other migration is running.......................................PASS
      4 Verifying request matches interrupted migration...............................PASS
      5 Verifying data layout on the source shelves...................................PASS
      6 Verifying final system capacity...............................................PASS
      7 Verifying destination capacity................................................PASS
      8 Verifying source shelves belong to same tier..................................PASS
      9 Verifying enclosure 1 is not used as source...................................PASS
     10 Verifying destination shelves are addable to storage..........................PASS
     11 Verifying no RAID reconstruction is going on in source shelves................PASS

Migration pre-check PASSED

Storage migration will reserve space in the filesystem to migrate data.
Space reservation may add up to an hour or more based on system resources.

Storage migration process initiated.
Check storage migration status to monitor progress.
```

storage migration status

```
# storage migration status
Id   Source        Destination   State       Percent    Estimated Time to Complete   Current Throttle
     Enclosure(s)  Enclosure(s)              Complete                                Setting
--   ------------  ------------  ---------   --------   --------------------------   ----------------
5    7:2           7:4           migrating   45%        30 hrs 18 mins               high
--   ------------  ------------  ---------   --------   --------------------------   ----------------
```

disk show state, migration in progress

```
# disk show state
Enclosure         Disk
  Row(disk-id)    1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
--------------    -----------------------------------------------
1                 .  .  .  .
2                 U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3                 U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
4                 U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
5                 v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6                 U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
7                 |--------|--------|--------|--------|
                  | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
      E(49-60)    |U  U  U |m  m  s |U  U  U |s  d  d |
      D(37-48)    |U  U  U |m  m  m |U  U  U |d  d  d |
      C(25-36)    |U  U  U |m  m  m |U  U  U |d  d  d |
      B(13-24)    |U  U  U |m  m  m |U  U  U |d  d  d |
      A( 1-12)    |U  U  U |m  m  m |U  U  U |d  d  d |
                  |--------|--------|--------|--------|
--------------    -----------------------------------------------

Legend   State               Count
------   -----------------   -----
.        In Use Disks        4
s        Spare Disks         2
v        Available Disks     15
U        Unknown Disks       90
m        Migrating Disks     14
d        Destination Disks   14
```

storage migration finalize

```
# storage migration finalize

Storage migration finalize restarts the filesystem.
This can take several minutes and the filesystem is unavailable until the operation completes.
        Do you want to continue? (yes|no) [no]: yes

Performing migration finalization pre-check:
(P1)    Verifying storage migration is ready for finalization....PASS
(P2)    Verifying there are no foreign disks.....................PASS
(P3)    Verifying data layout on the source shelves..............PASS

Migration finalization pre-check PASSED
Finalizing the storage migration with id 5:

Notifying filesystem to finalize migration...

Done.

Disabling the filesystem
Please wait..........
The filesystem is now disabled.
Removing source enclosures from filesystem...

Done.

Removing source enclosures from storage tier...

Done.

Enabling the filesystem
Please wait.....................
The filesystem is now enabled.
Storage migration with id 5 from enclosure(s) 7.2 to enclosure(s) 7.4 has been finalized.
```

disk show state, migration complete

```
# disk show state
Enclosure         Disk
  Row(disk-id)     1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
--------------    ---------------------------------------------
1                  .  .  .  .
2                  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3                  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
4                  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
5                  v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6                  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
7                 |--------|--------|--------|--------|
                  | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
      E(49-60)    |U  U  U |U  U  U |U  U  U |s  .  . |
      D(37-48)    |U  U  U |U  U  U |U  U  U |.  .  . |
      C(25-36)    |U  U  U |U  U  U |U  U  U |.  .  . |
      B(13-24)    |U  U  U |U  U  U |U  U  U |.  .  . |
      A( 1-12)    |U  U  U |U  U  U |U  U  U |.  .  . |
                  |--------|--------|--------|--------|
--------------    ---------------------------------------------

Legend   State             Count
------   ---------------   -----
.        In Use Disks      18
s        Spare Disks       1
v        Available Disks   15
U        Unknown Disks     105
------   ---------------   -----
```

Hinweis

Die Speichermigration wird derzeit nur auf dem aktiven Node unterstützt. Die Speichermigration wird auf dem Stand-by-Node eines HA-Clusters nicht unterstützt.

KAPITEL 12

Metadaten on Flash

Inhalt dieses Kapitels:

Übersicht über Metadata on Flash (MDoF)

MDoF erstellt Caches für Dateisystem-Metadaten mit Flash-Technologien. Der SSD-Cache ist ein Cache mit niedriger Latenz und hoher Anzahl an Eingabe-/Ausgabevorgängen pro Sekunde (IOPS, Input/Output Operations Per Second) zur Beschleunigung des Metadaten- und Datenzugriffs.

Hinweis

Die minimale erforderliche Softwareversion ist DD OS 6.0.

Das Zwischenspeichern von Dateisystem-Metadaten auf SSDs verbessert die I/O-Performance sowohl für herkömmliche als auch für zufällige Workloads.

Bei herkömmlichen Workloads ermöglicht die Auslagerung von zufälligem Zugriff auf Metadaten von HDDs auf SSDs den Festplatten, Streaming-Schreibanforderungen und Streaming-Leseanforderungen zu erfüllen.

Bei zufälligen Workloads bietet SSD-Cache Metadatenvorgänge mit niedriger Latenz, mit denen die HDDs Datenanforderungen anstelle von Cacheanfragen bedienen können.

Lesecache auf SSD verbessert die Performance bei zufälligen Lesevorgängen durch das Zwischenspeichern der Daten, auf die häufig zugegriffen wird. Das Schreiben von Daten auf NVRAM in Kombination mit Metadatenvorgängen mit niedriger Latenz, um den NVRAM-Drain zu beschleunigen, verbessert die Latenz zufälliger Schreibvorgänge. Das Fehlen des Cache verhindert den Dateisystembetrieb nicht. Es wirkt sich nur auf die Performance des Dateisystems aus.

Wenn der Cache-Tier erstellt wird, ist ein Dateisystem-Neustart nur erforderlich, wenn der Cache-Tier nach der Ausführung des Dateisystems hinzugefügt wird. Für neue Systeme mit Cache-Tier-Datenträgern ist kein Dateisystem-Neustart erforderlich, wenn der Cache-Tier vor der ersten Aktivierung des Dateisystems erstellt wird. Zusätzlicher Cache kann in einem Livesystem hinzugefügt werden, ohne die Notwendigkeit, das Dateisystem zu deaktivieren und zu aktivieren.

Hinweis

DD9500-Systeme, die von DD OS 5.7 auf DD OS 6.0 aktualisiert wurden, erfordern nach der erstmaligen Erstellung des Cache-Tier einen einmaligen Dateisystem-Neustart.

Eine bestimmte Bedingung im Hinblick auf die SSDs ist, dass die SSD eine Nur-Lese-Bedingung ausgibt, wenn die Anzahl der verbleibenden freien Blöcke nahe 0 geht. Wenn eine einzige Lesebedingung auftritt, behandelt DD OS das Laufwerk als Nur-Lese-Cache und sendet eine Warnmeldung.

MDoF wird auf den folgenden Data Domain-Systemen unterstützt:

- DD6300
- DD6800
- DD9300
- DD9500
- DD9800

- DD VE-Instanzen, einschließlich DD3300-Systemen, in Kapazitätskonfigurationen von 16 TB und höher (SSD-Cache-Tier für DD VE)

MDoF – Lizenzierung und Kapazität

Eine über ELMS aktivierte Lizenz ist für die Verwendung der Funktion MDoF erforderlich. Die SSD-Cachelizenz wird standardmäßig nicht aktiviert.

In der folgenden Tabelle werden die verschiedenen SSD-Kapazitätslizenzen und die SSD-Kapazitäten für das bestimmte System beschrieben:

Tabelle 116 SSD-Kapazitätslizenzen pro System

Modell	Arbeitsspeicher	Anzahl der SSDs	SSD-Kapazität
DD6300	48 GB (Basis)	1	800 GB
	96 GB (erweitert)	2	1600 GB
DD6800	192 GB (Basis)	2	1600 GB
	192 GB (erweitert)	4	3200 GB
DD9300	192 GB (Basis)	5	4000 GB
	384 GB (erweitert)	8	6400 GB
DD9500	256 GB (Basis)	8	6400 GB
	512 GB (erweitert)	15	12000 GB
DD9800	256 GB (Basis)	8	6400 GB
	768 GB (erweitert)	15	12000 GB

SSD-Cache-Tier für DD VE

DD VE-Instanzen und DD3300-Systeme benötigen keine Lizenz für den SSD-Cache-Tier. Die maximale unterstützte SSD-Kapazität ist 1 % der aktiven Tier-Kapazität.

In der folgenden Tabelle werden die verschiedenen SSD-Kapazitätslizenzen und die SSD-Kapazitäten für das bestimmte System beschrieben:

Tabelle 117 DD VE und DD3300 – SSD-Kapazität

Kapazitätskonfiguration	Maximale SDS-Kapazität
DD VE 16 TB	160 GB
DD VE 32 TB	320 GB
DD VE 48 TB	480 GB
DD VE 64 TB	640 GB
DD VE 96 TB	960 GB
DD3300 16 TB	160 GB
DD3300 32 TB	320 GB

SSD-Cache-Tier

Der SSD-Cache-Tier bietet den SSD-Cachespeicher für das Dateisystem. Das Dateisystem nutzt den erforderlichen Speicher vom SSD-Cache-Tier ohne aktiven Benutzereingriff.

MDoF-SSD-Cache-Tier – Systemmanagement

Beachten Sie die folgenden Hinweise für SSD-Cache:

- Wenn SSDs in einem Controller bereitgestellt werden, werden diese SSDs als interne Root-Laufwerke behandelt. Sie werden als Gehäuse 1 in der Ausgabe des Befehls `storage show all` angezeigt.
- Managen Sie einzelne SSDs mit dem Befehl `disk` auf dieselbe Weise, wie HDDs gemanagt werden.
- Führen Sie den Befehl `storage add` aus, um eine einzelne SSD oder ein einzelnes SSD-Gehäuse zum SSD-Cache-Tier hinzuzufügen.
- Der SSD-Cache-Tier-Bereich muss nicht gemanagt werden. Das Dateisystem nutzt den erforderlichen Speicher aus dem SSD-Cache-Tier und teilt diesen zwischen den Clients auf.
- Der Befehl `filesys create` erstellt ein SSD-Volume, wenn SSDs im System verfügbar sind.

  Hinweis

  Wenn SSDs später zum System hinzugefügt werden, sollte das System automatisch das SSD-Volume erstellen und das Dateisystem benachrichtigen. SSD Cache Manager benachrichtigt seine registrierten Clients, damit sie ihre Cachespeicherobjekte erstellen können.

- Wenn das SSD-Volume nur ein aktives Laufwerk enthält, geht das letzte Laufwerk offline und wird wieder online geschaltet, wenn das aktive Laufwerk aus dem System entfernt wird.

Im nächsten Abschnitt wird beschrieben, wie Sie den SSD-Cache-Tier aus Data Domain System Manager und mit der DD OS-Befehlszeilenoberfläche managen.

Managen von SSD-Cache-Tier

Mit den Speicherkonfigurationsfunktionen können Sie dem SSD-Cache-Tier Speicher hinzufügen und ihn daraus entfernen.

Vorgehensweise

1. Wählen Sie **Hardware** > **Storage** > **Overview** aus.
2. Erweitern Sie das Dialogfeld **Cache Tier**.
3. Klicken Sie auf **Konfigurieren**.

   Die maximale Speichermenge, die zum aktiven Tier hinzugefügt werden kann, hängt vom verwendeten DD-Controller ab.

Hinweis

Die Leiste der lizenzierten Kapazität zeigt den Umfang der lizenzierten Kapazität (verwendet und verbleibend) für die installierten Gehäuse an.

4. Aktivieren Sie das Kontrollkästchen für den Einschub, der hinzugefügt werden soll.
5. Klicken Sie auf die Schaltfläche **Add to Tier**.
6. Klicken Sie auf **OK**, um den Speicher hinzuzufügen.

Hinweis

Wenn Sie einen hinzugefügten Einschub entfernen möchten, wählen Sie ihn in der Liste „Tier Configuration“ aus, klicken Sie **Remove from Configuration** und klicken Sie dann auf **OK**.

CLI-Entsprechung
Wenn die Cache-Tier-SSDs in der Haupteinheit installiert sind:

a. Fügen Sie die SSDs dem Cache-Tier hinzu.

```
#  storage add disks 1.13,1.14 tier cache
Checking storage requirements...done
Adding disk 1.13 to the cache tier...done

Updating system information...done

Disk 1.13 successfully added to the cache tier.


Checking storage requirements...
done
Adding disk 1.14 to the cache tier...done

Updating system information...done

Disk 1.14 successfully added to the cache tier.
```

b. Überprüfen Sie den Status der neu hinzugefügten SSDs.

```
# disk show state
Enclosure   Disk
             1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
---------   ------------------------------------------------
1            .  .  .  .  s  .  .  s  s  s  s  s  v  v
2            U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3            U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
---------   ------------------------------------------------

Legend   State             Count
------   ---------------   -----
.        In Use Disks      6
s        Spare Disks       6
v        Available Disks   2
U        Unknown Disks     30
------   ---------------   -----
Total 44 disks
```

Wenn die Cache-Tier-SSDs in einem externen Einschub installiert sind:

a. Überprüfen Sie, ob das System die neue SSD erkennt. Im folgenden Beispiel ist der SSD-Einschub Gehäuse 2.

```
# disk show state
Enclosure   Disk
```

```
Row(disk-id) 1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
---------    ----------------------------------------------
1            .  .  .  .
2            U  U  U  U  U  U  U  U  -  -  -  -  -  -  -
3            .  .  .  .  .  .  .  .  .  .  .  .  .  .  v
4            .  .  .  .  .  .  .  .  .  .  .  .  .  .  v
5            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
7            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
8            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
9            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
10           |--------|--------|--------|--------|
             | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
   E(49-60)  |v  v  v |v  v  v |v  v  v |v  v  v |
   D(37-48)  |v  v  v |v  v  v |v  v  v |v  v  v |
   C(25-36)  |v  v  v |v  v  v |v  v  v |v  v  v |
   B(13-24)  |v  v  v |v  v  v |v  v  v |v  v  v |
   A( 1-12)  |v  v  v |v  v  v |v  v  v |v  v  v |
             |--------|--------|--------|--------|
11           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
12           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
13           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
---------    ----------------------------------------------

Legend   State               Count
------   ------------------  -----
.        In Use Disks        32
v        Available Disks     182
U        Unknown Disks       8
-        Not Installed Disks 7
------   ------------------ -----
Total 222 disks
```

b. Bestimmen Sie die Einschub-ID des SSD-Einschubs. SSDs werden in der Spalte `Type` als `SAS-SSD` oder `SATA-SSD` angezeigt.

```
#  disk show hardware
```

```
Disk        Slot  Manufacturer/Model                    Firmware  Serial No.              Capacity     Type
(enc/disk)
----------  ----  ------------------------------------  --------  ----------------------  ----------   --------
1.1         0     TG32C10400GA3EMC_____________118000371  PRO6E344  FG009826                372.61 GiB  SATA-SSD
1.2         1     TG32C10400GA3EMC_____________118000371  PRO6E344  FG0097VL                372.61 GiB  SATA-SSD
1.3         2     TG32C10400GA3EMC_____________118000371  PRO6E344  FG009881                372.61 GiB  SATA-SSD
1.4         3     TG32C10400GA3EMC_____________118000371  PRO6E344  FG00988X                372.61 GiB  SATA-SSD
2.1         0     HITACHI HUSMR148_CLAR800                C29C      07V4P2AA                745.22 GiB  SAS-SSD
2.2         1     HITACHI HUSMR148_CLAR800                C29C      07V4P3LA                745.22 GiB  SAS-SSD
2.3         2     HITACHI HUSMR148_CLAR800                C29C      07V4P2XA                745.22 GiB  SAS-SSD
2.4         3     HITACHI HUSMR148_CLAR800                C29C      07V4TW4A                745.22 GiB  SAS-SSD
2.5         4     HITACHI HUSMR148_CLAR800                C29C      07V4ULYA                745.22 GiB  SAS-SSD
2.6         5     HITACHI HUSMR148_CLAR800                C29C      07V4P0BA                745.22 GiB  SAS-SSD
2.7         6     HITACHI HUSMR148_CLAR800                C29C      07V4UVBA                745.22 GiB  SAS-SSD
2.8         7     HITACHI HUSMR148_CLAR800                C29C      07V4UTNA                745.22 GiB  SAS-SSD
```

c. Fügen Sie den SSD-Einschub dem Cache-Tier hinzu.

```
#  storage add enclosure 2 tier cache
```

```
sysadmin@apolloplus-1# storage add enclosure 2 tier cache

Checking storage requirements...done
Adding enclosure 2 to the cache tier...Enclosure 2 successfully added to the cache tier.

Updating system information...done

Successfully added: 2  done
```

d. Überprüfen Sie den Status der neu hinzugefügten SSDs.

```
# disk show state
Enclosure   Disk
Row(disk-id) 1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
---------    ----------------------------------------------
1            .  .  .  .
2            .  .  .  .  .  .  .  .  -  -  -  -  -  -  -
3            .  .  .  .  .  .  .  .  .  .  .  .  .  .  v
```

```
4            .  .  .  .  .  .  .  .  .  .  .  .  .  .  v
5            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
7            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
8            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
9            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
10          |--------|--------|--------|--------|
            | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
   E(49-60) |v  v  v |v  v  v |v  v  v |v  v  v |
   D(37-48) |v  v  v |v  v  v |v  v  v |v  v  v |
   C(25-36) |v  v  v |v  v  v |v  v  v |v  v  v |
   B(13-24) |v  v  v |v  v  v |v  v  v |v  v  v |
   A( 1-12) |v  v  v |v  v  v |v  v  v |v  v  v |
            |--------|--------|--------|--------|
11           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
12           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
13           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
---------   ---------------------------------------------

Legend   State               Count
------   ----------------   -----
.        In Use Disks       32
v        Available Disks    182
U        Unknown Disks      8
-        Not Installed Disks 7
------   ------------------ -----
Total 222 disks
```

So entfernen Sie eine Controller-gemountete SSD aus dem Cache-Tier:

```
# storage remove disk 1.13

Removing disk 1.13...done

Updating system information...done

Disk 1.13 successfully removed.
```

So entfernen Sie einen SSD-Einschub aus dem System:

```
# storage remove enclosure 2

Removing enclosure 2...Enclosure 2 successfully removed.

Updating system information...done

Successfuly removed: 2 done
```

SSD-Warnmeldungen

Es gibt drei für den SSD-Cache-Tier spezifische Warnmeldungen.

Die SSD-Cache-Tier-Warnmeldungen sind:

- Lizenzierung
  Wenn das Dateisystem aktiviert und weniger physische Cachekapazität vorhanden ist, als mit der Lizenz konfigurierbar, wird eine Warnmeldung mit der aktuellen, vorhandenen SSD-Kapazität und der Kapazitätslizenz erzeugt. Diese Warnmeldung wird als Warnung klassifiziert. Das Fehlen des Cache verhindert den Dateisystembetrieb nicht. Es wirkt sich nur auf die Performance des Dateisystems aus. Zusätzlicher Cache kann in einem Livesystem hinzugefügt werden, ohne die Notwendigkeit, das Dateisystem zu deaktivieren und zu aktivieren.
- Nur-Lese-Bedingung

Die SSD gibt eine Nur-Lese-Bedingung aus, wenn die Anzahl der verbleibenden freien Blöcke nahe 0 geht. Wenn eine einzige Lesebedingung auftritt, behandelt DD OS das Laufwerk als Nur-Lese-Cache.

Die Warnmeldung `EVT-STORAGE-00001` wird angezeigt, wenn die SSD in einen schreibgeschützten Zustand versetzt wird und ersetzt werden muss.

- Ende der Nutzungsdauer der SSD
  Wenn eine SSD das Ende ihrer Nutzungsdauer erreicht, generiert das System eine Warnmeldung zur fehlgeschlagenen Hardware und identifiziert die Position der SSD im SSD-Gehäuse. Diese Warnmeldung wird als kritische Warnung klassifiziert.

  Die Warnmeldung `EVT-STORAGE-00016` wird angezeigt, wenn der EOL-Zähler 98 erreicht. Das Laufwerk schlägt proaktiv fehl, wenn der EOL-Zähler 99 erreicht.

KAPITEL 13

SCSI-Ziel

Dieses Kapitel enthält Folgendes:

Überblick über SCSI Target

SCSI (Small Computer System Interface) Target ist ein Daemon für das einheitliche Management aller SCSI-Services und -Transporte. SCSI Target unterstützt DD VTL (Virtual Tape Library), DD Boost over FC (Fibre Channel) und vDisk/ProtectPoint Block Services sowie Elemente mit einer Ziel-LUN (Logical Unit Number) in einem DD-System.

Services und Transporte von SCSI Target

Der SCSI Target-Daemon wird gestartet, wenn FC-Ports vorhanden sind oder DD VTL lizenziert ist. Es bietet ein einheitliches Management für alle SCSI-Ziel-*services* und -*transporte*.

- Ein *Service* ist ein beliebiger Service mit einer Ziel-LUN in einem DD-System, der SCSI Target-Befehle verwendet, z. B. DD VTL (Bandlaufwerke und Wechsler), DD Boost over FC (Prozessorgeräte) oder vDisk (virtuelle Laufwerkgeräte).
- Ein *Transport* ermöglicht *Geräten*, für die *Initiatoren* sichtbar zu werden.
- Ein *Initiator* ist ein Backupclient, der mit einem System verbunden ist, um Daten mithilfe des FC-Protokolls zu lesen und schreiben. Ein bestimmter Initiator kann DD Boost über FC, vDisk oder DD VTL unterstützen, aber nicht alle drei.
- *Geräte* sind im SAN (Storage Area Network) über physische Ports sichtbar. Hostinitiatoren kommunizieren mit dem DD-System über das SAN.
- *Zugriffsgruppen* managen den Zugriff zwischen Geräten und Initiatoren.
- Ein *Endpunkt* ist das logische Ziel auf einem DD-System, mit dem ein Initiator verbunden ist. Sie können Endpunkte deaktivieren, aktivieren und umbenennen. Damit Endpunkte gelöscht werden können, darf die zugehörige Transporthardware nicht mehr vorhanden sein. Endpunkte werden automatisch erkannt und erstellt, wann eine neue Transportverbindung auftritt. Endpunkte haben die folgenden Attribute: Porttopologie, FCP2-RETRY-Status, WWPN und WWNN.
- *NPIV* (N_port ID Virtualization) ist eine FC-Funktion, mit der mehrere Endpunkte einen einzigen physischen Port gemeinsam nutzen können. NPIV reduziert Anforderungen an die Hardware und bietet Failover-Funktionen.
- In DD OS 6.0 können Benutzer die Reihenfolge der sekundären Systemadressen für Failover angeben. Wenn das System 0a, 0b, 1a, 1b angibt und der Benutzer 1b, 1a, 0a, 0b angibt, wird beispielsweise die benutzerdefinierte Reihenfolge für das Failover verwendet. Mit dem Befehl `scsitarget endpoint show detailed` wird die benutzerdefinierte Reihenfolge angezeigt.

Beachten Sie die folgenden Ausnahmen:

- DD Boost kann von FC- und IP-Clients gleichzeitig genutzt werden; die beiden Transporte können jedoch nicht denselben Initiator verwenden.
- Pro Zugriffsgruppe darf nur ein Initiator vorhanden sein. Jeder Zugriffsgruppe wird ein Typ zugewiesen (DD VTL, vDisk/ProtectPoint Block Services oder DD Boost over FC).

SCSI Target-Architekturen – unterstützt und nicht unterstützt

SCSI Target unterstützt folgende Architekturen:

- **DD VTL plus DD Boost over FC von unterschiedlichen Initiatoren:** Zwei unterschiedliche Initiatoren (auf einem oder verschiedenen Clients) können über DD VTL und DD Boost over FC auf ein DD-System zugreifen und dabei denselben oder verschiedene DD-System-Zielendpunkte verwenden.

- **DD VTL plus DD Boost over FC von einem Initiator zu zwei verschiedenen DD-Systemen:** Ein Initiator kann über einen beliebigen Service auf zwei verschiedene DD-Systeme zugreifen.

SCSI Target unterstützt die folgende Architektur nicht:

- **DD VTL plus DD Boost over FC von einem Initiator zum selben DD-System:** Ein Initiator kann nicht über verschiedene Services auf dasselbe DD-System zugreifen.

Schlankes Protokoll

Das schlanke Protokoll ist ein einfacher Daemon für VDisk und DD VTL, der auf SCSI-Befehle reagiert, wenn das primäre Protokoll nicht reagieren kann. Ein schlankes Protokoll in Fibre-Channel-Umgebungen mit mehreren Protokollen:

- verhindert, dass der Initiator hängt.
- verhindert unnötige Initiatorabbrüche.
- verhindert das Verschwinden von Initiatorgeräten.
- unterstützt den Stand-by-Modus.
- unterstützt schnelle und früh erkennbare Geräte.
- verbessert das HA-Protokollverhalten.
- erfordert keinen schnellen Zugriff auf die Registrierung.

Weitere Informationen über DD Boost und den CLI-Befehl „scscitarget“

Weitere Informationen über die Verwendung von DD Boost über DD System Manager finden Sie im zugehörigen Kapitel in diesem Handbuch. Andere Arten von Informationen über DD Boost finden Sie im *Data Domain Boost for OpenStorage Administration Guide*.

In diesem Kapitel liegt der Schwerpunkt auf der Verwendung von SCSI Target über DD System Manager. Nachdem Sie sich mit den grundlegenden Aufgaben vertraut gemacht haben, können Sie mit dem Befehl `scscitarget` im *Data Domain Operating System Command Reference Guide* erweiterte Managementaufgaben durchführen.

Vermeiden Sie bei starkem DD VTL-Datenverkehr die Ausführung des Befehls `scsitarget group use`, mit dem für ein oder mehrere SCSI Target- oder vDisk-Geräte in einer Gruppe zwischen primärer und sekundärer Liste der verwendeten Endpunkte gewechselt wird.

Ansicht „Fibre Channel“

Die Ansicht „Fibre Channel“ zeigt den aktuellen Status (ob Fibre Channel und/oder NPIV aktiviert sind/ist). Außerdem werden zwei Registerkarten angezeigt: „Resources“ und „Access Groups“. Ressourcen umfassen Ports, Endpunkte und Initiatoren. Eine Zugriffsgruppe enthält eine Sammlung von Initiator-WWPNs (weltweite Portnamen) oder Aliasnamen sowie die Laufwerke und Wechsler, auf die sie zugreifen dürfen.

Aktivieren von NPIV

NPIV (N_Port ID Virtualization) ist eine Fibre-Channel-Funktion, durch die mehrere Endpunkte einen einzigen physischen Port gemeinsam nutzen können. NPIV reduziert die Anforderungen an die Hardware und bietet Failover/Failback-Funktionen für Endpunkte. NPIV wird nicht standardmäßig konfiguriert; Sie müssen es aktivieren.

Hinweis

NPIV ist standardmäßig für die HA-Konfiguration aktiviert.

NPIV ermöglicht eine vereinfachte Konsolidierung mehrerer Systeme:

- NPIV ist ein ANSI T11-Standard, der es ermöglicht, einen einzigen physischen HBA-Port mit einer Fibre Channel-Fabric mit mehreren WWPNs zu registrieren.
- Die virtuellen und physischen Ports besitzen dieselben Porteigenschaften und verhalten sich genau gleich.
- Möglicherweise gibt es m:1-Beziehungen zwischen den Endpunkten und dem Port, d. h. mehrere Endpunkte können denselben physischen Port gemeinsam nutzen.

Das Aktivieren von NPIV ermöglicht insbesondere die folgenden Funktionen:

- Mehrere Endpunkte sind pro physischem Port zulässig, jeder mit einem virtuellen Port (NPIV). Der Basisport ist ein Platzhalter für den physischen Port und nicht mit einem Endpunkt verbunden.
- Endpunkt-Failover/Failback wird bei Verwendung von NPIV automatisch aktiviert.

  Hinweis

  Nachdem NPIV aktiviert ist, muss die „sekundäre Systemadresse“ auf den einzelnen Endpunkten angegeben werden. Falls dies nicht der Fall ist, erfolgt kein Endpunkt-Failover.

- Mehrere DD-Systeme können in einem einzelnen DD-System konsolidiert werden, die Anzahl der HBAs bleibt jedoch auf den einzelnen DD-Systemen identisch.
- Das Endpunkt-Failover wird ausgelöst, wenn FC-SSM erkennt, dass ein Port von offline zu online wechselt. Wenn der physische Port offline ist, bevor scsitarget aktiviert ist, und der Port weiterhin offline ist, nachdem scsitarget aktiviert ist, ist kein Endpunkt-Failover möglich, da FC-SSM kein Port-Offline-Ereignis erzeugt. Wenn der Port wieder online und automatisches Failback aktiviert ist, wird für alle Failover-Endpunkte, die diesen Port als primären Port verwenden, ein Failback zum primären Port durchgeführt.

Die Data Domain-HA-Funktionen erfordern, dass NPIV WWNs während des Failover-Prozesses zwischen den Nodes eines HA-Paars verschiebt.

Hinweis

Bevor Sie NPIV aktivieren, müssen die folgenden Bedingungen erfüllt sein:

- Das DD-System muss DD OS 5.7 ausführen.
- Alle Ports müssen an 4-Gbit-, 8-Gbit- und 16-Gbit-Fibre-Channel-HBAs und -SLICs angeschlossen sein.
- Die DD-System-ID muss gültig sein, d. h. sie darf nicht 0 sein.

Darüber hinaus werden Porttopologien und Portnamen geprüft und verhindern möglicherweise, dass NPIV aktiviert wird:

- NPIV ist zulässig, wenn die Topologie für *alle* Ports "Loop-preferred" ist.
- NPIV ist zulässig, wenn die Topologie für *einige* der Ports "Loop-preferred" ist; jedoch muss NPIV für "Loop-only"-Ports deaktiviert werden oder Sie müssen die Topologie für eine ordnungsgemäße Funktion in "Loop-preferred" ändern.
- NPIV ist *nicht* zulässig, wenn *keiner* der Ports die Topologie "Loop-preferred" aufweist.
- Wenn die Portnamen in Zugriffsgruppen vorhanden sind, werden die Portnamen durch ihre zugehörigen Endpunktnamen ersetzt.

Vorgehensweise

1. Wählen Sie**Hardware** > **Fibre Channel**.
2. Wählen Sie neben „NPIV: Disabled" die Option **Enable**.
3. Im Dialogfeld "Enable NPIV" werden Sie gewarnt, dass alle Fibre-Channel-Ports deaktiviert werden müssen, bevor NPIV aktiviert werden kann. Wenn Sie sicher sind, dass Sie dies tun möchten, wählen Sie **Yes**.

   CLI-Entsprechung

   a. Sorgen Sie dafür, dass NPIV aktiviert ist (global).

   ```
   # scsitarget transport option show npiv
   SCSI Target Transport Options
   Option   Value
   ------   --------
   npiv     disabled
   ------   --------
   ```

   b. Wenn NPIV deaktiviert ist, aktivieren Sie es. Sie müssen zunächst alle Ports deaktivieren.

   ```
   # scsitarget port disable all
   All ports successfully disabled.
   # scsitarget transport option set npiv enabled
   Enabling FiberChannel NPIV mode may require SAN zoning to
   be changed to configure both base port and NPIV WWPNs.
   Any FiberChannel port names used in the access groups will
   be converted to their corresponding endpoint names in order
   to prevent ambiguity.
       Do you want to continue? (yes|no) [no]:
   ```

   c. Reaktivieren Sie die deaktivierten Ports.

   ```
   # scsitarget port enable all
   All ports successfully enabled.
   ```

   d. Sorgen Sie dafür, dass die physischen Ports die NPIV-Einstellung „Auto“ aufweisen.

```
# scsitarget port show detailed 0a
System Address:     0a
Enabled:            Yes
Status:             Online
Transport:          FibreChannel
Operational Status: Normal
FC NPIV:            Enabled (auto)
.
.
.
```

e. Erstellen Sie einen neuen Endpunkt unter Verwendung der primären und sekundären Ports, die Sie ausgewählt haben.

```
# scsitarget endpoint add test0a0b system-address 0aprimary-
system-address 0a secondary-system-address 0b
```

Beachten Sie, dass der Endpunkt standardmäßig deaktiviert ist. Aktivieren Sie ihn.

```
# scsitarget endpoint enable test0a0b
```

Zeigen Sie dann die Endpunktinformationen an.

```
# scsitarget endpoint show detailed test0a0b
Endpoint:                 test0a0b
Current System Address:   0b
Primary System Address:   0a
Secondary System Address: 0b
Enabled:                  Yes
Status:                   Online
Transport:                FibreChannel
FC WWNN:                  50:02:18:80:08:a0:00:91
FC WWPN:                  50:02:18:84:08:b6:00:91
```

f. Verwenden Sie Zoning zum automatisch generierten WWPN des neu erstellten Endpunkts für ein Hostsystem.

g. Erstellen Sie ein DD VTL-, vDisk- oder DD Boost über Fibre Channel-Gerät (DFC) und stellen Sie dieses Gerät auf dem Hostsystem zur Verfügung.

h. Sorgen Sie dafür, dass das ausgewählte DD-Gerät auf dem Host zugänglich ist (Lese- und/oder Schreibzugriff).

i. Testen Sie das Endpunkt-Failover, indem Sie die „sekundäre“ Option verwenden, um den Endpunkt zur SSA (Secondary System Address) zu verschieben.

```
# scsitarget endpoint use test0a0b secondary
```

j. Sorgen Sie dafür, dass das ausgewählte DD-Gerät weiterhin auf dem Host zugänglich ist (Lese- und/oder Schreibzugriff). Testen Sie das Failback, indem Sie die „primäre“ Option verwenden, um den Endpunkt zurück zur PSA (Primary System Address) zu verschieben.

```
# scsitarget endpoint use test0a0b primary
```

k. Sorgen Sie dafür, dass das ausgewählte DD-Gerät weiterhin auf dem Host zugänglich ist (Lese- und/oder Schreibzugriff).

Deaktivieren von NPIV

Wenn Sie NPIV deaktivieren möchten, dürfen keine Ports mit mehreren Endpunkten vorhanden sein.

Hinweis

NPIV ist für die HA-Konfiguration erforderlich. Es ist standardmäßig aktiviert und kann nicht deaktiviert werden.

Vorgehensweise

1. Wählen Sie**Hardware** > **Fibre Channel**.
2. Wählen Sie neben "NPIV: Enabled" die Option **Disable**.
3. Prüfen Sie im Dialogfeld "Disable NPIV" alle Meldungen zum Korrigieren der Konfiguration. Wenn Sie fertig sind, wählen Sie **OK**.

Registerkarte „Resources“

Auf der Registerkarte **Hardware** > **Fibre Channel** > **Phyical Resources** werden Informationen zu Ports, Endpunkten und Initiatoren angezeigt.

Tabelle 118 Ports

Element	Beschreibung
System Address	Systemadresse für Port
WWPN	Eindeutiger weltweiter Portname, eine 64-Bit-Kennung (ein 60-Bit-Wert nach einer 4-Bit-*Network Address-Authority*-Kennung) des FC-Ports (Fibre Channel)
WWNN	Eindeutiger weltweiter Node-Name, eine 64-Bit-Kennung (ein 60-Bit-Wert nach einer 4-Bit-*Network Address-Authority*-Kennung) des FC-Node
Enabled	Portbetriebsstatus, entweder „Enabled“ oder „Disabled“
NPIV	NPIV-Status, entweder „Enabled“ oder „Disabled“
Link Status	Verbindungsstatus: entweder „Online“ oder „Offline“, je nachdem, ob der Port betriebsbereit ist und Datenverkehr verarbeiten kann
Operation Status	Betriebsstatus: entweder „Normal“ oder „Marginal“
# of Endpoints	Anzahl der Endpunkte, die diesem Port zugeordnet sind

Tabelle 119 Endpunkte

Element	Beschreibung
Name	Name des Endpunkts
WWPN	Eindeutiger weltweiter Portname, eine 64-Bit-Kennung (ein 60-Bit-Wert nach einer 4-Bit-*Network Address-Authority*-Kennung) des FC-Ports (Fibre Channel)
WWNN	Eindeutiger weltweiter Node-Name, eine 64-Bit-Kennung (ein 60-Bit-Wert nach einer 4-Bit-*Network Address-Authority*-Kennung) des FC-Node
System Address	Systemadresse des Endpunkts.
Enabled	Portbetriebsstatus, entweder „Enabled“ oder „Disabled“

Tabelle 119 Endpunkte (Fortsetzung)

Element	Beschreibung
Link Status	„Online“ oder „Offline“, je nachdem, ob der Port betriebsbereit ist und Datenverkehr verarbeiten kann

Tabelle 120 Initiators

Element	Beschreibung
Name	Name des Initiators
Service	Service-Unterstützung durch den Initiator, entweder DD VTL, DD Boost oder vDisk
WWPN	Eindeutiger weltweiter Portname, eine 64-Bit-Kennung (ein 60-Bit-Wert nach einer 4-Bit-*Network Address-Authority*-Kennung) des FC-Ports (Fibre Channel)
WWNN	Eindeutiger weltweiter Node-Name, eine 64-Bit-Kennung (ein 60-Bit-Wert nach einer 4-Bit-*Network Address-Authority*-Kennung) des FC-Node
Vendor Name	Initiatormodell
Online Endpoints	Endpunkte, die von diesem Initiator gesehen werden; Anzeige von `none` oder `offline`, wenn der Initiator nicht verfügbar ist

Konfigurieren eines Ports

Ports werden erkannt und ein einzelner Endpunkt wird automatisch für jeden Port beim Start erstellt.

Die Eigenschaften des Basisports hängen davon ab, ob NPIV aktiviert ist:

- Im Nicht-NPIV-Modus verwenden Ports dieselben Eigenschaften wie der Endpunkt, d. h. der WWPN für den Basisport und der Endpunkt sind identisch.
- Im NPIV-Modus werden die Basisporteigenschaften von Standardwerten abgeleitet, d. h. ein neuer WWPN wird für den Basisport generiert und beibehalten, um konsistentes Wechseln zwischen NPIV-Modi zu ermöglichen. Der NPIV-Modus bietet außerdem die Möglichkeit, mehrere Endpunkte pro Port zu unterstützen.

Vorgehensweise

1. Wählen Sie **Hardware** > **Fibre Channel** > **Resources**.
2. Wählen Sie unter **Ports** einen Port und wählen Sie dann**Modify** (Stift).
3. Wählen Sie im Dialogfeld "Configure Port", ob NPIV für diesen Port automatisch aktiviert oder deaktiviert werden soll.
4. Wählen Sie für "Topology" die Option "Loop Preferred", "Loop Only", "Point to Point" oder "Default".
5. Wählen Sie für "Speed" die Option "1 Gbps", "2 Gbps", "4 Gbps", "8 Gbps" oder "auto".
6. Wählen Sie **OK** aus.

Aktivieren eines Ports

Ports müssen aktiviert sein, bevor sie verwendet werden können.

Vorgehensweise

1. Wählen Sie**Hardware** > **Fibre Channel** > **Resources**.
2. Wählen Sie **More Tasks** > **Ports** > **Enable**. Wenn bereits alle Ports aktiviert sind, wird eine entsprechende Meldung angezeigt.
3. Klicken Sie im Dialogfeld „Enable Ports“ auf einen oder mehrere Ports in der Liste und wählen Sie **Next** aus.
4. Wählen Sie nach der Bestätigung **Next** aus, um die Aufgabe abzuschließen.

Deaktivieren eines Ports

Sie können einfach einen Port (oder Ports) deaktivieren oder ein Failover für alle Endpunkte des Ports (oder der Ports) zu einem anderen Port durchführen.

Vorgehensweise

1. Wählen Sie **Hardware** > **Fibre Channel** > **Resources** aus.
2. Wählen Sie **More Tasks** > **Ports** > **Disable** aus.
3. Wählen Sie im Dialogfeld „Disable Ports“ einen oder mehrere Ports aus der Liste aus und klicken Sie auf **Next**.
4. Das Bestätigungsdialogfeld können Sie bei der Deaktivierung des einfach den Port weiterhin oder können Sie außerdem auswählen, ein Failover alle Endpunkte an den Ports zu einem anderen Port.

Hinzufügen eines Endpunkts

Ein Endpunkt ist ein virtuelles Objekt, das einem zugrunde liegenden virtuellen Port zugeordnet ist. Im Nicht-NPIV-Modus (nicht verfügbar für HA-Konfiguration) ist nur ein einziger Endpunkt pro physischem Port zulässig und der Basisport wird verwendet, um diesen Endpunkt zur Fabric zu konfigurieren. Wenn NPIV aktiviert ist, sind mehrere Endpunkte pro physischem Port zulässig, jeder mit einem virtuellen Port (NPIV). Endpunkt-Failover/Failback ist aktiviert.

Hinweis

Der Nicht-NPIV-Modus ist nicht für HA-Konfigurationen verfügbar. NPIV ist standardmäßig aktiviert und kann nicht deaktiviert werden.

Hinweis

Im NPIV-Modus gilt für Endpunkte Folgendes:

- Sie haben eine primäre Systemadresse.
- Sie können 0 oder mehr sekundäre Systemadressen haben.
- Sie sind alle Kandidaten für Failover zu einer alternativen Systemadresse bei Ausfall eines Ports; Failover zu einem Grenzport wird jedoch nicht unterstützt.
- Es kann für Sie ein Failback zum primären Port durchgeführt werden, wenn der Port wieder online ist.

Hinweis

Bei Verwendung von NPIV wird empfohlen, dass Sie nur ein Protokoll (d. h. DD VTL Fibre Channel, DD Boost-over-Fibre Channel oder vDisk Fibre Channel) pro Endpunkt verwenden. Für Failover-Konfigurationen sollten sekundäre Endpunkte auch so konfiguriert werden, dass sie dasselbe Protokoll wie primäre verwenden.

Vorgehensweise

1. Wählen Sie**Hardware** > **Fibre Channel** > **Resources**.
2. Wählen Sie unter **Endpoints** die Option **Add** (Pluszeichen).
3. Geben Sie im Dialogfeld „Add Endpoint“ einen Namen für den Endpunkt ein (1 bis 128 Zeichen). Das Feld darf nicht leer sein oder das Wort „all“ oder eines der folgenden Zeichen enthalten: Sternchen (*), Fragezeichen (?), normale oder umgekehrte Schrägstriche (/, \) oder öffnende und schließende Klammern [(,)].
4. Wählen Sie für „Endpoint Status“ die Option „Enabled“ oder „Disabled“.
5. Wenn NPIV aktiviert ist, wählen Sie eine primäre Systemadresse aus der Drop-down-Liste. Die Adresse des primären Systems muss sich von allen sekundären Systemadressen unterscheiden.
6. Wenn NPIV aktiviert ist, aktivieren Sie für Failover zu sekundären Systemadressen das entsprechende Kontrollkästchen neben der sekundären Systemadresse.
7. Wählen Sie **OK** aus.

Konfigurieren eines Endpunkts

Nachdem Sie einen Endpunkt hinzugefügt haben, können Sie ihn über das Dialogfeld "Configure Endpoint" ändern.

Hinweis

Bei Verwendung von NPIV wird empfohlen, dass Sie nur ein Protokoll (d. h. DD VTL Fibre Channel, DD Boost-over-Fibre Channel oder vDisk Fibre Channel) pro Endpunkt verwenden. Für Failover-Konfigurationen sollten sekundäre Endpunkte auch so konfiguriert werden, dass sie dasselbe Protokoll wie primäre verwenden.

Vorgehensweise

1. Wählen Sie **Hardware** > **Fibre Channel** > **Resources**.
2. Wählen Sie unter **Endpoints** einen Endpunkt und anschließend **Modify** (Stift) aus.
3. Geben Sie im Dialogfeld „Configure Endpoint“ einen Namen für den Endpunkt ein (1 bis 128 Zeichen). Das Feld darf nicht leer sein oder das Wort „all“ oder eines der folgenden Zeichen enthalten: Sternchen (*), Fragezeichen (?), normale oder umgekehrte Schrägstriche (/, \) oder öffnende und schließende Klammern [(,)].
4. Wählen Sie für "Endpoint Status" die Option "Enabled" oder "Disabled".
5. Wählen Sie für "Primary system address" eine Option aus der Drop-down-Liste. Die Adresse des primären Systems muss sich von allen sekundären Systemadressen unterscheiden.
6. Aktivieren Sie für Failover zu sekundären Systemadressen das entsprechende Kontrollkästchen neben der sekundären Systemadresse.

7. Wählen Sie **OK** aus.

Ändern der Systemadresse eines Endpunkts

Sie können die aktive Systemadresse für einen SCSI-Zielendpunkt mithilfe der Befehlsoption `scsitarget endpoint modify` ändern. Dies ist nützlich, wenn der Endpunkt mit einer Systemadresse verknüpft ist, die nicht mehr existiert, z. B. nach einem Controllerupgrade oder wenn der Hostbusadapter eines Controller (Controller-HBA) verschoben wurde. Wenn die Systemadresse für einen Endpunkt geändert wird, werden alle Eigenschaften des Endpunkts, einschließlich WWPN und WWNN (World Wide Port Name und World Wide Node Name), sofern vorhanden, beibehalten und mit der neuen Systemadresse verwendet.

Im folgenden Beispiel wurde der Endpunkt „ep-1“ der Systemadresse „5a“ zugewiesen; diese Systemadresse ist jedoch nicht mehr gültig. Der Systemadresse „10a“ wurde ein neuer Controller-HBA hinzugefügt. Das SCSI-Zielsubsystem hat automatisch den neuen Endpunkt „ep-new“ für die neu erkannte Systemadresse erstellt. Da nur ein einziger Endpunkt mit einer bestimmten Systemadresse verknüpft werden kann, muss „ep-new“ gelöscht und „ep-1“ der Systemadresse „10a“ zugewiesen werden.

Hinweis

Es kann einige Zeit dauern, bis der geänderte Endpunkt online ist. Dies hängt von der SAN-Umgebung ab, da WWPN und WWNN auf eine andere Systemadresse verschoben wurden. Möglicherweise muss auch das SAN-Zoning gemäß der neuen Konfiguration aktualisiert werden.

Vorgehensweise

1. Zeigen Sie alle Endpunkte an, um die Endpunkte zu überprüfen, die geändert werden sollen:

   ```
   # scsitarget endpoint show list
   ```

2. Deaktivieren Sie alle Endpunkte:

   ```
   # scsitarget endpoint disable all
   ```

3. Löschen Sie die neuen, nicht benötigten Endpunkt „ep-new“:

   ```
   # scsitarget endpoint del ep-new
   ```

4. Ändern Sie den Endpunkt „ep-1“, den Sie verwenden möchten, indem Sie diesen der neuen Systemadresse „10a“ zuweisen:

   ```
   # scsitarget endpoint modify ep-1 system-address 10a
   ```

5. Aktivieren Sie alle Endpunkte:

   ```
   # scsitarget endpoint enable all
   ```

Aktivieren eines Endpunkts

Durch Aktivieren eines Endpunkts wird der Port nur aktiviert, wenn er aktuell deaktiviert ist. Das heißt, Sie befinden sich im Nicht-NPIV-Modus.

Vorgehensweise

1. Wählen Sie **Hardware** > **Fibre Channel** > **Physcal Resources** aus.
2. Wählen Sie **More Tasks** > **Endpoints** > **Enable** aus. Wenn bereits alle Endpunkte aktiviert sind, wird eine entsprechende Meldung angezeigt.

3. Klicken Sie im Dialogfeld „Enable Endpoints“ auf einen oder mehrere Endpunkte in der Liste und wählen Sie **Next** aus.
4. Wählen Sie nach der Bestätigung **Next** aus, um die Aufgabe abzuschließen.

Deaktivieren eines Endpunkts

Durch das Deaktivieren eines Endpunkts wird der zugeordnete Port nicht deaktiviert, es sei denn, alle Endpunkt, die den Port verwenden, werden deaktiviert. Das heißt, Sie befinden sich im Nicht-NPIV-Modus.

Vorgehensweise

1. Wählen Sie **Hardware** > **Fibre Channel** > **Resources** aus.
2. Wählen Sie **More Tasks** > **Endpoints** > **Disable** aus.
3. Wählen Sie im Dialogfeld „Disable Endpoints“ einen oder mehrere Endpunkte aus der Liste aus und klicken Sie auf **Next**. Wenn ein Endpunkt verwendet wird, wird eine Warnung angezeigt, dass eine Deaktivierung zu einer Systemunterbrechung führen könnte.
4. Wählen Sie **Next** aus, um die Aufgabe abzuschließen.

Löschen eines Endpunkts

Hiermit kann ein Endpunkt gelöscht werden, wenn die zugrunde liegende Hardware nicht mehr verfügbar ist. Wenn die zugrunde liegende Hardware noch vorhanden ist oder wieder verfügbar wird, wird jedoch automatisch ein neuer Endpunkt für die Hardware erkannt und basierend auf den Standardwerten konfiguriert.

Vorgehensweise

1. Wählen Sie **Hardware** > **Fibre Channel** > **Resources** aus.
2. Wählen Sie **More Tasks** > **Endpoints** > **Delete**.
3. Wählen Sie im Dialogfeld „Delete Endpoints“ einen oder mehrere Endpunkte aus der Liste aus und klicken Sie auf **Next**. Wenn ein Endpunkt verwendet wird, wird eine Warnung angezeigt, dass eine Löschung zu einer Systemunterbrechung führen könnte.
4. Wählen Sie **Next** aus, um die Aufgabe abzuschließen.

Hinzufügen eines Initiators

Fügen Sie Initiatoren hinzu, um mit dem System verbundene Backupclients bereitzustellen und Daten mithilfe des FC-Protokolls (Fibre Channel) zu lesen und zu schreiben. Ein bestimmter Initiator kann DD Boost über FC oder DD VTL unterstützen, aber nicht beides. Maximal 1024 Initiatoren können für ein DD-System konfiguriert werden.

Vorgehensweise

1. Wählen Sie **Hardware** > **Fibre Channel** > **Resources** aus.
2. Wählen Sie unter "Initiators" die Option "Add" (Pluszeichen).
3. Geben Sie im Dialogfeld "Add Initiator" den eindeutigen WWPN des Ports in dem angegebenen Format ein.
4. Geben Sie einen Namen für den Initiator ein.
5. Wählen Sie die Adressierungsmethode aus: **Auto** wird für die Standardadressierung verwendet und **VSA** (Volume Set Addressing) wird hauptsächlich für die Adressierung von virtuellen Bussen, Zielen und LUNs verwendet.

6. Wählen Sie **OK** aus.

CLI-Entsprechung

```
# scsitarget group add My_Group initiator My_Initiator
```

Ändern oder Löschen eines Initiators

Bevor Sie einen Initiator löschen können, muss dieser offline und mit keiner Gruppe verknüpft sein. Andernfalls erhalten Sie eine Fehlermeldung und der Initiator wird nicht gelöscht. Sie müssen alle Initiatoren in einer Zugriffsgruppe löschen, bevor Sie die Zugriffsgruppe löschen können. Wenn der Initiator sichtbar bleibt, kann dieser automatisch neu erkannt werden.

Vorgehensweise

1. Wählen Sie **Hardware** > **Fibre Channel** > **Resources** aus.
2. Wählen Sie unter „Initiators“ einen der Initiatoren aus. Wenn Sie ihn löschen möchten, wählen Sie das Löschsymbol (X) aus. Wenn Sie ihn ändern möchten, wählen Sie das Bearbeitungssymbol (Stift) aus, um das Dialogfeld „Modify Initiator“ anzuzeigen.
3. Ändern Sie den Namen und die Adressmethode des Initiators [**Auto** wird für die Standardadressierung verwendet, **VSA** (Volume Set Addressing) hauptsächlich für die Adressierung virtueller Busse, Ziele und LUNs.]
4. Wählen Sie **OK** aus.

Empfehlung zum Festlegen von Initiatoraliasnamen – nur CLI
Die Festlegung von Initiatoraliasnamen wird dringend empfohlen, um Verwechslungen und menschliche Fehler beim Konfigurationsprozess zu vermeiden.

```
# vtl initiator set alias NewAliasName wwpn 21:00:00:e0:8b:9d:0b:e8
# vtl initiator show
Initiator  Group    Status   WWNN                     WWPN                     Port
---------  -------  -------  -----------------------  -----------------------  ---
NewVTL     aussie1  Online   20:00:00:e0:8b:9d:0b:e8  21:00:00:e0:8b:9d:0b:e8  6a
                    Offline  20:00:00:e0:8b:9d:0b:e8  21:00:00:e0:8b:9d:0b:e8  6b

Initiator  Symbolic Port Name  Address Method
---------  ------------------  --------------
NewVTL                              auto
---------  ------------------  --------------
```

Festlegen einer festen Adresse (Loop-ID)

Bei einiger Backupsoftware ist es erforderlich, dass alle Private-Loop-Ziele über eine feste IP-Adresse (Loop-ID) verfügen, die nicht mit einem anderen Node in Konflikt steht. Der Bereich für eine Loop-ID liegt zwischen 0 und 125.

Vorgehensweise

1. Wählen Sie **Hardware** > **Fibre Channel** > **Resources**.
2. Wählen Sie **More Tasks** > **Set Loop ID**.
3. Geben Sie in das Dialogfeld „Set Loop ID“ die Loop-ID (zwischen 0 und 125) ein und klicken Sie auf **OK**.

Festlegen von Failover-Optionen

Sie können die Optionen für automatisches Failover und Failback festlegen, wenn NPIV aktiviert ist.

Hier das erwartete Verhalten für Fibre Channel-Port-Failover nach Anwendung:

- Es wird erwartet, dass der DD Boost-over-Fibre Channel-Vorgang ohne Benutzereingriff fortgesetzt wird.
- Der DD VTL Fibre Channel-Vorgang wird voraussichtlich beim Failover der DD VTL Fibre Channel-Endpunkte unterbrochen. Möglicherweise müssen Sie eine Erkennung (Betriebssystemerkennung und Konfiguration von DD VTL-Geräten) für die Initiatoren unter Verwendung des betroffenen Fibre-Channel-Endpunkts durchführen. Sie sollten davon ausgehen, aktive Backup-und Wiederherstellungsvorgänge erneut starten zu müssen.
- Der vDisk Fibre Channel-Vorgang wird voraussichtlich ohne Benutzereingriff bei einem Failover der Fibre Channel-Endpunkte fortgesetzt.

Automatisches Failback wird nicht garantiert, wenn alle Ports deaktiviert und dann später aktiviert werden (evtl. ausgelöst vom Administrator), da die Reihenfolge, in der Ports aktiviert werden, nicht festgelegt ist.

Vorgehensweise

1. Wählen Sie **Hardware** > **Fibre Channel** > **Resources** aus.
2. Wählen Sie **More Tasks** > **Set Failover Options**.
3. Geben Sie im Dialogfeld "Set Failover Options" die Failover- und Failback-Verzögerung (in Sekunden) an und ob das automatische Failback aktiviert werden soll. Wählen Sie **OK**.

Registerkarte „Access Groups“

Die Registerkarte **Hardware** > **Fibre Channel** > **Access Groups** bietet Informationen zu DD Boost- und DD VTL-Zugriffsgruppen. Durch Auswahl des Links zu *View DD Boost Groups* or *View VTL Groups* gelangen Sie zu den DD Boost- oder DD VTL-Seiten.

Tabelle 121 Zugriffsgruppen

Element	Beschreibung
Group Name	Name der Zugriffsgruppe.
Service	Service für diese Zugriffsgruppe: DD Boost oder DD VTL.
Endpoints	Endpunkte, die dieser Zugriffsgruppe zugeordnet sind.
Initiators	Initiatoren, die dieser Zugriffsgruppe zugeordnet sind.
Number of Devices	Anzahl der Geräte, die dieser Zugriffsgruppe zugeordnet sind.

Unterschiede beim Monitoring von FC-Links zwischen DD OS-Versionen

Unterschiedliche DD OS-Versionen verarbeiten das Monitoring von FC-Links (Fibre Channel) auf unterschiedliche Weise.

DD OS 5.3 und höher
Das Portmonitoring erkennt einen FC-Port beim Systemstart und gibt eine Warnmeldung aus, wenn der Port aktiviert und offline ist. Zum Entfernen der Warnmeldung deaktivieren Sie einen nicht genutzten Port mithilfe der `scsitarget port`-Befehle.

DD OS 5.1 bis 5.3
Wenn ein Port offline ist, werden Sie mit einer Warnmeldung benachrichtigt, dass die Verbindung unterbrochen wurde. Diese Warnmeldung ist gemanagt, was bedeutet, dass sie aktiv bleibt, bis sie gelöscht wird. Diese Warnmeldung wird angezeigt, wenn der DD VTL-FC-Port online oder deaktiviert ist. Wenn der Port nicht verwendet wird, deaktivieren Sie ihn, sofern er nicht überwacht werden muss.

DD OS 5.0 bis 5.1
Wenn ein Port offline ist, werden Sie mit einer Warnmeldung benachrichtigt, dass die Verbindung unterbrochen wurde. Die Warnmeldung ist nicht gemanagt, was bedeutet, dass sie nicht aktiv bleibt und nicht in der Liste der aktuellen Warnmeldungen angezeigt wird. Wenn ein Port online ist, werden Sie mit einer Warnmeldung benachrichtigt, dass die Verbindung aktiv ist. Wenn der Port nicht verwendet wird, deaktivieren Sie ihn, sofern er nicht überwacht werden muss.

DD OS 4.9 bis 5.0
Ein FC-Port muss in einer DD VTL-Gruppe enthalten sein, um überwacht werden zu können.

KAPITEL 14

Arbeiten mit DD Boost

Dieses Kapitel enthält die folgenden Themen:

Informationen über Data Domain Boost

Data Domain Boost (DD Boost) bietet eine erweiterte Integration in Backup- und Unternehmensanwendungen für mehr Performance und Anwenderfreundlichkeit. DD Boost verteilt Schritte des Deduplizierungsprozesses auf den Backupserver oder Anwendungsclients und ermöglicht so eine clientseitige Deduplizierung für schnellere und effizientere Backup- und Recovery-Funktionen.

DD Boost ist ein optionales Produkt, für das eine separate Lizenz erforderlich ist, damit es auf dem Data Domain-System betrieben werden kann. Sie können einen DD Boost-Softwarelizenzschlüssel für ein Data Domain-System direkt von Data Domain erwerben.

Hinweis

Eine spezielle Lizenz, BLOCK-SERVICES-PROTECTPOINT, ist verfügbar, um Clients, die ProtectPoint-Blockservices verwenden, DD Boost-Funktionalität ohne DD Boost-Lizenz bereitzustellen. Wenn DD Boost nur für ProtectPoint-Clients aktiviert ist, das heißt, wenn nur die BLOCK-SERVICES-PROTECTPOINT-Lizenz installiert ist, gibt der Lizenzstatus an, dass DD Boost nur für ProtectPoint aktiviert ist.

DD Boost umfasst zwei Komponenten: eine Komponente, die auf dem Backupserver ausgeführt wird, und eine Komponente, die auf dem Data Domain-System ausgeführt wird.

- Im Kontext der NetWorker-Backupanwendung, der Avamar-Backupanwendung und anderen DDBoost-Partnerbackupanwendungen wird die Komponente, die auf dem Backupserver (DD Boost-Bibliotheken) ausgeführt wird, in die jeweilige Backupanwendung integriert.
- Im Kontext von Symantec-Backupanwendungen (NetBackup und Backup Exec) sowie dem Oracle RMAN-Plug-in müssen Sie eine entsprechende Version des DD Boost-Plug-ins herunterladen, die auf jedem Medienserver installiert wird. Das DD Boost-Plug-in umfasst die DD Boost-Bibliotheken für die Integration in den DD Boost-Server, der auf dem Data Domain-System ausgeführt wird.

Die Backupanwendung (z. B. Avamar, NetWorker, NetBackup oder Backup Exec) legt Policies fest, die steuern, wann Backups und Duplizierungen stattfinden. Das Management von Backups, Duplizierung und Wiederherstellungen erfolgt über eine einzige Konsole und der Administrator kann alle Funktionen von DD Boost, einschließlich der WAN-effizienten Replicator-Software, nutzen. Die Anwendung managt alle Dateien (Datensammlungen) im Katalog, einschließlich der vom Data Domain-System erstellten Dateien.

Im Data Domain-System werden Speichereinheiten, die Sie erstellen, für Backupanwendungen bereitgestellt, die das DD Boost-Protokoll verwenden. Bei Symantec-Anwendungen werden Speichereinheiten als Laufwerkpools angezeigt. Bei NetWorker werden Speichereinheiten als logische Speichereinheiten (LSUs) angezeigt. Eine Speichereinheit ist ein MTree und unterstützt deshalb MTree-Quota-Einstellungen. (Erstellen Sie keinen MTree anstelle einer Speichereinheit.)

Dieses Kapitel enthält keine Installationsanweisungen, diese finden Sie in der Dokumentation für das Produkt, das Sie installieren möchten. Informationen zum Einrichten von DD Boost mit Symantec-Backupanwendungen (NetBackup und Backup Exec) finden Sie beispielsweise im *Data Domain Boost for OpenStorage Administration Guide*. Weitere Informationen zum Einrichten von DD Boost mit einer anderen Anwendung finden Sie in der anwendungsspezifischen Dokumentation.

Zusätzliche Informationen zum Konfigurieren und Managen von DD Boost auf dem Data Domain-System finden Sie auch im *Data Domain Boost for OpenStorage Administration Guide* (für NetBackup und Backup Exec) und im *Data Domain Boost for Partner Integration Administration Guide* (für andere Backupanwendungen).

Managen von DD Boost mit DD System Manager

Rufen Sie die Ansicht „DD Boost“ in DD System Manager auf.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** Vergewissern Sie sich, dass das Dateisystem aktiviert ist und ausgeführt wird, indem Sie den Status prüfen.
2. Wählen Sie **Protocols** > **DD Boost**.

   Wenn Sie zu der DD Boost-Seite ohne Lizenz gehen, wird als Status angezeigt, dass DD Boost nicht lizenziert ist. Klicken Sie auf **Add License** und geben Sie eine gültige Lizenz in das Dialogfeld „Add License Key“ ein.

   Hinweis

   Eine spezielle Lizenz, BLOCK-SERVICES-PROTECTPOINT, ist verfügbar, um Clients, die ProtectPoint-Blockservices verwenden, DD Boost-Funktionalität ohne DD Boost-Lizenz bereitzustellen. Wenn DD Boost nur für ProtectPoint-Clients aktiviert ist, das heißt, wenn nur die BLOCK-SERVICES-PROTECTPOINT-Lizenz installiert ist, gibt der Lizenzstatus an, dass DD Boost nur für ProtectPoint aktiviert ist.

   Verwenden Sie die DD Boost-Registerkarten „Settings“, „Active Connections“, „IP Network“, „Fibre Channel“ und „Storage Unit“ für das Management von DD Boost.

Festlegen von DD Boost-Benutzernamen

Ein DD Boost-Benutzer ist auch ein DD OS-Benutzer. Legen Sie einen DD Boost-Benutzernamen fest, indem Sie einen vorhandenen DD OS-Benutzernamen auswählen oder einen neuen DD OS-Benutzernamen erstellen und diesen Namen zu einem DD Boost-Benutzer machen.

Backupanwendungen nutzen den DD Boost-Benutzernamen und das Passwort für die Verbindung mit dem Data Domain-System. Sie müssen diese Anmeldedaten auf jedem Backupserver konfigurieren, der eine Verbindung mit diesem System herstellt. Das Data Domain-System unterstützt mehrere DD Boost-Benutzer. Vollständige Informationen zum Einrichten von DD Boost mit Symantec NetBackup und Backup Exec finden Sie im *Data Domain Boost for OpenStorage Administration Guide*. Informationen zum Einrichten von DD Boost mit anderen Anwendungen finden Sie im *Data Domain Boost for Partner Integration Administration Guide* und in der anwendungsspezifischen Dokumentation.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost**.
2. Wählen Sie **Add** (+) über der Liste "Users with DD Boost Access" aus.

   Das Dialogfeld „Add User“ wird angezeigt.

3. Um einen vorhandenen Benutzer auszuwählen, markieren Sie den Benutzernamen in der Drop-down-Liste.

Es empfiehlt sich, dass Sie einen Benutzernamen auswählen, dessen Managementberechtigungen auf *none* festgelegt wurden.

4. Um einen neuen Benutzer zu erstellen und auszuwählen, wählen Sie **Create a new Local User** aus und gehen Sie folgendermaßen vor:
   a. Geben Sie den neuen Benutzernamen in das Feld „User“ ein.

      Der Benutzer muss in der Backupanwendung konfiguriert werden, um eine Verbindung zum Data Domain-System herstellen zu können.

   b. Geben Sie das Passwort zweimal in die entsprechenden Felder ein.
5. Klicken Sie auf **Hinzufügen**.

Ändern der DD Boost-Benutzerpasswörter

Ändern Sie ein DD Boost-Benutzerpasswort.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **Settings**.
2. Wählen Sie einen Benutzer aus der Liste „Users with DD Boost Access“ aus.
3. Klicken Sie auf die Schaltfläche **Edit** (Bleistiftsymbol) über der DD Boost-Benutzerliste.

   Das Dialogfeld „Change Password“ wird angezeigt.
4. Geben Sie das Passwort zweimal in die entsprechenden Felder ein.
5. Klicken Sie auf **Change**.

Entfernen eines DD Boost-Benutzernamens

Entfernen Sie einen Benutzer in der DD Boost-Zugriffsliste.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **Settings**.
2. Wählen Sie den zu entfernenden Benutzer in der Liste „Users with DD Boost Access“ aus.
3. Klicken Sie über der DD Boost-Benutzerliste auf **Remove** (X).

   Das Dialogfeld „Remove User“ wird angezeigt.
4. Klicken Sie auf **Remove**.

   Nach dem Entfernen bleibt der Benutzer in der DD OS-Zugriffsliste.

Aktivieren von DD Boost

Verwenden Sie die Registerkarte „DD Boost“, um DD Boost zu aktivieren und einen DD Boost-Benutzer auszuwählen oder hinzuzufügen.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **Settings**.
2. Klicken Sie im Bereich „DD Boost Status“ auf **Enable**.

   Das Dialogfeld „Enable DD Boost“ wird angezeigt.

3. Wählen Sie einen vorhandenen Benutzernamen aus dem Menü aus oder fügen Sie einen neuen Benutzer hinzu, indem Sie den Namen, das Passwort und die Rolle angeben.

Konfigurieren von Kerberos

Sie können Kerberos mit der Registerkarte „DD Boost Settings“ konfigurieren.

Vorgehensweise

1. Wählen Sie **Protocols > DD Boost > Settings** aus.
2. Klicken Sie im Bereich „Kerberos Mode status“ auf **Configure**.

   Die Registerkarte „Authentication“ unter **Administration > Access** wird angezeigt.

   Hinweis

   Außerdem können Sie Kerberos aktivieren, indem Sie direkt zu „Authentication“ unter **Administration > Access** im System Manager navigieren.
3. Klicken Sie unter „Active Directory/Kerberos Authentication“ auf **Configure**.

   Das Dialogfeld „Active Directory/Kerberos Authentication“ wird angezeigt. Wählen Sie den Typ des Kerberos Key Distribution Center (KDC) aus, den Sie verwenden möchten:

   - **Disabled**
     Wenn Sie **Disabled** auswählen, verwenden NFS-Clients die Kerberos-Authentifizierung nicht. CIFS-Clients verwenden die Arbeitsgruppenauthentifizierung.
   - **Windows/Active Directory**
     Geben Sie den Bereichsnamen, Benutzernamen und das Passwort für die Active Directory-Authentifizierung ein.
   - **Unix**
     a. Geben Sie den Bereichsnamen, die IP-Adresse/Hostnamen von einem bis drei KDC-Servern an.
     b. Laden Sie die Keytab-Datei aus einem der KDC-Server hoch.

Deaktivieren von DD Boost

Durch die Deaktivierung von DD Boost werden alle aktiven Verbindungen mit dem Backupserver getrennt. Wenn Sie DD Boost deaktivieren oder löschen, wird der DD Boost FC-Service ebenfalls deaktiviert.

Bevor Sie beginnen

Vergewissern Sie sich vor der Deaktivierung, dass keine Jobs mehr über Ihre Backupanwendung ausgeführt werden.

Hinweis

Die Dateireplikation, die von DD Boost zwischen zwei Data Domain-Wiederherstellungen gestartet wird, wird nicht abgebrochen.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **Settings** aus.

2. Klicken Sie im Bereich „DD Boost Status“ auf **Disable**.
3. Klicken Sie im Bestätigungsdialogfeld „Disable DD Boost“ auf **OK**.

Anzeigen von DD Boost-Speichereinheiten

Rufen Sie die Registerkarte „Storage Units“ auf, um DD Boost-Speichereinheiten anzuzeigen und zu managen.

Die Registerkarte „DD Boost Storage Unit“:

- Listet die Speichereinheiten auf und stellt die folgenden Informationen für jede Speichereinheit bereit:

Tabelle 122 Informationen zur Speichereinheit

Element	Beschreibung
Storage Unit	Der Name der Speichereinheit.
Benutzer	Der DD Boost-Benutzer, dem die Speichereinheit gehört.
Quota Hard Limit	Der Prozentsatz des verwendeten festen Quotas.
Last 24 hr Pre-Comp	Die Menge an Rohdaten von der Backupanwendung, die in den letzten 24 Stunden geschrieben wurde.
Last 24 hr Post-Comp	Die Menge an Speicher, der in den letzten 24 Stunden nach der Komprimierung verwendet wurde.
Last 24 hr Comp Ratio	Das Komprimierungsverhältnis für die letzten 24 Stunden.
Weekly Avg Post-Comp	Die durchschnittliche Menge des verwendeten komprimierten Speichers in den letzten fünf Wochen.
Last Week Post-Comp	Die durchschnittliche Menge des verwendeten komprimierten Speichers in den letzten sieben Tagen.
Weekly Avg Comp Ratio	Das durchschnittliche Komprimierungsverhältnis für die letzten fünf Wochen.
Last Week Comp Ratio	Das durchschnittliche Komprimierungsverhältnis für die letzten sieben Tage.

- Ermöglicht Ihnen das Erstellen, Ändern und Löschen von Speichereinheiten.
- Zeigt vier zugehörige Registerkarten für eine in der Liste ausgewählte Speichereinheit an: Storage Unit, Space Usage, Daily Written und Data Movement.

  Hinweis

  Die Registerkarte „Data Movement“ ist nur verfügbar, wenn die optionale Data Domain Extended Retention (ehemals DD Archiver)-Lizenz installiert ist.

- Führt Sie zu **Replication** > **On-Demand** > **File Replication**, wenn Sie auf den Link **View DD Boost Replications** klicken.

  Hinweis

  Eine DD Replicator-Lizenz ist erforderlich, damit DD Boost andere Registerkarten als die Registerkarte „File Replication“ anzeigt.

Erstellen einer Speichereinheit

Sie müssen mindestens eine Speichereinheit auf dem Data Domain-System erstellen und dieser Speichereinheit einen DD Boost-Benutzer zuweisen. Verwenden Sie zum Erstellen einer Speichereinheit die Registerkarte „Storage Units“.

Jede Speichereinheit ist ein Unterverzeichnis der obersten Ebene des Verzeichnisses `/data/col1`. Es gibt keine Hierarchie unter Speichereinheiten.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **Storage Units**.
2. Klicken Sie auf **Create** (+).

   Das Dialogfeld „Create Storage Unit“ wird angezeigt.

3. Geben Sie den Namen für die Speichereinheit in das Feld „Name“ ein.

   Der Name für jede Speichereinheit muss eindeutig sein. Namen für Speichereinheiten können bis zu 50 Zeichen enthalten. Die folgenden Zeichen sind zulässig:

   - Große und kleine Buchstaben: A-Z, a-z
   - Ziffern: 0-9
   - eingebettetes Leerzeichen

     Hinweis

     Der Name der Speichereinheit muss in doppelte Anführungszeichen (") gesetzt werden, wenn ein eingebettes Leerzeichen im Namen vorhanden ist.

   - Komma (,)
   - Punkt (.), solange er nicht vor dem Namen steht
   - Ausrufezeichen (!)
   - Doppelkreuz (#)
   - Dollarzeichen ($)
   - Prozentvorzeichen (%)
   - Pluszeichen (+)
   - At-Zeichen (@)
   - Gleichheitszeichen (=)
   - Kaufmännisches Und (&)
   - Semikolon (;)
   - Klammern [(und)]
   - Eckige Klammern ([und])
   - Geschweifte Klammern ({und})
   - Einschaltungszeichen (^)
   - Tilde (~)
   - Apostroph (gerades einzelnes Anführungszeichen)
   - Abgeschrägtes einzelnes Anführungszeichen (')
   - Minuszeichen (-)

- Unterstrich (_)

4. Um einen vorhandenen Benutzernamen auszuwählen, der auf diese Speichereinheit zugreifen kann, wählen Sie den Benutzernamen in der Drop-down-Liste aus.

   Wählen Sie einen Benutzernamen aus, dessen Managementberechtigungen auf *none* festgelegt wurden (wenn möglich).

5. Wählen Sie zum Erstellen und Auswählen eines neuen Benutzernamens, der Zugriff auf diese Speichereinheit erhält, **Create a new Local User** aus und gehen Sie dann wie folgt vor:

   a. Geben Sie den neuen Benutzernamen in das Feld „User“ ein.

      Der Benutzer muss in der Backupanwendung konfiguriert werden, um eine Verbindung zum Data Domain-System herstellen zu können.

   b. Geben Sie das Passwort zweimal in die entsprechenden Felder ein.

6. Um Speicherplatzbeschränkungen festzulegen, mit denen eine übermäßige Speicherplatznutzung durch eine Speichereinheit vermieden wird, geben Sie entweder ein weiches oder ein hartes Quota-Limit oder beides ein. Bei einem weichen Limit wird eine Warnmeldung gesendet, wenn die Größe der Speichereinheit das Limit überschreitet, es können jedoch weiterhin Daten auf diese Einheit geschrieben werden. Wenn das harte Limit erreicht wird, können keine Daten auf die Speichereinheit geschrieben werden.

   Hinweis

   Quota-Limits sind vorkomprimierte Werte. Um Quota-Limits festzulegen, wählen Sie **Set to Specific Value** aus und geben Sie den Wert ein. Wählen Sie die Maßeinheit aus: MiB, GiB, TiB oder PiB.

   Hinweis

   Wenn variable und feste Grenzwerte festgelegt werden, kann die variable Grenze einer Quota die feste Grenze der Quota nicht übersteigen.

7. Klicken Sie auf **Create**.
8. Wiederholen Sie die obigen Schritte für jedes Data Domain Boost-aktivierte System.

Anzeigen von Speichereinheitinformationen

Auf der Registerkarte „DD Boost Storage Units“ können Sie eine Speichereinheit auswählen und auf die Registerkarten „Storage Unit“, „Space Usage“, „Daily Written“ und „Data Movement“ für die ausgewählte Speichereinheit zugreifen.

Registerkarte „Storage Unit“
Die Registerkarte „Storage Unit“ zeigt detaillierte Informationen für eine ausgewählte Speichereinheit in den Bereichen „Summary“ und „Quota“ an. Im Bereich „Snapshot“ werden Snapshots angezeigt. Sie können neue Snapshots und Planungen erstellen und es steht eine Link zur Registerkarte **Data Management** > **Snapshot** zur Verfügung.

- Im Bereich „Summary“ werden zusammengefasste Informationen für die ausgewählte Speichereinheit angezeigt.

Tabelle 123 Bereich „Summary“

Element „Summary“	Beschreibung
Total Files	Die Gesamtanzahl von Dateien auf der Speichereinheit. Um Komprimierungsdetails anzuzeigen, die Sie in eine Protokolldatei herunterladen können, klicken Sie auf den Link „Download Compression Details“. Dieser Vorgang kann mehrere Minuten in Anspruch nehmen. Nach Abschluss des Vorgangs klicken Sie auf „Download“.
Full Path	`/data/col1/filename`
Status	R: Lesen; W: Schreiben; Q: Quota definiert
Pre-Comp Used	Die Menge des vorkomprimierten Speichers, der bereits verwendet wird.

- Im Bereich „Quota“ werden Quota-Informationen für die ausgewählte Speichereinheit angezeigt.

  Tabelle 124 Bereich „Quota“

Element „Quota“	Beschreibung
Quota-Durchsetzung	Aktiviert oder deaktiviert. Wenn Sie auf „Quota“ klicken, gelangen Sie zur Registerkarte **Data Management** > **Quota**, in der Sie Quotas konfigurieren können.
Pre-Comp Soft Limit	Der aktuelle Wert der variablen Quotas für die Speichereinheit.
Pre-Comp Hard Limit	Der aktuelle Wert der festen Quotas für die Speichereinheit.
Quota Summary	Der Prozentsatz des verwendeten festen Grenzwerts.

  So ändern Sie die auf der Registerkarte angezeigten weichen und harten Limits vor der Komprimierung:

  1. Klicken Sie im Bereich „Quota“ auf die Schaltfläche **Configure**.
  2. Geben Sie im Dialogfeld „Configure Quota“ Werte für harte und weiche Quotas ein und wählen Sie die Maßeinheit aus: MiB, GiB, TiB oder PiB. Klicken Sie auf **OK**.

- Snapshots
  Im Bereich „Snapshots“ werden Informationen über die Snapshots der Speichereinheit angezeigt.

  Tabelle 125 Bereich „Snapshots“

Element	Beschreibung
Total Snapshots	Die Gesamtzahl der Snapshots, die für diesen MTree erstellt wurden. Insgesamt können für jeden MTree 750 Snapshots erstellt werden.
Expired	Die Anzahl der Snapshots in diesem MTree, die zur Löschung markiert wurden, jedoch noch nicht mithilfe eines Bereinigungsvorgangs entfernt wurden.
Unexpired	Die Anzahl der Snapshots in diesem MTree, die nicht zur Löschung markiert wurden.

Tabelle 125 Bereich „Snapshots“ (Fortsetzung)

Element	Beschreibung
Oldest Snapshot	Das Datum des ältesten Snapshot für diesen MTree.
Newest Snapshot	Das Datum des neuesten Snapshot für diesen MTree.
Next Scheduled	Das Datum des nächsten geplanten Snapshot.
Assigned Snapshot Schedules	Der Name der Snapshot-Planung, die diesem MTree zugewiesen wurde.

Im Bereich „Snapshots“ können Sie die folgenden Aufgaben ausführen:

- Weisen Sie eine Snapshot-Planung zu einer ausgewählten Speichereinheit zu: Klicken Sie auf **Assign Snapshot Schedules**. Aktivieren Sie das Kontrollkästchen der Planung, klicken Sie auf **OK** und dann auf **Close**.
- Erstellen Sie eine neue Planung: Klicken Sie auf **Assign Snapshot Schedules**. Geben Sie einen Namen für die neue Planung ein.

  Hinweis

  Der Name des Snapshot kann nur aus Buchstaben, Ziffern, `_`, `-`, `%d` (numerischer Tag des Monats: 01 bis 31), `%a` (abgekürzter Wochentagsname), `%m` (numerischer Monat des Jahres: 01 bis 12), `%b` (abgekürzter Monatsname), `%y` (Jahr, zweistellig), `%Y` (Jahr, vierstellig), `%H` (Stunde: 00 bis 23) und `%M` (Minute: 00 bis 59) bestehen, nach dem Muster im Dialogfeld. Geben Sie das neue Muster ein und klicken Sie auf **Validate Pattern & Update Sample**. Klicken Sie auf **Weiter**.

  – Wählen Sie aus, wann die Planung ausgeführt werden soll: wöchentlich, täglich (oder an ausgewählten Tagen), monatlich an bestimmten Tagen, die Sie auswählen, indem Sie auf dieses Datum im Kalender klicken, oder am letzten Tag des Monats. Klicken Sie auf **Weiter**.

  – Geben Sie die Tageszeiten an, an denen die Planung ausgeführt werden soll: Wählen Sie entweder „At Specific Times“ oder „In Intervals“ aus. Wenn Sie einen bestimmten Zeitpunkt auswählen, wählen Sie den Zeitpunkt aus der Liste aus. Klicken Sie auf „Add“ (**+**), um eine Zeit (24-Stunden-Format) hinzuzufügen. Für die Intervalle wählen Sie „In Intervals“ aus und wählen Sie Start- und Endzeiten und die Häufigkeit („Every“), z. B. alle acht Stunden. Klicken Sie auf **Next**.

  – Geben Sie die Aufbewahrungsfrist für die Snapshots in Tagen, Monaten oder Jahren an. Klicken Sie auf **Next**.

  – Überprüfen Sie die Zusammenfassung Ihrer Konfiguration. Klicken Sie auf **Back**, um Werte zu bearbeiten. Klicken Sie auf **Finish**, um die Planung zu erstellen.

- Durch Klicken auf den Link „Snapshots“ gelangen Sie zur Registerkarte **Data Management** > **Snapshots**.

Registerkarte „Space Usage“

Das Diagramm auf der Registerkarte „Space Usage“ zeigt eine visuelle Darstellung der Datennutzung für die Speichereinheit im Verlauf der Zeit an.

- Klicken Sie auf einen Punkt auf der Linie des Diagramms, um ein Feld mit den Daten für diesen Punkt anzuzeigen.

- Klicken Sie auf **Print** (unten im Diagramm), um das Standarddruckdialogfeld anzuzeigen.
- Klicken Sie auf **Show in new window**, um das Diagramm in einem neuen Browserfenster anzuzeigen.

Es gibt zwei Typen von Diagrammdaten: „Logical Space Used (Pre-Compression)“ und „Physical Capacity Used (Post-Compression)“.

Registerkarte „Daily Written“
Die Ansicht „Daily Written“ enthält ein Diagramm, das die täglich auf das System geschriebenen Daten über einen Zeitraum von 7 bis 120 Tagen visuell darstellt. Die über einen bestimmten Zeitraum dargestellten Datenmengen beziehen sich auf vor- und nachkomprimierte Daten.

Registerkarte „Data Movement“
Eine Grafik im gleichen Format wie die Grafik „Daily Written“, die den Speicherplatz anzeigt, der in den Speicherbereich „DD Extended Retention“ verschoben wurde (wenn die DD Extended Retention-Lizenz aktiviert ist).

Ändern einer Speichereinheit

Verwenden Sie die Registerkarte „Modify Storage Unit“, um eine Speichereinheit umzubenennen, einen anderen vorhandenen Benutzer auszuwählen, einen neuen Benutzer zu erstellen und auszuwählen und Quota-Einstellungen zu bearbeiten.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **Storage Units**.
2. Wählen Sie aus der Liste „Storage Unit“ die Speichereinheit aus, die Sie ändern möchten.
3. Klicken Sie auf das Bleistiftsymbol.

   Das Dialogfeld „Modify Storage Unit“ wird angezeigt.

4. Um die Speichereinheit umzubenennen, bearbeiten Sie den Text im Feld **Name**.
5. Um einen anderen vorhandenen Benutzer auszuwählen, wählen Sie den Benutzernamen aus der Drop-down-Liste aus.

   Wählen Sie einen Benutzernamen aus, dessen Managementberechtigungen auf *none* festgelegt wurden (wenn möglich).

6. Um einen neuen Benutzer zu erstellen und auszuwählen, wählen Sie **Create a new Local User** aus und gehen Sie folgendermaßen vor:

   a. Geben Sie den neuen Benutzernamen in das Feld „User“ ein.

      Der Benutzer muss in der Backupanwendung konfiguriert werden, um eine Verbindung zum Data Domain-System herstellen zu können.

   b. Geben Sie das Passwort zweimal in die entsprechenden Felder ein.

7. Bearbeiten Sie die Quota-Einstellungen nach Bedarf.

   Um Speicherplatzbeschränkungen festzulegen, mit denen eine übermäßige Speicherplatznutzung durch eine Speichereinheit vermieden wird, geben Sie entweder ein weiches oder ein hartes Quota-Limit oder beides ein. Bei einem weichen Limit wird eine Warnmeldung gesendet, wenn die Größe der Speichereinheit das Limit überschreitet, es können jedoch weiterhin Daten auf diese Einheit geschrieben werden. Wenn das harte Limit erreicht wird, können keine Daten auf die Speichereinheit geschrieben werden.

Hinweis

Quota-Limits sind vorkomprimierte Werte. Um Quota-Limits festzulegen, wählen Sie **Set to Specific Value** aus und geben Sie den Wert ein. Wählen Sie die Maßeinheit aus: MiB, GiB, TiB oder PiB.

Hinweis

Wenn variable und feste Grenzwerte festgelegt werden, kann die variable Grenze einer Quota die feste Grenze der Quota nicht übersteigen.

8. Klicken Sie auf **Bearbeiten**.

Umbenennen einer DD Boost-Speichereinheit

Verwenden Sie zum Umbenennen einer Speichereinheit das Dialogfeld „Modify Storage Unit“.

Beim Umbenennen einer Speichereinheit wird der Name der Speichereinheit geändert. Folgende Eigenschaften bleiben jedoch erhalten:

- Eigentum des Benutzernamens
- Konfiguration des Streamlimits
- Konfiguration der Kapazitäts-Quota und gemeldete physische Größe
- AIR-Zuordnung auf dem lokalen Data Domain-System

Vorgehensweise

1. Gehen Sie zu **Protocols** > **DD Boost** > **Storage Units**.
2. Wählen Sie in der Liste „Storage Unit“ die Speichereinheit aus, die Sie umbenennen möchten.
3. Klicken Sie auf das Bleistiftsymbol.

   Das Dialogfeld „Modify Storage Unit“ wird angezeigt.

4. Bearbeiten Sie den Text im Feld **Name**.
5. Klicken Sie auf **Bearbeiten**.

Löschen einer Speichergruppe

Verwenden Sie die Registerkarte „Storage Units“, um eine Speichereinheit im Data Domain-System zu löschen. Beim Löschen einer Speichereinheit wird die Speichereinheit mit allen in der Speichereinheit enthaltenen Images im Data Domain-System entfernt.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **Storage Units**.
2. Wählen Sie die Speichereinheit aus, die aus der Liste gelöscht werden soll.
3. Klicken Sie auf **Delete** (X).
4. Klicken Sie auf **OK**.

Ergebnisse

Die Speichereinheit wird aus Ihrem Data Domain-System entfernt. Sie müssen die zugehörigen Katalogeinträge der Backupanwendung manuell löschen.

Wiederherstellen einer DD Boost-Speichereinheit

Verwenden Sie zum Wiederherstellen einer Speichereinheit die Registerkarte „Storage Units“.

Beim Wiederherstellen einer Speichereinheit wird eine zuvor gelöschte Speichereinheit einschließlich der folgenden Eigenschaften wiederhergestellt:

- Eigentum des Benutzernamens
- Konfiguration des Streamlimits
- Konfiguration der Kapazitäts-Quota und gemeldete physische Größe
- AIR-Zuordnung auf dem lokalen Data Domain-System

Hinweis

Gelöschte Speichereinheiten sind bis zur nächsten Ausführung des Befehls `filesys clean` verfügbar.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **Storage Units** > **More Tasks** > **Undelete Storage Unit...**.
2. Wählen Sie im Dialogfeld „Undelete Storage Units“ die Speichereinheiten aus, die Sie wiederherstellen möchten.
3. Klicken Sie auf **OK**.

Auswählen von DD Boost-Optionen

Verwenden Sie das Dialogfeld „DD Boost Options“, um Einstellungen für die verteilte Segmentverarbeitung, virtuelle synthetische Backups, die Optimierung bei niedriger Bandbreite für die Dateireplikation, die Verschlüsselung für die Dateireplikation und die Netzwerkeinstellung für die Dateireplikation (IPv4 oder IPv6) festzulegen.

Vorgehensweise

1. Um die DD Boost-Optionseinstellungen anzuzeigen, wählen Sie **Protocols** > **DD Boost** > **Settings** > **Advanced Options**.
2. Um die Einstellungen zu ändern, wählen Sie **More Tasks** > **Set Options**.

   Das Dialogfeld „DD Boost Options“ wird angezeigt.

3. Wählen Sie Optionen aus, die aktiviert werden sollen.
4. Heben Sie die Auswahl von Optionen auf, die deaktiviert werden sollen.

   Um eine Option für „File Replication Network Preference“ rückgängig zu machen, wählen Sie die andere Option aus.

5. Stellen Sie die DD Boost-Sicherheitsoptionen ein.

   a. Wählen Sie den **Authentication Mode** aus:

   - None
   - Two-way

- Two-way Password

b. Wählen Sie die **Encryption Strength** aus:

- None
- Medium
- High

Das Data Domain-System vergleicht den globalen Authentifizierungsmodus und die Verschlüsselungsstärke mit dem Authentifizierungsmodus und der Verschlüsselungsstärke pro Client, um den effektiven Authentifizierungsmodus und die effektive Verschlüsselungsstärke zu berechnen. Das System verwendet nicht den höchsten Authentifizierungsmodus aus einem Eintrag und die höchsten Verschlüsselungseinstellungen aus einem anderen Eintrag. Der effektive Authentifizierungsmodus und die effektive Verschlüsselungsstärke stammen aus einem einzelnen Eintrag, der den höchsten Authentifizierungsmodus bereitstellt.

6. Klicken Sie auf **OK**.

Hinweis

Sie können auch verteilte Segmentverarbeitung über die `ddboost option`-Befehle managen, die im *Data Domain Operating System Command Reference Guide* detailliert beschrieben werden.

Verteilte Segmentverarbeitung

Die verteilte Segmentverarbeitung steigert den Backupdurchsatz in nahezu allen Fällen durch Eliminierung doppelter Datenübertragungen zwischen dem Medienserver und dem Data Domain-System.

Sie können auch verteilte Segmentverarbeitung über die `ddboost option`-Befehle managen, die im *Data Domain Operating System Command Reference Guide* detailliert beschrieben werden.

Hinweis

Die verteilte Segmentverarbeitung ist standardmäßig mit Data Domain Extended Retention-Konfigurationen (ehemals Data Domain Archiver) aktiviert und kann nicht deaktiviert werden.

Virtuelle synthetische Backups

Ein virtuelles synthetisches komplettes Backup ist eine Kombination aus dem letzten kompletten (synthetischen oder kompletten) Backup und allen nachfolgenden inkrementellen Backups. Virtuelle synthetische Backups sind standardmäßig aktiviert.

Optimierung bei niedriger Bandbreite

Wenn Sie die Dateireplikation über ein Netzwerk mit niedriger Bandbreite (WAN) nutzen, können Sie die Replikation beschleunigen, indem Sie die Optimierung bei niedriger Bandbreite verwenden. Diese Funktion stellt eine zusätzliche Komprimierung während der Datenübertragung bereit. Die Komprimierung bei niedriger Bandbreite ist für Data Domain-Systeme mit installierter Replikationslizenz verfügbar.

Die Optimierung bei niedriger Bandbreite, die standardmäßig deaktiviert ist, ist auf die Verwendung in Netzwerken mit weniger als 6 Mbit/s aggregierter Bandbreite

ausgelegt. Verwenden Sie diese Option nicht, wenn eine maximale Schreibperformance für das Dateisystem erforderlich ist.

Hinweis

Sie können die Optimierung bei niedriger Bandbreite auch über die `ddboost file-replication` -Befehle managen, die ausführlich im *Data Domain Operating System Command Reference Guide* beschrieben sind.

Verschlüsselung der Dateireplikation

Sie können den Datenreplikationsstream verschlüsseln, indem Sie die DD Boost-Option zur Verschlüsselung der Dateireplikation aktivieren.

Hinweis

Wenn die DD Boost-Verschlüsselung für die Dateireplikation auf Systemen ohne die Data-at-Rest-Option verwendet wird, muss sie sowohl auf dem Quell- als auch dem Zielsystem aktiviert werden.

TCP-Porteinstellungen der Managed File Replication
Für die DD Boost Managed File Replication verwenden Sie auf dem Data Domain-Quellsystem und -Zielsystem denselben globalen Listen-Port. Verwenden Sie zum Festlegen des Listen-Ports den Befehl `replication option` wie im *Data Domain Operating System Command Reference Guide* beschrieben.

Netzwerkeinstellung „File Replication“

Verwenden Sie diese Option, um den bevorzugten Netzwerktyp für die Replikation der DD Boost-Datei auf IPv4 oder auf IPv6 festzulegen.

Managen von Zertifikaten für DD Boost

Ein Hostzertifikat ermöglicht es DD Boost-Clientprogrammen, beim Herstellen einer Verbindung die Identität des Systems zu überprüfen. Zertifikate der Zertifizierungsstelle identifizieren Zertifizierungsstellen, die vom System als vertrauenswürdig eingestuft werden müssen. Die Themen in diesem Abschnitt beschreiben, wie Sie Host- und Zertifizierungsstellenzertifikate managen.

Hinzufügen eines Hostzertifikats für DD Boost

Fügen Sie ein Hostzertifikat zu Ihrem System hinzu. DD OS unterstützt ein Hostzertifikat für DD Boost.

Vorgehensweise

1. Wenn Sie noch kein Hostzertifikat angefordert haben, fordern Sie eines von einer vertrauenswürdige Zertifizierungsstelle an.
2. Nachdem Sie ein Hostzertifikat erhalten haben, kopieren oder verschieben Sie es auf den Computer, auf dem Sie DD Service Manager ausführen.
3. Starten Sie DD System Manager auf dem System, auf dem Sie ein Hostzertifikat hinzufügen möchten.

Hinweis

DD System Manager unterstützt das Zertifikatsmanagement nur auf dem Managementsystem (dem System, auf dem DD System Manager ausgeführt wird).

4. Wählen Sie **Protocols** > **DD Boost** > **More Tasks** > **Manage Certificates...**.

Hinweis

Wenn Sie versuchen, Zertifikate auf einem verwalteten System remote zu verwalten, zeigt DD System Manager oben im Zertifikatmanagementdialog eine Infomeldung an. Um Zertifikate für ein System verwalten zu können, müssen Sie DD System Manager auf diesem System starten.

5. Klicken Sie im Bereich „Host Certificate“ auf **Add**.
6. Gehen Sie wie folgt vor, um ein Hostzertifikat hinzuzufügen, das in eine .p12-Datei eingeschlossen ist:
   a. Wählen Sie **I want to upload the certificate as a .p12 file**.
   b. Geben Sie das Passwort in das Feld **Password** ein.
   c. Klicken Sie auf **Browse** und wählen Sie die Hostzertifikatdatei aus, die an das System hochgeladen werden soll.
   d. Klicken Sie auf **Add**.
7. Gehen Sie wie folgt vor, um ein Hostzertifikat hinzuzufügen, das in eine .pem-Datei eingeschlossen ist:
   a. Wählen Sie **I want to upload the public key as a .pem file and use a generated private key**.
   b. Klicken Sie auf **Browse** und wählen Sie die Hostzertifikatdatei aus, die an das System hochgeladen werden soll.
   c. Klicken Sie auf **Add**.

Hinzufügen von Zertifikaten der Zertifizierungsstelle für DD Boost

Fügen Sie ein Zertifikat für eine vertrauenswürdige Zertifizierungsstelle zu Ihrem System hinzu. DD OS unterstützt mehrere Zertifikate für vertrauenswürdige Zertifizierungsstellen.

Vorgehensweise

1. Erwerben Sie für die vertrauenswürdige Zertifizierungsstelle ein Zertifikat.
2. Kopieren oder verschieben Sie das Zertifikat der vertrauenswürdigen Zertifizierungsstelle auf den Computer, auf dem DD Service Manager ausgeführt wird.
3. Starten Sie DD System Manager auf dem System, auf dem Sie das Zertifikat der Zertifizierungsstelle hinzufügen möchten.

Hinweis

DD System Manager unterstützt das Zertifikatsmanagement nur auf dem Managementsystem (dem System, auf dem DD System Manager ausgeführt wird).

4. Wählen Sie **Protocols** > **DD Boost** > **More Tasks** > **Manage Certificates...**.

   Hinweis

   Wenn Sie versuchen, Zertifikate auf einem verwalteten System remote zu verwalten, zeigt DD System Manager oben im Zertifikatmanagementdialog eine Infomeldung an. Um Zertifikate für ein System verwalten zu können, müssen Sie DD System Manager auf diesem System starten.

5. Klicken Sie im Bereich „CA Certificates“ auf **Add**.

   Das Dialogfeld „Add CA Certificate for DD Boost“ wird angezeigt.

6. Gehen Sie wie folgt vor, um ein Zertifikat der Zertifizierungsstelle hinzuzufügen, das in eine .pem-Datei eingeschlossen ist:

   a. Wählen Sie **I want to upload the certificate as a .pem file**.

   b. Klicken Sie auf **Browse**, wählen Sie die Zertifikatdatei aus, die in das System hochgeladen werden soll, und klicken Sie auf **Open**.

   c. Klicken Sie auf **Add**.

7. Gehen Sie wie folgt vor, um ein Zertifikat der Zertifizierungsstelle mittels Kopieren und Einfügen hinzuzufügen:

   a. Kopieren Sie den Zertifikattext mithilfe der Steuerelemente in Ihrem Betriebssystem in die Zwischenablage.

   b. Wählen Sie **I want to copy and paste the certificate text**.

   c. Fügen Sie den Zertifikattext im Feld unter der Auswahl für Kopieren und Einfügen ein.

   d. Klicken Sie auf **Add**.

Managen von DD Boost-Clientzugriff und -Clientverschlüsselung

Verwenden Sie die Registerkarte „DD Boost Settings“ für die Konfiguration der Clients oder Clientgruppe, die eine DD Boost-Verbindung mit dem Data Domain-System herstellen können, sowie zum Festlegen, ob eine Verschlüsselung verwendet werden soll. Standardmäßig ist das System so konfiguriert, dass alle Clients ohne Verschlüsselung Zugriff haben.

Hinweis

Die Aktivierung der In-Flight-Verschlüsselung wirkt sich negativ auf die Performance des Systems aus.

Hinweis

DD Boost bietet Optionen für globale Authentifizierung und Verschlüsselung, um Ihr System gegen Man-in-the-Middle(MITM)-Angriffe zu verteidigen. Sie geben Authentifizierungs- und Verschlüsselungseinstellungen mit CLI-Befehlen auf dem Data Domain-System mit der GUI an. Weitere Informationen finden Sie im *Data Domain Boost for OpenStorage 3.4 Administration Guide* und Hinzufügen eines DD Boost-Clients auf Seite 358 oder im *Data Domain 6.1 Command Reference Guide*.

Hinzufügen eines DD Boost-Clients

Erstellen Sie einen zulässigen DD Boost-Client und geben Sie an, ob der Client eine Verschlüsselung verwendet.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **Settings**.
2. Klicken Sie im Abschnitt „Allowed Clients“ auf **Create (+)**.

   Das Dialogfeld „Add Allowed Client“ wird angezeigt.

3. Geben Sie den Hostnamen des Clients ein.

   Hierbei kann es sich um einen vollständig qualifizierten Domainname (z. B. host1.emc.com) oder um einen Hostnamen mit einem Platzhalter (z. B. *.emc.com) handeln.

4. Wählen Sie die Verschlüsselungsstärke aus.

   Folgende Optionen stehen zur Verfügung: „None“ (keine Verschlüsselung), „Medium“ (AES128-SHA1) oder „High“ (AES256-SHA1).

5. Wählen Sie den Authentifizierungsmodus aus.

   Folgende Optionen stehen zur Verfügung: „One Way“, „Two Way“, „Two Way Password“ oder „Anonymous“.

6. Klicken Sie auf **OK**.

Ändern eines DD Boost-Clients

Ändern Sie Name, Verschlüsselungsstärke und Authentifizierungsmodus eines zulässigen DD Boost-Clients.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **Settings**.
2. Wählen Sie in der Liste „Allowed Clients“ den Client aus, für den Sie Änderungen vornehmen möchten.
3. Klicken Sie auf die Schaltfläche **Edit**, die als Stiftsymbol angezeigt wird.

   Das Dialogfeld „Modify Allowed Client“ wird angezeigt.

4. Wenn Sie den Namen eines Clients ändern möchten, bearbeiten Sie den Clienttext.
5. Wenn Sie die Verschlüsselungsstärke ändern möchten, wählen Sie die entsprechende Option aus.

   Folgende Optionen stehen zur Verfügung: „None“ (keine Verschlüsselung), „Medium“ (AES128-SHA1) oder „High“ (AES256-SHA1).

6. Wenn Sie den Authentifizierungsmodus ändern möchten, wählen Sie die entsprechende Option aus.

   Folgende Optionen stehen zur Verfügung: „One Way“, „Two Way“ oder „Anonymous“.

7. Klicken Sie auf **OK**.

Entfernen eines DD Boost-Clients

Löschen Sie einen zulässigen DD Boost-Client.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **Settings**.
2. Wählen Sie den Client aus der Liste aus.
3. Klicken Sie auf **Delete (X)**.

   Das Dialogfeld „Delete Allowed Clients“ wird angezeigt.
4. Wählen Sie nach der Bestätigung den Clientnamen aus. Klicken Sie auf **OK**.

Informationen über Schnittstellengruppen

Mit dieser Funktion können Sie mehrere Ethernetlinks zu einer Gruppe zusammenfassen und somit nur eine Schnittstelle auf dem Data Domain-System mit der Backupanwendung registrieren. Die DD Boost Library verhandelt mit dem Data Domain-System, um die beste Schnittstelle für das Senden von Daten zu erhalten. Lastenausgleich bietet einen höheren physischen Durchsatz im Data Domain-System.

Durch Konfigurieren einer Schnittstellengruppe wird ein privates Netzwerk innerhalb des Data Domain-Systems erstellt, das sich aus den IP-Adressen, die als Gruppe angegeben sind, zusammensetzt. Clients werden einer einzigen Gruppe zugewiesen und die Gruppenschnittstelle verwendet zur Verbesserung von Datenübertragungsperformance und Zuverlässigkeit den Lastenausgleich.

Beispiel: In der Symantec NetBackup-Umgebung verwenden Medienserverclients eine einzige IP-Adresse des öffentlichen Netzwerks, um auf das Data Domain-System zuzugreifen. Jegliche Kommunikation mit dem Data Domain-System wird über diese verwaltete IP-Verbindung initiiert, die auf dem NetBackup-Server konfiguriert ist.

Wenn eine Schnittstellengruppe konfiguriert wird und das Data Domain-System Daten von den Medienserverclients erhält, wird für die Datenübertragung ein Lastenausgleich durchgeführt und die Daten werden auf alle Schnittstellen in der Gruppe verteilt, sodass ein höherer Eingabe-/Ausgabedurchsatz erreicht wird, insbesondere für Kunden, die mehrere 1-GigE-Verbindungen verwenden.

Der Lastenausgleich für die Datenübertragung basiert auf der Anzahl der Verbindungen, die auf den Schnittstellen ausstehen. Nur für Verbindungen für Backup- und Wiederherstellungsjobs wird ein Lastenausgleich durchgeführt. Überprüfen Sie die aktiven Verbindungen, um mehr Informationen über die Anzahl der ausstehenden Verbindungen für die Schnittstellen in einer Gruppe zu erhalten.

Wenn eine Schnittstelle in der Gruppe ausfällt, werden alle Jobs in Flight zu dieser Schnittstelle automatisch auf integren Betriebslinks wieder aufgenommen (ohne Erkennung durch die Backupanwendungen). Alle Jobs, die nach dem Ausfall gestartet werden, werden auch auf eine integre Schnittstelle in der Gruppe geleitet. Wenn die Gruppe deaktiviert ist oder ein Versuch fehlschlägt, eine alternative Schnittstelle wiederherzustellen, wird die verwaltete IP für die Recovery verwendet. Fehler in einer Gruppe nutzen keine Schnittstellen aus einer anderen Gruppe.

Berücksichtigen Sie beim Managen von Schnittstellengruppen folgende Informationen.

- Die IP-Adresse muss auf dem Data Domain-System konfiguriert werden und dessen Schnittstelle aktiviert sein. Um die Schnittstellenkonfiguration zu prüfen, wählen Sie die Seite **Hardware** > **Ethernet** > **Interfaces** und prüfen Sie auf freie Ports. Im Kapitel `net` im *Data Domain Operating System Command Reference Guide*

oder im *Data Domain Operating System Initial Configuration Guide* finden Sie Informationen zum Konfigurieren einer IP-Adresse für eine Schnittstelle.

- Zum Managen von Schnittstellengruppen können Sie die `ifgroup`-Befehle verwenden. Diese Befehle werden im *Data Domain Operating System Command Reference Guide* ausführlich beschrieben.
- Schnittstellengruppen bieten vollständigen Support für statische IPv6-Adressen, d. h. dieselben Funktionen für IPv6 wie für IPv4. Gleichzeitige IPv4- und IPv6-Clientverbindungen sind zulässig. Für einen mit IPv6 verbundenen Client sind nur IPv6-ifgroup-Schnittstellen sichtbar. Ein mit IPv4 verbundener Client erkennt nur IPv4-IFGROUP-Schnittstellen. Einzelne ifgroups enthalten alle IPv4- bzw. alle IPv6-Adressen. Detaillierte Informationen finden Sie im *Data Domain Boost for Partner Integration Administration Guide* oder im *Data Domain Boost for OpenStorage Administration Guide*.
- Konfigurierte Schnittstellen werden in den aktiven Verbindungen aufgeführt, auf dem unteren Teil der Seite „Activities“.

Hinweis

Unter Verwendung von DD Boost auf HA-Systemen auf Seite 372 erhalten Sie wichtige Informationen zur Verwendung von Schnittstellengruppen mit HA-Systemen.

In den folgenden Themen wird beschrieben, wie Sie Schnittstellengruppen managen.

Schnittstellen

IFGROUP unterstützt physische und virtuelle Schnittstellen.

Eine IFGROUP-Schnittstelle ist Mitglied einer einzigen IFGROUP *<group-name>* und kann aus den folgenden Elementen bestehen:

- Physische Schnittstellen wie `eth0a`
- Virtuelle Schnittstelle, erstellt für Link-Failover oder Linkzusammenfassung, wie `veth1`
- Virtuelle Aliasschnittstelle wie `eth0a:2` oder `veth1:2`
- Virtuelle VLAN-Schnittstelle wie `eth0a.1` oder `veth1.1`
- Innerhalb einer IFGROUP *<group-name>* müssen alle Schnittstellen eindeutige Schnittstellen sein (Ethernet, virtuelles Ethernet), um im Fall eines Netzwerkfehlers ein Failover sicherzustellen.

IFGROUP bietet vollständige Unterstützung für statische IPv6-Adressen, d. h. dieselben Funktionen für IPv6 wie für IPv4. Gleichzeitige IPv4- und IPv6-Clientverbindungen sind zulässig. Für einen mit IPv6 verbundenen Client sind nur IPv6-IFGROUP-Schnittstellen sichtbar. Ein mit IPv4 verbundener Client erkennt nur IPv4-IFGROUP-Schnittstellen. Einzelne IFGROUPS enthalten alle IPv4- bzw. alle IPv6-Adressen.

Weitere Informationen finden Sie im *Data Domain Boost for Partner Integration Administration Guide* oder im *Data Domain Boost for OpenStorage Administration Guide*.

Schnittstellenerzwingung

Mithilfe von IFGROUP können Sie eine Verbindung über ein privates Netzwerk erzwingen und so sicherstellen, dass ein fehlgeschlagener Job nach einem Netzwerkfehler keine Verbindung über das öffentliche Netzwerk herstellt.

Bei aktivierter Schnittstellendurchsetzung können fehlgeschlagene Jobs nur über eine alternative IP-Adresse eines privaten Netzwerks einen erneuten Versuch durchführen.

Die Schnittstellendurchsetzung ist nur für Clients verfügbar, die IFGROUP-Schnittstellen verwenden.

Die Schnittstellendurchsetzung ist standardmäßig deaktiviert (FALSE). Zum Aktivieren der Schnittstellendurchsetzung müssen Sie die folgende Einstellung in die Systemregistrierung einfügen:

`system.ENFORCE_IFGROUP_RW=TRUE`

Nachdem Sie diesen Eintrag in die Registrierung eingefügt haben, müssen Sie `filesys restart` ausführen, damit die Einstellung wirksam wird.

Weitere Informationen finden Sie im *Data Domain Boost for Partner Integration Administration Guide* oder im *Data Domain Boost for OpenStorage Administration Guide*.

Clients

IFGROUP unterstützt verschiedene Benennungsformate für Clients. Die Clientauswahl basiert auf einer festgelegten Reihenfolge.

Ein IFGROUP-Client ist Mitglied einer einzigen ifgroup *<group-name>* und kann aus den folgenden Elementen bestehen:

- Ein vollständig qualifizierter Domainname (FQDN), z. B. „ddboost.datadomain.com“
- Ein partieller Host, der es Ihnen ermöglicht, nach den ersten *n* Zeichen des Hostnamens zu suchen. Beispiel: Wenn n=3, sind gültige Formate `rtp_.*emc.com` und `dur_.*emc.com`. Fünf verschiedene Werte von *n* (1-5) werden unterstützt.
- Platzhalter wie `*.datadomain.com` oder „`*`“
- Ein Kurzname für den Client, z. B. „ddboost“
- Ein öffentlicher IP-Bereich für den Client, z. B. 128.5.20.0/24

Vor der Lese- bzw. Schreibverarbeitung fordert der Client eine IFGROUP-IP-Adresse vom Server an. Für die Auswahl der Client-IFGROUP-Zuordnung werden die Clientinformationen gemäß der folgenden Reihenfolge ausgewertet.

1. IP-Adresse des verbundenen Data Domain-Systems. Wenn in der IFGROUP-Schnittstelle bereits eine aktive Verbindung zwischen Client und Data Domain-System vorhanden ist, werden die IFGROUP-Schnittstellen dem Client zur Verfügung gestellt.
2. Verbundener Client-IP-Bereich. Die IP-Maske wird mit der Quell-IP-Adresse des Clients verglichen; bei einer Übereinstimmung in der Liste der IFGROUP-Clients werden die IFGROUP-Schnittstellen dem Client zur Verfügung gestellt.
   - Für IPv4 können Sie fünf verschiedene Bereichsmasken auswählen, basierend auf einem Netzwerk.
   - Bei IPv6 sind die festen Masken /64, /112 und /128 verfügbar.

   Diese Prüfung des Hostbereichs ist bei separaten VLANs mit vielen Clients nützlich, wenn kein eindeutiger Teilhostname (Domain) vorhanden ist.
3. Clientname: `abc-11.d1.com`
4. Name der Clientdomain: `*.d1.com`
5. Alle Clients: `*`

Weitere Informationen finden Sie im *Data Domain Boost for Partner Integration Administration Guide*.

Erstellen von Schnittstellengruppen

Verwenden Sie die Registerkarte „IP Network“, um Schnittstellengruppen zu erstellen und Schnittstellen und Clients zu den Gruppen hinzuzufügen.

Mehrere Schnittstellengruppen verbessern die Effizienz von DD Boost, da sie Folgendes ermöglichen:

- Konfigurieren von DD Boost für die Verwendung spezieller Schnittstellen, die in Gruppen konfiguriert sind
- Zuweisen von Clients zu einer dieser Schnittstellengruppen
- Überwachen, welche Schnittstellen mit DD Boost-Clients aktiv sind

Erstellen Sie zunächst Schnittstellengruppen und fügen Sie dann Clients (wenn neue Medienserver verfügbar werden) zu einer Schnittstellengruppe hinzu.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **IP Network**.
2. Klicken Sie im Abschnitt "Interface Groups" auf "Add" (**+**).
3. Geben Sie den Namen für die Schnittstellengruppe ein.
4. Wählen Sie eine oder mehrere Schnittstellen aus. Sie können maximal 32 Schnittstellen konfigurieren.

   Hinweis

   Je nach Aliaskonfigurationen können einige Schnittstellen möglicherweise nicht ausgewählt werden, wenn sie eine physische Schnittstelle mit einer anderen Schnittstelle in derselben Gruppe gemeinsam nutzen. Dies ist darauf zurückzuführen, dass sich jede Schnittstelle in der Gruppe auf einer anderen physischen Schnittstelle befinden muss, damit eine Failover Recovery sichergestellt ist.

5. Klicken Sie auf **OK**.
6. Klicken Sie im Abschnitt "Configured Clients" auf "Add" (**+**).
7. Geben Sie einen vollständig qualifizierten Clientnamen oder `*.mydomain.com` ein.

   Hinweis

   Der *-Client ist anfangs für die Standardgruppe verfügbar. Der *-Client kann nur Mitglied einer Schnittstellengruppe (ifgroup) sein.

8. Wählen Sie eine zuvor konfigurierte Schnittstellengruppe aus und klicken Sie auf **OK**.

Aktivieren und Deaktivieren von Schnittstellengruppen

Verwenden Sie zum Aktivieren und Deaktivieren von Schnittstellengruppen die Registerkarte „IP Network“.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **IP Network**.

2. Wählen Sie im Abschnitt „Interface Groups“ die Schnittstellengruppe in der Liste.

   Hinweis

   Wenn für die Schnittstellengruppe nicht sowohl Clients als auch Schnittstellen zugewiesen wurden, können Sie die Gruppe nicht aktivieren.

3. Klicken Sie auf **Edit** (Stift).
4. Klicken Sie auf **Enabled**, um die Schnittstellengruppe zu aktivieren; deaktivieren Sie das Kontrollkästchen zum Deaktivieren.
5. Klicken Sie auf **OK**.

Ändern von Schnittstellengruppennamen und Schnittstellen

Verwenden Sie die Registerkarte „IP Network“, um den Namen einer Schnittstellengruppe und die der Gruppe zugewiesenen Schnittstellen zu ändern.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **IP Network**.
2. Wählen Sie im Abschnitt „Interface Groups“ die Schnittstellengruppe aus der Liste.
3. Klicken Sie auf **Edit** (Stift).
4. Geben Sie den Namen erneut ein, um den Namen zu ändern.

   Der Gruppenname muss ein bis 24 Zeichen lang sein und darf nur Buchstaben, Ziffern, Unterstriche und Bindestriche enthalten. Er darf mit keinem anderen Gruppennamen identisch sein und darf nicht „default“, „yes“, „no“ oder „all“ lauten.

5. Wählen Sie in der Liste „Interfaces“ Clientschnittstellen aus oder heben Sie die Auswahl auf.

   Hinweis

   Wenn Sie alle Schnittstellen aus der Gruppe entfernen, wird diese automatisch deaktiviert.

6. Klicken Sie auf **OK**.

Löschen einer Schnittstellengruppe

Verwenden Sie die Registerkarte „IP Network“, um eine Schnittstellengruppe zu löschen. Beim Löschen einer Schnittstellengruppe werden alle Schnittstellen und Clients gelöscht, die dieser Gruppe zugewiesen sind.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **IP Network**.
2. Wählen Sie im Abschnitt „Interface Groups“ die Schnittstellengruppe in der Liste. Die Standardgruppe kann nicht gelöscht werden.
3. Klicken Sie auf „Delete“ (**X**).
4. Bestätigen Sie den Löschvorgang.

Hinzufügen eines Clients zu einer Schnittstellengruppe

Verwenden Sie die Registerkarte „IP Network“, um Clients zu Schnittstellengruppen hinzuzufügen.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **IP Network**.
2. Klicken Sie im Abschnitt "Configured Clients" auf "Add" (**+**).
3. Geben Sie einen Namen für den Client ein.

   Clientnamen müssen eindeutig sein und können aus den folgenden Elementen bestehen:

   - **FQDN**
   - ***.domain**
   - Öffentlicher IP-Bereich des Clients:
     - Bei IPv4 stellt `xx.xx.xx.0/24` eine 24-Bit-Maske für die Verbindung der IP-Adresse bereit. Der Wert „/24“ gibt an, welche Bits maskiert werden, wenn die Quell-IP-Adresse des Clients für den Zugriff auf die IFGROUP ausgewertet wird.
     - Bei IPv6 wird mit `xxxx::0/112` eine 112-Bit-Maske für die verbundene IP-Adresse angegeben. Der Wert „/112“ gibt an, welche Bits maskiert werden, wenn die Quell-IP-Adresse des Clients für den Zugriff auf die IFGROUP ausgewertet wird.

   Clientnamen dürfen maximal 128 Zeichen lang sein.
4. Wählen Sie eine zuvor konfigurierte Schnittstellengruppe aus und klicken Sie auf **OK**.

Ändern des Namens oder der Schnittstellengruppe eines Clients

Verwenden Sie die Registerkarte „IP Network“, um den Namen oder die Schnittstellengruppe eines Clients zu ändern.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **IP Network**.
2. Wählen Sie im Abschnitt "Configured Clients" den Client.
3. Klicken Sie auf **Edit**(Stift).
4. Geben Sie einen neuen Clientnamen ein.

   Clientnamen müssen eindeutig sein und können aus den folgenden Elementen bestehen:

   - **FQDN**
   - ***.domain**
   - Öffentlicher IP-Bereich des Clients:
     - Bei IPv4 stellt `xx.xx.xx.0/24` eine 24-Bit-Maske für die Verbindung der IP-Adresse bereit. Der Wert „/24“ gibt an, welche Bits maskiert werden, wenn die Quell-IP-Adresse des Clients für den Zugriff auf die IFGROUP ausgewertet wird.
     - Bei IPv6 wird mit `xxxx::0/112` eine 112-Bit-Maske für die verbundene IP-Adresse angegeben. Der Wert „/112“ gibt an, welche Bits maskiert

werden, wenn die Quell-IP-Adresse des Clients für den Zugriff auf die IFGROUP ausgewertet wird.

Clientnamen dürfen maximal 128 Zeichen lang sein.

5. Wählen Sie eine neue Schnittstellengruppe aus dem Menü aus.

Hinweis

Die alte Schnittstellengruppe ist deaktiviert, wenn sie keine Clients hat.

6. Klicken Sie auf **OK**.

Löschen eines Clients aus der Schnittstellengruppe

Verwenden Sie die Registerkarte „IP Network“, um einen Client aus einer Schnittstellengruppe zu löschen.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **IP Network**.
2. Wählen Sie im Abschnitt „Configured Clients“ den Client aus.
3. Klicken Sie auf „Delete“ (**X**).

Hinweis

Wenn die Schnittstellengruppe, zu der der Client gehört, keine weiteren Clients hat, wird die Schnittstellengruppe deaktiviert.

4. Bestätigen Sie den Löschvorgang.

Verwenden von Schnittstellengruppen für Managed File Replication (MFR)

Schnittstellengruppen können verwendet werden, um die für DD Boost-MFR verwendeten Schnittstellen zu steuern, um die Replikationsverbindung über ein bestimmtes Netzwerk zu leiten und um mehrere Netzwerkschnittstellen mit hoher Bandbreite und Zuverlässigkeit für Failover-Bedingungen verwenden zu können. Alle Data Domain-IP-Typen werden unterstützt: IPv4 oder IPv6, Alias-IP/VLAN-IP und LACP-Failover-Zusammenfassung.

Hinweis

Für die Replikation verwendete Schnittstellengruppen unterscheiden sich von den zuvor beschriebenen Schnittstellengruppen und werden nur für DD Boost-Managed File Replication (MFR) unterstützt. Detaillierte Informationen zur Verwendung von Schnittstellengruppen für MFR finden Sie im *Data Domain Boost for Partner Integration Administration Guide* oder im *Data Domain Boost for OpenStorage Administration Guide*.

Ohne die Verwendung von Schnittstellengruppen erfordert eine Konfiguration für die Replikation mehrere Schritte:

1. Hinzufügen eines Eintrags in der `/etc/hosts`-Datei auf dem Data Domain-Quellsystem für das Data Domain-Zielsystem und harte Programmierung einer der privaten LAN-Netzwerkschnittstellen als Ziel-IP-Adresse.
2. Hinzufügen einer Route auf dem Data Domain-Quellsystem zum Data Domain-Zielsystem, wobei ein physischer oder virtueller Port auf dem Data Domain-Quellsystem zur Remoteziel-IP-Adresse angeben werden muss.

3. Konfigurieren von LACP über das Netzwerk auf alle Switche zwischen den Data Domain-Systemen für den Lastenausgleich und Failover.
4. Es sind verschiedene Anwendungen erforderlich, um unterschiedliche Namen für das Data Domain-Zielsystem zu verwenden und so Benennungskonflikte in der `/etc/hosts`-Datei zu vermeiden.

Die Verwendung von Schnittstellengruppen für die Replikation vereinfacht diese Konfiguration durch die Verwendung der DD OS-System Manager- oder DD OS-CLI-Befehle. Die Verwendung von Schnittstellengruppen zum Konfigurieren des Replikationspfads bietet Ihnen die folgenden Möglichkeiten:

- Umleiten einer durch den Hostnamen aufgelösten IP-Adresse vom öffentlichen Netzwerk weg, indem eine andere private Data Domain-System-IP-Adresse verwendet wird.
- Identifizieren einer Schnittstellengruppe basierend auf konfigurierten Auswahlkriterien, wodurch eine einzelne Schnittstellengruppe bereitgestellt wird, von der aus alle Schnittstellen vom Data Domain-Zielsystem erreichbar sind.
- Auswählen einer privaten Netzwerkschnittstelle aus einer Liste von Schnittstellen, die zu einer Gruppe gehören, wodurch sichergestellt wird, dass die Schnittstelle ordnungsgemäß funktioniert.
- Bereitstellen des Lastenausgleichs über mehrere Data Domain-Schnittstellen in demselben privaten Netzwerk.
- Bereitstellen einer Failover-Schnittstelle für das Recovery der Schnittstellen in der Schnittstellengruppe.
- Bereitstellen von Host-Failover, wenn dies auf dem Data Domain-Quellsystem konfiguriert ist.
- Verwenden von NAT (Network Address Translation)

Der Auswahlreihenfolge zur Ermittlung einer passenden Schnittstellengruppe für die Dateireplikation lautet wie folgt:

1. Lokaler MTree-Pfad (Speichereinheit) und ein bestimmter Remote-Data-Domain-Hostname
2. Lokaler MTree-Pfad (Speichereinheit) mit einem beliebigen Remote-Data-Domain-Hostnamen
3. Beliebiger MTree-Pfad (Speichereinheit) mit einem bestimmten -Data-Domain-Hostnamen

Der gleiche MTree kann nur dann in mehreren Schnittstellengruppen auftreten, wenn er einen anderen Data Domain-Hostnamen hat. Der gleiche Data Domain-Hostname kann nur dann in mehreren Schnittstellengruppen auftreten, wenn er einen anderen MTree-Pfad hat. Es wird erwartet, dass der Remotehostname ein FQDN ist, z. B. dd890-1.emc.com.

Die Auswahl der Schnittstellengruppe erfolgt lokal auf dem Data Domain-Quellsystem und dem Data Domain-Zielsystem, und zwar unabhängig voneinander. Bei einem WAN-Replikationsnetzwerk muss nur die Remoteschnittstellengruppe konfiguriert werden, da die Quell-IP-Adresse dem Gateway für die Remote-IP-Adresse entspricht.

Hinzufügen eines Replikationspfads zu einer Schnittstellengruppe

Verwenden Sie die Registerkarte "IP Network", um Replikationspfade zu Schnittstellengruppen hinzuzufügen.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **IP Network**.

2. Klicken Sie im Abschnitt "Configured Replication Paths" auf "Add" (**+**).
3. Geben Sie Werte für **MTree** und/oder **Remote Host** ein.
4. Wählen Sie eine zuvor konfigurierte Schnittstellengruppe aus und klicken Sie auf **OK**.

Ändern eines Replikationspfads für eine Schnittstellengruppe

Verwenden Sie die Registerkarte "IP Network", um die Replikationspfade für Schnittstellengruppen zu ändern.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **IP Network**.
2. Wählen Sie im Abschnitt "Configured Replication Paths" den Replikationspfad.
3. Klicken Sie auf **Edit** (Stift).
4. Ändern Sie beliebige oder alle Werte für **MTree**, **Remote Host** oder **Interface Group**.
5. Klicken Sie auf **OK**.

Löschen eines Replikationspfads für eine Schnittstellengruppe

Verwenden Sie die Registerkarte „IP Network“, um Replikationspfade für Schnittstellengruppen zu löschen.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **IP Network**.
2. Wählen Sie im Abschnitt „Configured Replication Paths“ den Replikationspfad aus.
3. Klicken Sie auf „Delete“ (**X**).
4. Klicken Sie im Dialogfeld „Delete Replication Path(s)“ auf **OK**.

Löschen von DD Boost

Verwenden Sie diese Option, um alle Daten (Daten-Images) zu entfernen, die sich in den Speichereinheiten befinden. Wenn Sie DD Boost deaktivieren oder löschen, wird der DD Boost FC-Service ebenfalls deaktiviert. Nur ein Administrator-Benutzer kann DD Boost löschen.

Vorgehensweise

1. Entfernen Sie manuell alle entsprechenden Katalogeinträge der Backupanwendung (lassen Sie sie ablaufen).

   Hinweis

   Wenn mehrere Backupanwendungen dasselbe Data Domain-System verwenden, entfernen Sie alle Einträge aus jedem Katalog dieser Anwendungen.

2. Wählen Sie **Protocols** > **DD Boost** > **More Tasks** > **Destroy DD Boost...**.
3. Geben Sie Ihre Administrator-Anmeldedaten ein, wenn Sie dazu aufgefordert werden.
4. Klicken Sie auf **OK**.

Konfigurieren von DD Boost-over-Fibre Channel

In früheren Versionen von DD OS wurde die gesamte Kommunikation zwischen der DD Boost Library und den Data Domain-Systemen mithilfe des IP-Netzwerks durchgeführt. DD OS bietet nun Fibre Channel als einen alternativen Übertragungsmechanismus für die Kommunikation zwischen der DD Boost Library und dem Data Domain-System.

Hinweis

Windows-, Linux-, HP-UX- (64-Bit-Itanium-Architektur), AIX-und Solaris-Clientumgebungen werden unterstützt.

Aktivieren von DD Boost-Benutzern

Bevor Sie auf einem Data Domain-System den DD Boost-over-FC-Service konfigurieren können, müssen Sie mindestens einen DD Boost-Benutzer hinzufügen und DD Boost aktivieren.

Bevor Sie beginnen

- Melden Sie sich bei DD System Manager an. Anweisungen hierzu finden Sie unter „An- und Abmelden bei DD System Manager“.
  CLI-Entsprechung

```
login as: sysadmin
Data Domain OS 5.7.x.x-12345
Using keyboard-interactive authentication.
Password:
```

- Stellen Sie bei Verwendung der Befehlszeilenoberfläche sicher, dass der Daemon des SCSI-Ziels aktiviert ist:

```
# scsitarget enable
Please wait ...
SCSI Target subsystem is enabled.
```

  Hinweis

  Wenn Sie DD System Manager verwenden, wird der Daemon des SCSI-Ziels bei der Aktivierung des DD Boost-over-FC-Service (später in diesem Verfahren) automatisch aktiviert.

- Überprüfen Sie, ob die DD Boost-Lizenz installiert ist. Wählen Sie in DD System Manager **Protocols** > **DD Boost** > **Settings** aus. Wenn der Status angibt, dass DD Boost nicht lizenziert ist, klicken Sie auf **Add License** und geben Sie im Dialogfeld „Add License Key“ eine gültige Lizenz ein.
  CLI-Entsprechungen

```
# license show
```

```
# license add license-code
```

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **Settings**.
2. Geben Sie im Abschnitt "Users with DD Boost Access" einen oder mehrere DD Boost-Benutzernamen ein.

   Ein DD Boost-Benutzer ist auch ein DD OS-Benutzer. Wenn Sie einen DD Boost-Benutzernamen angeben, können Sie einen vorhandenen DD OS-Benutzernamen auswählen oder Sie können einen neuen DD OS-Benutzernamen erstellen und diesen Namen zu einem DD Boost-Benutzer

machen. Diese Version unterstützt mehrere DD Boost-Benutzer. Detaillierte Anweisungen finden Sie unter „Festlegen von DD Boost-Benutzernamen“.

CLI-Entsprechungen

```
# user add username [password password]
```

```
# ddboost set user-name exampleuser
```

3. Klicken Sie zum Aktivieren von DD Boost auf **Enable**.

   CLI-Entsprechung

   ```
   # ddboost enable
   Starting DDBOOST, please wait..............
   DDBOOST is enabled.
   ```

Ergebnisse

Nun können Sie den DD Boost-over-FC-Service auf dem Data Domain-System konfigurieren.

Konfiguration von DD Boost

Nachdem Sie Benutzer hinzugefügt und DD Boost aktiviert haben, müssen Sie die Fibre Channel-Option aktivieren und den DD Boost-Fibre Channel-Servernamen festlegen. Je nach Anwendung müssen Sie zudem eine oder mehrere Speichereinheiten erstellen und die DD Boost-API bzw. das DD Boost-Plug-in auf den Medienservern installieren, die auf das Data Domain-System zugreifen.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **Fibre Channel**.
2. Klicken Sie zum Aktivieren des Fibre Channel-Transports auf die Schaltfläche **Enable**.

   CLI-Entsprechung

   ```
   # ddboost option set fc enabled
   Please wait...
   DD Boost option "FC" set to enabled.
   ```

3. Um die Standardeinstellung (Hostname) für den DD Boost-Fibre Channel-Servernamen zu ändern, klicken Sie auf **Edit**, geben Sie einen neuen Servernamen ein und klicken Sie auf **OK**.

   CLI-Entsprechung

   ```
   # ddboost fc dfc-server-name set DFC-ddbeta2
   DDBoost dfc-server-name is set to "DFC-ddbeta2" for DDBoost FC.
   Configure clients to use "DFC-DFC-ddbeta2" for DDBoost FC.
   ```

4. Rufen Sie **Protocols** > **DD Boost** > **Storage Units** auf, um eine Speichereinheit zu erstellen (wenn nicht bereits von der Anwendung eine erstellt wurde).

   Sie müssen mindestens eine Speichereinheit auf dem Data Domain-System erstellen und dieser Speichereinheit einen DD Boost-Benutzer zuweisen. Detaillierte Anweisungen finden Sie unter „Erstellen einer Speichereinheit“.

   CLI-Entsprechung

```
# ddboost storage-unit create storage_unit_name-su
```

5. Installieren Sie die DD Boost-API bzw. das DD Boost-Plug-in (falls erforderlich, je nach Anwendung).

   Die Software des DD Boost OpenStorage-Plug-ins muss auf den NetBackup-Medienservern installiert werden, die auf das Data Domain-System zugreifen müssen. Dieses Plug-in enthält die erforderliche DD Boost Library, die in das Data Domain-System integriert werden kann. Detaillierte Anweisungen zur Installation und Konfiguration finden Sie im *Data Domain Boost for Partner Integration Administration Guide* oder im *Data Domain Boost for OpenStorage Administration Guide*.

Ergebnisse

Nun können Sie die Konnektivität überprüfen und Zugriffsgruppen erstellen.

Überprüfen von Verbindungen und Erstellen von Zugriffsgruppen

Navigieren Sie zu **Hardware** > **Fibre Channel** > **Resources**, um Initiatoren und Endpunkte für Zugriffspunkte zu managen. Navigieren Sie zu **Protocols** > **DD Boost** > **Fibre Channel**, um DD Boost-over-FC-Zugriffsgruppen zu erstellen und zu managen.

Hinweis

Vermeiden Sie Änderungen an der Zugriffsgruppe in einem Data Domain-System während aktiven Backups oder Wiederherstellungen. Eine Änderung kann dazu führen, dass ein aktiver Job fehlschlägt. Die Auswirkungen von Änderungen während aktiver Jobs hängen von der Kombination aus Backupsoftware und Hostkonfigurationen ab.

Vorgehensweise

1. Wählen Sie **Hardware** > **Fibre Channel** > **Resources** > **Initiators**, um zu überprüfen, ob Initiatoren vorhanden sind.

   Es wird empfohlen, Initiatoren Aliase zuzuweisen, um Verwechslungen während des Konfigurationsprozesses zu vermeiden.

   CLI-Entsprechung

```
# scsitarget initiator show list
Initiator      System Address                Group   Service
-----------   ----------------------   ----------   -------
initiator-1    21:00:00:24:ff:31:b7:16         n/a       n/a
initiator-2    21:00:00:24:ff:31:b8:32         n/a       n/a
initiator-3    25:00:00:21:88:00:73:ee         n/a       n/a
initiator-4    50:06:01:6d:3c:e0:68:14         n/a       n/a
initiator-5    50:06:01:6a:46:e0:55:9a         n/a       n/a
initiator-6    21:00:00:24:ff:31:b7:17         n/a       n/a
initiator-7    21:00:00:24:ff:31:b8:33         n/a       n/a
initiator-8    25:10:00:21:88:00:73:ee         n/a       n/a
initiator-9    50:06:01:6c:3c:e0:68:14         n/a       n/a
initiator-10   50:06:01:6b:46:e0:55:9a         n/a       n/a
tsm6_p23       21:00:00:24:ff:31:ce:f8   SetUp_Test       VTL
-----------   ----------------------   ----------   -------
```

2. Um einem Initiator einen Alias zuzuweisen, wählen Sie einen der Initiatoren aus und klicken Sie auf das Bleistiftsymbol (zum Bearbeiten). Geben Sie im Feld „Name“ des Dialogfelds „Modify Initiator“ den Alias ein und klicken Sie auf **OK**.

   CLI-Entsprechungen

```
# scsitarget initiator rename initiator-1 initiator-renamed
Initiator 'initiator-1' successfully renamed.
```

```
# scsitarget initiator show list
Initiator           System Address                 Group
Service
-----------------   ----------------------   ----------
-------
initiator-2         21:00:00:24:ff:31:b8:32          n/a
n/a
initiator-renamed   21:00:00:24:ff:31:b7:16          n/a
n/a
-----------------   ----------------------   ----------
-------
```

3. Überprüfen Sie auf der Registerkarte „Resources“, ob Endpunkte vorhanden und aktiviert sind.

   CLI-Entsprechung

   ```
   # scsitarget endpoint show list
   -------------   --------------   ------------   -------   ------
   endpoint-fc-0   5a               FibreChannel   Yes       Online
   endpoint-fc-1   5b               FibreChannel   Yes       Online
   -------------   --------------   ------------   -------   ------
   ```

4. Gehen Sie zu **Protocols** > **DD Boost** > **Fibre Channel**.
5. Klicken Sie im Bereich „DD Boost Access Groups“ auf das **+**-Symbol, um eine Zugriffsgruppe hinzuzufügen.
6. Geben Sie einen eindeutigen Namen für die Zugriffsgruppe ein. Doppelte Namen werden nicht unterstützt.

   CLI-Entsprechung

   ```
   # ddboost fc group create test-dfc-group
   DDBoost FC Group "test-dfc-group" successfully created.
   ```

7. Wählen Sie einen oder mehrere Initiatoren aus. Optional können Sie den Initiatornamen ersetzen, indem Sie einen neuen Namen eingeben. Klicken Sie auf **Next**.

   CLI-Entsprechung

   ```
   #ddboost fc group add test-dfc-group initiator initiator-5
   Initiator(s) "initiator-5" added to group "test-dfc-group".
   ```

   Ein Initiator ist ein mit einem Backupclient verbundener Port an einem Hostbusadapter, der mit einem System verbunden ist, um Daten unter Verwendung des Fibre Channel-Protokolls zu lesen und zu schreiben. Der WWPN ist der eindeutige World Wide Port Name des Fibre Channel-Ports auf dem Medienserver.

8. Geben Sie die Anzahl der von der Gruppe zu verwendenden DD Boost-Geräte an. Durch diese Anzahl wird festgelegt, welche Geräte der Initiator erkennen kann, und daher auch die Anzahl der I/O-Pfade zum Data Domain-System. Der Standardwert ist 1, der Mindestwert ist 1 und der Höchstwert 64.

   CLI-Entsprechung

   ```
   # ddboost fc group modify Test device-set count 5
   Added 3 devices.
   ```

   Die empfohlenen Werte für die verschiedenen Clients finden Sie im *Data Domain Boost-Administrationshandbuch für OpenStorage*.

9. Geben Sie an, welche Endpunkte in die Gruppe einbezogen werden sollen: alle, keine oder treffen Sie Ihre Auswahl aus der Liste von Endpunkten. Klicken Sie auf **Next**.

CLI-Entsprechungen

```
# scsitarget group add Test device ddboost-dev8 primary-
endpoint allsecondary-endpoint all
Device 'ddboost-dev8' successfully added to group.
```

```
# scsitarget group add Test device ddboost-dev8 primary-
endpointendpoint-fc-1 secondary-endpoint fc-port-0
Device 'ddboost-dev8' is already in group 'Test'.
```

Beim Bereitstellen von LUNs über angeschlossene FC-Ports an HBAs kann für Ports „primary“, „secondary“ oder „none“ festgelegt werden. Ein primärer Port für eine Gruppe von LUNs ist der Port, der diese LUNs derzeit bei einer Fabric ankündigt. Ein sekundärer Port (Secondary) ist ein Port, der LUNs bei einem Ausfall des primären Pfads sendet (manuelle Intervention erforderlich). Die Einstellung „None“ wird verwendet, wenn ausgewählte LUNs nicht verfügbar gemacht werden sollen. Die Bereitstellung von LUNs hängt von der SAN-Topologie ab.

10. Überprüfen Sie die Zusammenfassung und nehmen Sie ggf. Änderungen vor. Klicken Sie auf **Finish**, um die Zugriffsgruppe zu erstellen, die in der Liste „DD Boost Access Groups“ angezeigt wird.

    CLI-Entsprechung

    ```
    # scsitarget group show detailed
    ```

Hinweis

Wenn Sie die Einstellungen für eine vorhandene Zugriffsgruppe ändern möchten, wählen Sie diese in der Liste aus und klicken auf Sie auf das Bleistiftsymbol zum Ändern.

Löschen von Zugriffsgruppen

Verwenden Sie die Registerkarte „Fibre Channel“ zum Löschen von Zugriffsgruppen.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD Boost** > **Fibre Channel**.
2. Wählen Sie die zu löschende Gruppe in der Liste „DD Boost Access Groups“ aus.

Hinweis

Sie können keine Gruppe löschen, der Initiatoren zugewiesen sind. Bearbeiten Sie zunächst die Gruppe, um die Initiatoren zu löschen.

---

3. Klicken Sie auf „Delete“ (**X**).

Verwendung von DD Boost auf HA-Systemen

HA bietet nahtloses Failover für jede Anwendung unter Verwendung von DD Boost – d. h., jeder Backup- oder Wiederherstellungsvorgang wird fortgesetzt, ohne dass eine manuelle Intervention erforderlich ist. Alle anderen DD Boost-Benutzerszenarien werden auch auf HA-Systemen unterstützt, wie Managed File Replication (MFR), Distributed Segment Processing (DSP), Filecopy und Dynamic Interface Groups (DIG).

Beachten Sie diesen besonderen Aspekte zur Verwendung von DD Boost auf HA-Systemen:

- Auf HA-fähigen Data Domain-Systemen erfolgen Failover des DD-Servers in weniger als 10 Minuten. Die Recovery von DD Boost-Anwendungen kann jedoch länger dauern, da die Boost-Anwendungs-Recovery erst beginnen kann, wenn das DD-Server-Failover abgeschlossen ist. Darüber hinaus kann die Boost-Anwendungs-Recovery erst starten, wenn die Anwendung die Boost-Bibliothek aufruft.
- DD Boost auf HA-Systemen erfordert, dass die Boost-Anwendungen Boost-HA-Bibliotheken verwenden; für Anwendungen, die Nicht-HA-Boost-Bibliotheken verwenden, ist das Failover nicht nahtlos.
- Es erfolgt ein nahtloses MFR-Failover, wenn Quell- und Zielsystem HA-fähig sind. MFR wird auch auf partiellen HA-Konfigurationen unterstützt (d. h., wenn entweder das Quell- oder das Zielsystem aktiviert ist, aber nicht beide), wenn der Ausfall auf dem HA-fähigen System erfolgt. Detaillierte Informationen finden Sie im *DD Boost for OpenStorage Administration Guide* oder im *DD Boost for Partner Integration Administration Guide*.
- Dynamische Schnittstellengruppen sollten keine IP-Adressen umfassen, die mit der direkten Verbindung zwischen den aktiven und Stand-by-Data Domain-Systemen verknüpft sind.
- DD Boost-Clients müssen konfiguriert werden, um Floating IP-Adressen zu verwenden.

Informationen über die DD Boost-Registerkarten

Dieser Abschnitt enthält Informationen über die DD Boost-Registerkarten in DD System Manager.

Settings

Verwenden Sie die Registerkarte „Settings“, um DD Boost zu aktivieren oder zu deaktivieren, Clients und Benutzer auszuwählen und erweiterte Optionen festzulegen.

Auf der Registerkarte „Settings“ wird der DD Boost-Status („Enabled“ oder „Disabled“) angezeigt. Verwenden Sie die Schaltfläche **Status**, um zwischen **Enabled** und **Disabled** zu wechseln.

Wählen Sie unter **Allowed Clients** die Clients aus, die Zugriff auf das System haben sollen. Managen Sie die Clientliste mithilfe der Schaltflächen **Add**, **Modify** und **Delete**.

Wählen Sie unter **Users with DD Boost Access** die Benutzer aus, die über DD Boost-Zugriff verfügen sollen. Managen Sie die Benutzerliste mithilfe der Schaltflächen **Add**, **Change Password** und **Remove**.

Erweitern Sie den Bereich **Advanced Options**, um anzuzeigen, welche erweiterten Optionen aktiviert sind. Navigieren Sie zu **More Tasks** > **Set Options**, um diese Optionen zurückzusetzen.

Aktive Verbindungen

Verwenden Sie die Registerkarte „Active Connections“, um Informationen über Clients, Schnittstellen und ausgehende Dateien anzuzeigen.

Tabelle 126 Informationen zu verbundenen Clients

Element	Beschreibung
Client	Name des verbundenen Clients.
Idle	Gibt an, ob der Client im Leerlauf ist („Yes“) oder nicht („No“).
CPUs	Anzahl der CPUs des Clients, z. B. 8.
Memory (GiB)	Arbeitsspeichermenge des Clients (in GiB), z. B. 7,8.
Plug-In Version	Version des installierten DD Boost-Plug-ins, z. B. 2.2.1.1.
Betriebssystemversion	Version des installierten Betriebssystems, z. B. Linux 2.6.1 7-1.2142_FC4smp x86_64.
Application Version	Version der installierten Backupanwendung, z. B. NetBackup 6.5.6.
Verschlüsselung	Gibt an, ob die Verbindung verschlüsselt ist („Yes“) oder nicht („No“).
DSP	Gibt an, ob die Verbindung die verteilte Segmentverarbeitung (Distributed Segment Processing, DSP) verwendet oder nicht.
Transport	Typ des verwendeten Transports, z. B. IPv4, IPv6 oder DFC (Fibre Channel).

Tabelle 127 Informationen zu konfigurierten Schnittstellenverbindungen

Element	Beschreibung
Schnittstelle	IP-Adresse der Schnittstelle.
Interface Group	Wählen Sie eine der folgenden Optionen aus: • Name der Schnittstellengruppe. • „None“, wenn die Verbindung in keiner Gruppe Mitglied ist.
Backup	Anzahl der aktiven Backupverbindungen.
Wiederherstellung	Anzahl der aktiven Wiederherstellungsverbindungen.
Replikation	Anzahl der aktiven Replikationsverbindungen.
Synthetic	Anzahl der synthetischen Backups.
Gesamt	Gesamtanzahl aller Verbindungen für die Schnittstelle.

Tabelle 128 Replikationsinformationen für ausgehende Dateien

Element ausgehender Dateien	Beschreibung
Dateiname	Name der ausgehenden Image-Datei.
Target Host	Name des Hosts, der die Datei empfängt.
Logical Bytes to Transfer	Anzahl der logischen Bytes, die übertragen werden.

Tabelle 128 Replikationsinformationen für ausgehende Dateien (Fortsetzung)

Element ausgehender Dateien	Beschreibung
Logical Bytes Transferred	Anzahl der logischen Bytes, die bereits übertragen wurden.
Low Bandwidth Optimization	Anzahl der Bytes mit niedriger Bandbreite, die bereits übertragen wurden.

IP Network

Die Registerkarte „IP Network“ führt konfigurierte Schnittstellengruppen auf. Die Details umfassen Angaben dazu, ob eine Gruppe aktiviert ist, sowie die konfigurierten Clientschnittstellen. Administratoren können das Menü „Interface Group“ dazu verwenden, anzuzeigen, welche Clients einer Schnittstellengruppe zugeordnet sind.

Fibre Channel

Die Registerkarte "Fibre Channel" listet konfigurierte DD Boost-Zugriffsgruppen auf. Verwenden Sie die Registerkarte "Fibre Channel", um Zugriffsgruppen zu erstellen und zu löschen und Initiatoren, Geräte und Endpunkte für DD Boost-Zugriffsgruppen zu konfigurieren.

Speichereinheiten

Verwenden Sie die Registerkarte „Storage Unit“ zum Erstellen, Ändern und Löschen von Speichereinheiten. Um detaillierte Informationen über eine aufgeführte Speichereinheit anzuzeigen, wählen Sie den entsprechenden Namen aus.

Tabelle 129 Storage unit: Detaillierte Informationen

Element	Beschreibung
Existing Storage Units	
Storage Unit Name	Der Name der Speichereinheit.
Pre-Comp Used	Die Menge des vorkomprimierten Speichers, der bereits verwendet wird.
Pre-Comp Soft Limit	Der aktuelle Wert der variablen Quotas für die Speichereinheit.
% of Pre-Comp Soft Limit Used	Der Prozentsatz der verwendeten festen Quotas.
Pre-Comp Hard Limit	Der aktuelle Wert der festen Quotas für die Speichereinheit.
% of Pre-Comp Hard Limit Used	Der Prozentsatz der verwendeten festen Quotas.
Storage Unit Details	Wählen Sie die Speichereinheit in der Liste aus.
Total Files	Die Gesamtanzahl von Dateien auf der Speichereinheit.
Download Files	Ein Link, um Details zur Speichereinheitsdatei im TSV-Format herunterzuladen. Sie müssen Pop-up-Meldungen zulassen, um diese Funktion nutzen zu können.
Compression Ratio	Das erreichte Komprimierungsverhältnis der Dateien.

Tabelle 129 Storage unit: Detaillierte Informationen (Fortsetzung)

Element	Beschreibung
Metadata Size	Der belegte Speicherplatz für Metadateninformationen.
Storage Unit Status	Der aktuelle Status der Speichereinheit (Kombinationen werden unterstützt). Mögliche Statuswerte: • D – gelöscht • RO – nur Lesen • RW – Lesen/Schreiben • RD – Replikationsziel • RLE – DD Retention Lock aktiviert • RLD – DD Retention Lock deaktiviert
Quota-Durchsetzung	Klicken Sie auf „Quota“, um die Seite „Data Management“ zu öffnen, die die von MTrees verwendeten Werte/ Prozentwerte für das feste und variable Quota aufführt.
Quota Summary	Der Prozentsatz des verwendeten festen Grenzwerts.
Original Size	Die Größe der Datei vor der Komprimierung.
Global Compression Size	Die Gesamtgröße nach der globalen Komprimierung der Dateien in der Speichereinheit, als sie gespeichert wurden.
Locally Compressed Size	Die Gesamtgröße nach der lokalen Komprimierung der Dateien in der Speichereinheit, als sie gespeichert wurden.

KAPITEL 15

DD Virtual Tape Library

Inhalt dieses Kapitels:

Übersicht über DD Virtual Tape Library

Data Domain Virtual Tape Library (DD VTL) ist ein festplattenbasiertes Backupsystem, das die Verwendung physischer Bänder emuliert. Die VTL ermöglicht Backupanwendungen, über Funktionen, die nahezu identisch zu einer physischen Bandbibliothek sind, eine Verbindung zum DD-Systemspeicher herzustellen und diesen zu managen.

Virtuelle Bandlaufwerke sind für Backup-Software zugänglich wie physische Bandlaufwerke. Nach der Erstellung dieser Laufwerke in einer DD VTL werden sie der Backupsoftware als SCSI-Bandlaufwerke angezeigt. Die DD VTL selbst wird der Backupsoftware als SCSI-Robotergerät angezeigt, das über Standardtreiberschnittstellen zugänglich ist. Allerdings wird die Verschiebung von Medienwechslern und Backup-Images durch die Backupsoftware gemanagt – nicht über das DD-System, das als DD VTL konfiguriert ist.

Die folgenden Begriffe haben eine besondere Bedeutung, wenn sie mit DD VTL verwendet werden:

- *Bibliothek*: Eine Bibliothek emuliert eine physische Bandbibliothek mit Laufwerken, Wechsler, CAPs (Cartridge Access Ports) und Steckplätzen (Kassettensteckplätzen).
- *Band*: Ein Band wird als Datei dargestellt. Bänder können aus einem Vault in eine Bibliothek importiert werden. Bänder können aus einer Bibliothek in den Vault exportiert werden. Bänder können innerhalb einer Bibliothek zwischen Laufwerken, Steckplätzen und CAPs verschoben werden.
- *Pool*: Ein Pool ist eine Sammlung von Bändern, die einem Verzeichnis auf einem Dateisystem zugeordnet ist. Pools werden verwendet, um Bänder an ein Ziel zu replizieren. Sie können verzeichnisbasierte Pools in MTree-basierte Pools konvertieren, um die zahlreicheren Funktionen von MTrees zu nutzen.
- *Vault*: Der Vault enthält Bänder, die von keiner Bibliothek verwendet werden. Bänder befinden sich entweder in einer Bibliothek oder im Vault.

DD VTL wurde mit spezieller Backupsoftware und speziellen Hardwarekonfigurationen getestet und wird von diesen unterstützt. Weitere Informationen finden Sie im entsprechenden *Backupkompatibilitätsleitfaden* auf der Onlinesupport-Website.

DD VTL unterstützt die gleichzeitige Verwendung der Bandbibliothek- und Dateisystemschnittstellen (NFS/CIFS/DD Boost).

Wenn DR (Disaster Recovery) erforderlich ist, können Pools und Bänder mithilfe von DD Replicator an ein DD-Remotesystem repliziert werden.

Sie können Bänder mit der DD Retention Lock Governance-Software sperren, um die Daten auf den Bändern vor Änderungen zu schützen.

Hinweis

Derzeit unterstützt Data Domain bei 16 Gbit/s Fabric- und Punkt-zu-Punkt-Topologien. Bei anderen Topologien können Probleme auftreten.

Planen einer DD VTL

Für die DD VTL-Funktion (Virtual Tape Library, virtuelle Bandbibliothek) gelten sehr spezifische Anforderungen, wie ordnungsgemäße Lizenzierung, Schnittstellenkarten,

Benutzerberechtigungen usw. Diese Anforderungen werden im Folgenden ausführlich mit Empfehlungen aufgeführt.

- Eine entsprechende DD VTL-Lizenz
  - DD VTL ist eine lizenzierte Funktion und erfordert die Verwendung von NDMP (Network Data Management Protocol) über IP (Internet Protocol) oder DD VTL über FC (Fibre Channel).
  - Eine zusätzliche Lizenz (I/OS-Lizenz) ist für IBM i-Systeme erforderlich.
  - Wenn Sie eine DD VTL über DD System Manager hinzufügen, wird automatisch die DD VTL-Funktion deaktiviert und aktiviert.
- Eine installierte FC-Schnittstellenkarte oder DD VTL, die so konfiguriert ist, dass sie NDMP verwendet.
  - Wenn die DD VTL-Kommunikation zwischen einem Backupserver und einem DD-System durch die FC-Schnittstelle erfolgt, muss auf dem DD-System eine FC-Schnittstellenkarte installiert sein. Beachten Sie Folgendes: Wann immer eine FC-Schnittstellenkarte von einem DD-System entfernt wird (oder darin geändert wird), muss jede DD VTL-Konfiguration aktualisiert werden, die dieser Karte zugeordnet ist.
  - Wenn die DD VTL-Kommunikation zwischen einem Backupserver und einem DD-System über NDMP erfolgt, ist keine FC-Schnittstellenkarte erforderlich. Sie müssen jedoch die TapeServer-Zugriffsgruppe konfigurieren. Zudem gelten bei Verwendung von NDMP keine der Initiator- und Portfunktion.
  - Der Netzfilter muss konfiguriert werden, damit der NDMP-Client Informationen an das DD-System senden kann. Führen Sie den Befehl **`net filter add operation allow clients <client-IP-address>`** aus, um Zugriff für den NDMP-Client zu ermöglichen.
    - Führen Sie für zusätzliche Sicherheit den Befehl **`net filter add operation allow clients <client-IP-address> interfaces <DD-interface-IP-address>`** aus.
    - Fügen Sie dem Befehl die Option **`seq-id 1`** hinzu, um diese Regel vor anderen Netzfilterregeln durchzusetzen.
- Eine MIndestdatensatzgröße (Blockgröße) der Backupsoftware.
  - Es wird dringend empfohlen, festzulegen, dass die Backupsoftware eine Mindestgröße für Datensätze (Blöcke) von 64 KiB oder mehr verwendet. Größere Datensätze ergeben üblicherweise eine höhere Performance und bessere Datenkomprimierung.
  - Je nach Ihrer Backupanwendung werden Daten, die mit der ursprünglichen Größe geschrieben werden, unter Umständen unlesbar, wenn Sie die Größe nach der Erstkonfiguration ändern.
- Den entsprechenden Benutzerzugriff auf das System.
  - Bei einfachen Bandvorgängen und Monitoring ist nur eine Benutzeranmeldung erforderlich.
  - Um DD VTL-Services zu aktivieren und zu konfigurieren und andere Konfigurationsaufgaben durchzuführen, ist eine sysadmin-Anmeldung erforderlich.

DD VTL-Beschränkungen

Prüfen Sie vor dem Einrichten oder Verwenden einer DD VTL die Beschränkungen hinsichtlich Größe, Steckplätzen usw.

- I/O-Größe: Die maximal unterstützte I/O-Größe für alle DD-Systeme mit DD VTL ist 1 MB.
- Bibliotheken: DD VTL unterstützt maximal 64 Bibliotheken pro DD-System (d. h. 64 DD VTL-Instanzen auf jedem DD-System).
- Initiatoren: DD VTL unterstützt bis zu 1.024 Initiatoren oder WWPNs (weltweite Portnamen) pro DD-System.
- Bandlaufwerke: Informationen über Bandlaufwerke finden Sie im nächsten Abschnitt.
- Daten-Streams – Informationen zu Daten-Streams werden in der folgenden Tabelle angezeigt.

Tabelle 130 An ein Data Domain-System gesendete Datenstreams

Modell	RAM/NVRAM	Backupschreibstreams	Backuplesestreams	Repl[a]-Quellstreams	Repl[a]-Zielstreams	Gemischt
DD140, DD160, DD610	4 GB oder 6 GB/0,5 GB	16	4	15	20	w<= 16 ; r<= 4 ReplSrc<=15; ReplDest<=20; ReplDest+w<=16; w+r+ReplSrc <=16;Total<=20
DD620, DD630, DD640	8 GB/0,5 GB oder 1 GB	20	16	30	20	w<=20; r<=16; ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; Total<=30
DD640, DD670	16 GB oder 20 GB/1 GB	90	30	60	90	w<=90; r<=30; ReplSrc<=60; ReplDest<=90; ReplDest+w<=90; Total<=90
DD670, DD860	36 GB/1 GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD860	72 GB[b]/1 GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD890	96 GB/2 GB	180	50	90	180	w<=180; r<=50; ReplSrc <=90;ReplDest<=180; ReplDest +w<=180; Total<=180
DD990	128 oder 256 GB[b]/4 GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD2200	8 GB	20	16	16	20	w<=20; r<=16; ReplSrc<=16; ReplDest<=20; ReplDest+w<=20; Total<=20
DD2200	16 GB	60	16	30	60	w<=60; r<=16; ReplSrc<=30; ReplDest<=60; ReplDest+w<=60; Total<=60

Tabelle 130 An ein Data Domain-System gesendete Datenstreams (Fortsetzung)

Modell	RAM/NVRAM	Backupschreibstreams	Backuplesestreams	Repl[a]-Quellstreams	Repl[a]-Zielstreams	Gemischt
DD2500	32 GB oder 64 GB/2 GB	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; Total<=180
DD4200	128 GB[b]/4 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD4500	192 GB[b]/4 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD7200	128 oder 256 GB[b]/4 GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD9500	256/512 GB	1.885	300	540	1.080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest +w<=1080; Total<=1885
DD9800	256/768 GB	1.885	300	540	1.080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest +w<=1080; Total<=1885
DD6300	48/96 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD6800	192 GB	400	110	220	400	w<=400; r<=110; ReplSrc<=220; ReplDest<=400; ReplDest +w<=400; Total<=400
DD9300	192/384 GB	800	220	440	800	w<=800; r<=220; ReplSrc<=440; ReplDest<=800; ReplDest +w<=800; Total<=800
Data Domain Virtual Edition (DD VE)	6 TB oder 8 TB oder 16 TB/ 0,5 TB oder 32 TB oder 48 TB oder 64 TB oder 96 TB	16	4	15	20	w<= 16 ; r<= 4 ReplSrc<=15; ReplDest<=20; ReplDest+w<=16; w+r+ReplSrc <=16;Total<=20

a. DirRepl, OptDup, MTreeRepl-Streams
b. Die Data Domain Extended Retention-Softwareoption ist für diese Geräte nur mit erweitertem (maximalem) Arbeitsspeicher verfügbar.

- Steckplätze: DD VTL unterstützt maximal:
  - 32.000 Steckplätze pro Bibliothek
  - 64.000 Steckplätze pro DD-System

  Das DD-System fügt automatisch Steckplätze hinzu, um sicherzustellen, dass die Anzahl der Steckplätze gleich oder größer als die Anzahl der Laufwerke ist.

Hinweis

Einige Gerätetreiber (z. B. IBM AIX Atape-Gerätetreiber) begrenzen die Bibliothekskonfiguration auf bestimmte Laufwerks-/Steckplatzwerte, die möglicherweise stärker einschränken als die vom DD-System unterstützten Werte. Backupanwendungen und von diesen Anwendungen verwendete Laufwerke können von diesen Beschränkungen betroffen sein.

- CAPs (Cartridge Access Ports): DD VTL unterstützt maximal:
  - 100 CAPs pro Bibliothek
  - 1.000 CAPs pro DD-System

Anzahl der von einer DD VTL unterstützten Laufwerke

Die maximale Anzahl der Laufwerke, die von einer DD VTL unterstützt wird, hängt von der Anzahl der CPU-Kerne und der Menge des installierten Arbeitsspeichers (RAM und ggf. NVRAM) auf einem DD-System ab.

Hinweis

Es gibt keine Verweise auf Modellnummern in dieser Tabelle, da es zahlreiche Kombinationen von CPU-Kernen und Arbeitsspeicher für jedes Modell gibt und die Anzahl der unterstützten Laufwerke *ausschließlich* von den CPU-Kernen und -Arbeitsspeichern abhängt und nicht vom bestimmten Modell selbst.

Tabelle 131 Anzahl der von einer DD VTL unterstützten Laufwerke

Anzahl der CPU-Kerne	RAM (GB)	NVRAM (GB)	Maximale Anzahl unterstützter Laufwerke
Weniger als 32	4 oder weniger	NA	64
	Mehr als 4 bis 38	NA	128
	39 bis 128	NA	256
	Mehr als 128	NA	540
32 bis 39	Bis zu 128	Weniger als 4	270
	Bis zu 128	4 oder mehr	540
	Mehr als 128	NA	540
40 bis 59	NA	NA	540
60 oder mehr	NA	NA	1.080

Bänderstrichcodes

Wenn Sie ein Band erstellen, müssen Sie einen einzigartigen *Strichcode* zuweisen (keine doppelten Strichcodes, da dies zu einem unvorhersehbarem Verhalten führen kann). Jeder Strichcode besteht aus acht Zeichen: Die ersten sechs Zeichen sind Zahlen oder Großbuchstaben (0-9, A-Z) und die beiden letzten Zeichen sind der Bandcode für die unterstützte Bandart, wie in der folgenden Tabelle gezeigt.

Hinweis

Obwohl ein DD VTL-Strichcode aus acht Zeichen besteht, können entweder sechs oder acht Zeichen an eine Backupanwendung übertragen werden, je nach Wechslertyp.

Tabelle 132 Bandcodes nach Bandart

Bandtyp	Standardkapazität (wenn nicht angemerkt)	Bandcode
LTO-1	100 GiB	L1
LTO-1	50 GiB (nicht standardmäßig)	LA[a]
LTO-1	30 GiB (nicht standardmäßig)	LB
LTO-1	10 GiB (nicht standardmäßig)	LC
LTO-2	200 GiB	L2
LTO-3	400 GiB	L3
LTO-4	800 GiB	L4
LTO-5 (Standard)	1,5 TiB	L5

a. Für TSM verwenden Sie den L2-Bandcode, wenn der LA-Code ignoriert wird.

Für mehrere Bandbibliotheken werden Strichcodes automatisch inkrementell erhöht, wenn das sechste Zeichen (direkt vor dem„ L“) eine Ziffer ist. Wenn ein Überlauf (9 bis 0) auftritt, verschiebt sich die Nummerierung um eine Position nach links. Wenn das nächste zu erhöhende Zeichen ein Buchstabe ist, wird die inkrementelle Erhöhung gestoppt. Hier einige Beispielstrichcodes mit Beispielen zu der inkrementellen Erhöhung:

- 000000L1 erstellt Bänder mit einer Kapazität von 100 GiB und kann eine Anzahl von bis zu 100.000 Bändern akzeptieren (von 000000 bis 99999).
- AA0000LA erstellt Bänder mit einer Kapazität von 50 GiB und kann eine Anzahl von bis zu 10.000 Bändern akzeptieren (von 0000 bis 9999).
- AAAA00LB erstellt Bänder mit einer Kapazität von 30 GiB und kann eine Anzahl von bis zu 100 Bändern akzeptieren (von 00 bis 99).
- AAAAAALC erstellt ein Band mit einer Kapazität von 10 GB. Es kann nur ein Band mit diesem Namen erstellt werden.
- AAA350L1 erstellt Bänder mit einer Kapazität von 100 GiB und kann eine Anzahl von bis zu 650 Bändern akzeptieren (von 350 bis 999).
- 000AAALA erstellt ein Band mit einer Kapazität von 50 GB. Es kann nur ein Band mit diesem Namen erstellt werden.
- 5M7Q3KLB erstellt ein Band mit einer Kapazität von 30 GB. Es kann nur ein Band mit diesem Namen erstellt werden.

LTO-Bandlaufwerkskompatibilität

In Ihrer Konfiguration können sich verschiedene Generationen der LTO-Technologie (Linear Tape-Open) befinden. Informationen zur Kompatibilität zwischen diesen Generationen sind in einer Tabelle aufgeführt.

In dieser Tabelle gelten die folgenden Definitionen:

- RW: lese- und schreibkompatibel
- R: nur lesekompatibel
- —: nicht kompatibel

Tabelle 133 LTO-Bandlaufwerkskompatibilität

Bandformat	LTO-5	LTO-4	LTO-3	LTO-2	LTO-1
LTO-5	RW				
LTO-4	RW	RW	–	–	–
LTO-3	R	RW	RW	–	–
LTO-2		R	RW	RW	–
LTO-1		–	R	RW	RW

Einrichten einer DD VTL

Verwenden Sie zum Einrichten einer einfachen DD VTL den Configuration Wizard, wie im Abschnitt *Erste Schritte* beschrieben.

Eine vergleichbare Dokumentation finden Sie im *Data Domain Operating System Initial Configuration Guide*.

Fahren Sie dann mit den folgenden Themen fort, um die DD VTL zu aktivieren, Bibliotheken zu erstellen sowie Bänder zu erstellen und zu importieren.

HA-Systeme und DD VTL

HA-Systeme sind kompatibel mit DD VTL; wenn ein DD VTL-Job jedoch während eines Failover durchgeführt wird, muss der Job manuell neu gestartet werden, nachdem das Failover abgeschlossen ist.

Der *Backupkompatibilitätsleitfaden für Data Domain Operating System* bietet zusätzliche Details zu HBA-, Switch-, Firmware- und Treiberanforderungen für die DD VTL-Verwendung in einer HA-Umgebung.

DD VTL-Band-zu-Cloud

DD VTL unterstützt das Speichern des VTL-Vault im DD Cloud Tier-Speicher. Um diese Funktionalität zu verwenden, muss das Data Domain-System eine unterstützte Cloud Tier-Konfiguration sein und eine Cloud Tier-Lizenz neben der VTL-Lizenz aufweisen.

Konfigurieren und lizenzieren Sie den DD Cloud Tier-Speicher vor dem Konfigurieren von DD VTL, um Cloudspeicher für den Vault zu verwenden. DD Cloud Tier auf Seite 499 enthält zusätzliche Informationen über die Anforderungen für DD Cloud Tier und die Konfiguration von DD Cloud Tier.

Die Anforderungen in Bezug auf FC und Netzwerkschnittstelle für VTL sind für cloudbasierten und lokalen Vault-Speicher gleich. DD VTL erfordert keine spezielle Konfiguration für die Verwendung des Cloudspeichers für den Vault. Wählen Sie bei der Konfiguration von DD VTL den Cloudspeicher als Vault-Speicherort. Beim Arbeiten mit einem cloudbasierten Vault gibt es jedoch einige Datenmanagementoptionen, die einzigartig für den cloudbasierten Vault sind. Weitere Informationen erhalten Sie unter Arbeiten mit dem cloudbasierten Vault auf Seite 407.

Managen einer DD VTL

Sie können eine DD VTL mit der Data Domain System Manager(DD System Manager)- oder Data Domain Operating System(DD OS)-Befehlszeilenoberfläche (CLI, Command Line Interface) managen. Nach der Anmeldung können Sie den Status des DD VTL-Prozesses und Lizenzinformationen prüfen und Optionen prüfen und konfigurieren.

Anmelden

Um eine grafische Benutzeroberfläche (GUI) zu verwenden und Ihre DD Virtual tape Library (DD VTL) zu managen, melden Sie sich bei DD System Manager an.

CLI-Entsprechung

Sie können sich auch bei der Befehlszeilenoberfläche anmelden:

```
login as: Sysadmin
Data Domain OS
Using keyboard-interactive authentication.
Password:
```

Aktivieren des SCSI-Ziel Daemons (nur Befehlszeilenoberfläche)

Wenn Sie sich über die Befehlszeilenoberfläche anmelden, müssen Sie den scsitarget-Daemon (Fibre-Channel-Service) aktivieren. Dieser Daemon wird während der DD VTL- bzw. DD Boost-FC-Aktivierungsauswahl in DD System Manager aktiviert. In der Befehlszeilenoberfläche müssen diese Prozesse getrennt aktiviert werden.

```
# scsitarget enable
Please wait ...
SCSI Target subsystem is enabled.
```

Zugriff auf DD VTL

Klicken Sie im Menü links von DD System Manager auf **Protocols** > **VTL**.

Status

Im Bereich **Virtual Tape Libraries** > **VTL Service** sehen Sie den Status des DD VTL-Prozesses oben, beispielsweise **Enabled: Running**. Der erste Teil des Status lautet **Enabled** (ein) oder **Disabled** (aus). Der zweite Teil besteht aus einem der folgenden Prozessstatus.

Tabelle 134 DD VTL-Prozessstatus

State	Beschreibung
Running	Der DD VTL-Prozess ist aktiviert und aktiv (grün dargestellt).
Starting	Der DD VTL-Prozess wird gestartet.
Stopping	Der DD VTL-Prozess wird beendet.
Stopped	Der DD VTL-Prozess ist deaktiviert (rot angezeigt).
Timing out	Der DD VTL-Prozess ist abgestürzt und versucht einen automatischen Neustart.

Tabelle 134 DD VTL-Prozessstatus (Fortsetzung)

State	Beschreibung
Stuck	Nach mehreren fehlgeschlagenen automatischen Neustarts ist der DD VTL-Prozess nicht in der Lage, normal herunterzufahren, sodass versucht wird, ihn zu beenden.

DD VTL-Lizenz
Die Zeile „VTL License“ zeigt Ihnen, ob Ihre DD VTL-Lizenz angewendet wurde. Wenn sie „Unlicensed“ lautet, wählen Sie **Add License**. Geben Sie Ihren Lizenzschlüssel im Dialogfeld „Add License Key“ ein. Klicken Sie auf **Next** und auf **OK**.

Hinweis

Alle Lizenzinformationen sollten im Rahmen des werkseitigen Konfigurationsprozesses vorhanden sein; wenn die DD VTL jedoch später erworben wurde, war der DD VTL-Lizenzschlüssel zu diesem Zeitpunkt evtl. nicht verfügbar.

CLI-Entsprechung
Über die Befehlszeilenoberfläche können Sie auch prüfen, ob die DD VTL-Lizenz installiert wurde:

```
# license show
## License Key                   Feature
--    ------------------        -----------
1     DEFA-EFCD-FCDE-CDEF        Replication
2     EFCD-FCDE-CDEF-DEFA        VTL
--    ------------------        -----------
```

Wenn keine Lizenz vorhanden ist, können Sie der Dokumentation zur jeweiligen Einheit (Übersichtskarte zur schnellen Installation) entnehmen, welche Lizenzen erworben wurden. Geben Sie den folgenden Befehl ein, um den Lizenzschlüssel anzugeben.

```
# license add license-code
```

I/OS-Lizenz (für IBM i-Benutzer)
Für Kunden von IBM i steht in der I/OS License-Zeile, ob Ihre I/OS-Lizenz angewendet wurde. Wenn sie „Unlicensed“ lautet, wählen Sie **Add License**. Sie müssen eine gültige I/OS-Lizenz in einem der folgenden Formate eingeben: `xxxx-xxxx-xxxx-xxxx` oder `xxxx-xxxx-xxxx-xxxx-xxxx`. Ihre I/OS-Lizenz muss installiert werden, bevor eine Bibliothek und die Laufwerke zur Verwendung auf einem IBM i-System erstellt werden. Klicken Sie auf **Next** und auf **OK**.

Aktivieren einer DD VTL

Wenn die DD VTL aktiviert wird, wird der WWN des Data Domain-HBA an die Kunden-Fabric übertragen. Zudem werden alle Bibliotheken und Bibliothekslaufwerke aktiviert. Wenn ein Weiterleitungsplan in Form eines Prozesses zur Änderungskontrolle benötigt wird, muss dieser Prozess aktiviert werden, um Zoning zu ermöglichen.

Vorgehensweise

1. Sorgen Sie dafür, dass Sie eine DD VTL-Lizenz haben und dass das Dateisystem aktiviert ist.
2. Wählen Sie **Virtual Tape Libraries** > **VTL Service**.
3. Wählen Sie rechts vom Bereich „Status“ **Enable** aus.
4. Wählen Sie im Dialogfeld „Enable Service“ **OK** aus.

5. Wenn die DD VTL aktiviert wurde, beachten Sie, dass sich der Status ändert in **Enabled: Running** in Grün. Beachten Sie außerdem, dass die konfigurierten DD VTL-Optionen im Bereich „Option Defaults“ angezeigt werden.

   CLI-Entsprechung

   ```
   # vtl enable Starting VTL, please wait ... VTL ist aktiviert.
   ```

Deaktivieren einer DD VTL

Beim Deaktivieren einer DD VTL werden alle Bibliotheken geschlossen und der DD VTL-Prozess wird heruntergefahren.

Vorgehensweise

1. Wählen Sie **Virtual Tape Libraries** > **VTL Service**.
2. Wählen Sie rechts neben dem Bereich „Status“ die Option **Disable**.
3. Wählen Sie im Dialogfeld „Disable Service“ **OK**.
4. Beachten Sie, dass sich der Status nach dem Deaktivieren der DD VTL zu **Disabled: Stopped** geändert hat und rot dargestellt wird.

   CLI-Entsprechung

   ```
   # vtl disable
   ```

Standardwerte der DD VTL-Option

Der Bereich „Option Default“ der Seite „VTL Service“ zeigt die aktuellen Einstellungen für standardmäßige DD VTL-Optionen (auto-eject, auto-offline und barcode-length) an, die Sie konfigurieren können.

Im Bereich **Virtual Tape Libraries** > **VTL Service** werden die aktuellen Standardoptionen für Ihre DD VTL angezeigt. Wählen Sie **Configure**, um diese Werte zu ändern.

Tabelle 135 Optionsstandardwerte

Element	Beschreibung
Eigenschaft	Listet die konfigurierten Optionen auf: • auto-eject • auto-offline • barcode-length
Wert	Legt den Wert für jede konfigurierte Option fest: • auto-eject: default (disabled), enabled oder disabled • auto-offline: default (disabled), enabled oder disabled • barcode-length: default (8), 6 oder 8

Konfigurieren von DD VTL-Standardoptionen

Sie können DD VTL-Standardoptionen beim Hinzufügen einer Lizenz, beim Erstellen einer Bibliothek oder zu einem späteren Zeitpunkt konfigurieren.

Hinweis

DD VTLs sind standardmäßig zugewiesene globale Optionen und diese Optionen werden aktualisiert, sobald sich globale Optionen ändern, es sei denn, Sie ändern sie manuell über diese Methode.

Vorgehensweise

1. Wählen Sie **Virtual Tape Libraries** > **VTL Service**.
2. Wählen Sie im Bereich "Option Defaults" die Option **Configure**. Ändern Sie im Dialogfeld "Configure Default Options" eine oder alle standardmäßigen Optionen.

Tabelle 136 DD VTL-Standardoptionen

Option	Werte	Anmerkungen
auto-eject	default (disabled), enable oder disable	Die Aktivierung von auto-eject führt dazu, dass jedes Band, das in einen CAP (Cartridge Access Port) platziert wird, automatisch zum virtuellen Vault verschoben wird, mit Ausnahme der folgenden Fälle: • Das Band kam aus dem Vault, in diesem Fall bleibt das Band im CAP. • Der Befehl `ALLOW_MEDIUM_REMOVAL` wurde mit einem 0-Wert (false) an die Bibliothek ausgegeben, um das Entfernen des Mediums aus dem CAP für die Außenwelt zu verhindern.
auto-offline	default (disabled), enable oder disable	Bei der Aktivierung von auto-offline wird ein Laufwerk automatisch offline geschaltet, bevor ein Vorgang zum Verschieben von Bändern durchgeführt wird.
barcode-length	default (8), 6 oder 8 [automatisch festgelegt auf 6 für L180, RESTORER-L180 und DDVTL-Wechslermodelle]	Obwohl ein DD VTL Barcode aus 8 Zeichen besteht, können entweder 6 oder 8 Zeichen an eine Backupanwendung

Tabelle 136 DD VTL-Standardoptionen (Fortsetzung)

Option	Werte	Anmerkungen
		übertragen werden, je nach Wechslertyp.

3. Wählen Sie **OK** aus.
4. Um alle diese Serviceoptionen zu deaktivieren, wählen Sie **Reset to Factory**. Die Werte werden umgehend auf die werkseitigen Standardwerte zurückgesetzt.

Arbeiten mit Bibliotheken

Eine Bibliothek emuliert eine physische Bandbibliothek mit Laufwerken, Wechsler, CAPs (Cartridge Access Ports) und Steckplätzen (Kassettensteckplätzen). Wenn Sie **Virtual Tape Libraries** > **VTL Service** > **Libraries** auswählen, werden detaillierte Informationen zu allen konfigurierten Bibliotheken angezeigt.

Tabelle 137 Informationen zur Bibliothek

Element	Beschreibung
Name	Name einer konfigurierten Bibliothek
Drives	Anzahl der Laufwerke, die in der Bibliothek konfiguriert sind
Slots	Anzahl der in der Bibliothek konfigurierten Steckplätze
CAPs	Anzahl der in der Bibliothek konfigurierten CAPs (Cartridge Access Ports)

Über das Menü „More Tasks“ können Sie Bibliotheken erstellen und löschen sowie nach Bändern suchen.

Erstellen von Bibliotheken

DD VTL unterstützt maximal 64 Bibliotheken pro System, d. h. 64 gleichzeitig aktive virtuelle Bandbibliotheksinstanzen auf jedem DD-System.

Vorgehensweise

1. Wählen Sie **Virtual Tape Libraries** > **VTL Service** > **Libraries** aus.
2. Wählen Sie **More Tasks** > **Library** > **Create**.
3. Geben Sie im Dialogfeld „Create Library“ die folgenden Informationen ein:

Tabelle 138 Dialogfeld „Create Library“

Feld	Benutzereingabe
Library Name	Geben Sie einen Namen mit einer Länge zwischen 1 und 32 alphanumerischen Zeichen ein.
Number of Drives	Geben Sie die Anzahl der Laufwerke ein (1 bis 98, siehe Anmerkung). Die Anzahl der zu erstellenden Laufwerke entspricht der Anzahl der Datenstreams, die in eine Bibliothek geschrieben werden.

Tabelle 138 Dialogfeld „Create Library“ (Fortsetzung)

Feld	Benutzereingabe
	Hinweis Die maximale Anzahl der Laufwerke, die von einer DD VTL unterstützt wird, hängt von der Anzahl der CPU-Kerne und der Menge des installierten Arbeitsspeichers (RAM und ggf. NVRAM) auf einem DD-System ab.
Drive Model	Wählen Sie das gewünschte Modell aus der Drop-down-Liste aus: • IBM-LTO-1 • IBM-LTO-2 • IBM-LTO-3 • IBM-LTO-4 • IBM-LTO-5 (Standard) • HP-LTO-3 • HP-LTO-4 Laufwerkstypen oder Medientypen dürfen in einer Bibliothek nicht gemischt verwendet werden, da dies zu unerwarteten Ergebnissen und/oder Fehlern beim Backupvorgang führen kann.
Number of Slots	Geben Sie die Anzahl der Steckplätze der Bibliothek ein. Im Folgenden sind einige Aspekte aufgeführt, die Sie berücksichtigen sollten: • Die Anzahl der Steckplätze muss größer oder gleich der Anzahl der Laufwerke sein. • Pro Bibliothek dürfen bis zu 32.000 Steckplätze verwendet werden. • Pro System dürfen bis zu 64.000 Steckplätze verwendet werden. • Sorgen Sie dafür, dass genügend Steckplätze vorhanden sind, sodass Bänder in der DD VTL bleiben und nicht in einen Vault exportiert werden müssen, um eine Neukonfiguration von DD VTL zu vermeiden und den Managementoverhead zu reduzieren. • Berücksichtigen Sie alle Anwendungen, die nach der Anzahl der Steckplätze lizenziert wurden. Für eine übliche 100-GB-Kassette in einem DD580-System sollten Sie beispielsweise 5000 Steckplätze konfigurieren. Das ist für bis zu 500 TB ausreichend (entsprechend komprimierbare Daten vorausgesetzt).
Number of CAPs	(Optional) Geben Sie die Anzahl der CAPs (Cartridge Access Ports) ein.

Tabelle 138 Dialogfeld „Create Library“ (Fortsetzung)

Feld	Benutzereingabe
	• Pro Bibliothek dürfen bis zu 100 Steckplätze verwendet werden. • Pro System dürfen bis zu 1000 Steckplätze verwendet werden. Weitere Informationen hierzu finden Sie in der Dokumentation zu Ihrer jeweiligen Backup-Softwareanwendung auf der Onlinesupport-Website.
Changer Model Name	Wählen Sie das gewünschte Modell aus der Drop-down-Liste aus: • L180 (Standard) • RESTORER-L180 • TS3500 (das für IBMi-Bereitstellungen zu verwenden ist) • I2000 • I6000 • DDVTL Weitere Informationen hierzu finden Sie in der Dokumentation zu Ihrer jeweiligen Backup-Softwareanwendung auf der Onlinesupport-Website. Informationen zur Kompatibilität von emulierten Bibliotheken in unterstützte Software finden Sie in der Supportmatrix zu DD VTL.
Optionen	
auto-eject	default (disabled), enable, disable
auto-offline	default (disabled), enable, disable
barcode-length	default (8), 6, 8 [automatisch festgelegt auf 6 für L180, RESTORER-L180 und DDVTL-Wechslermodelle]

4. Wählen Sie **OK** aus.

   Nachdem im Statusdialogfeld „Create Library“ der Status **Completed** angezeigt wird, wählen Sie **OK** aus.

   Die neue Bibliothek wird unter dem Bibliothekssymbol in der VTL-Servicestruktur angezeigt und die von Ihnen konfigurierten Optionen als Symbole unter der Bibliothek. Durch Auswahl der Bibliothek werden im Informationsbereich Details zur Bibliothek angezeigt.

   Beachten Sie, dass der Zugriff auf virtuelle Bandbibliotheken und Laufwerke durch Zugriffsgruppen verwaltet wird.

CLI-Entsprechung

```
# vtl add NewVTL model L180 slots 50 caps 5
This adds the VTL library, NewVTL. Use 'vtl show config NewVTL'
to view it.

# vtl drive add NewVTL count 4 model IBM-LTO-3
This adds 4 IBM-LTO-3 drives to the VTL library, NewVTL.
```

Löschen von Bibliotheken

Wenn sich ein Band in einem Laufwerk innerhalb einer Bibliothek befindet und diese Bibliothek gelöscht wird, wird das Band in den Vault verschoben. Der Pool des Bands ändert sich jedoch nicht.

Vorgehensweise

1. Wählen Sie **Virtual Tape Libraries** > **VTL Service** > **Libraries** aus.
2. Wählen Sie **More Tasks** > **Library** > **Delete**.
3. Aktivieren Sie im Dialogfeld „Delete Libraries“ das Kontrollkästchen der zu löschenden Elemente oder bestätigen Sie die Auswahl:
   - Der Name jeder Bibliothek oder
   - Bibliotheksnamen, um alle Bibliotheken zu löschen
4. Klicken Sie auf **Next**.
5. Überprüfen Sie die zu löschenden Bibliotheken und wählen Sie in den Bestätigungsdialogfeldern **Submit** aus.
6. Wenn im Dialogfeld „Delete Libraries Status“ `Completed` angezeigt wird, wählen Sie **Close** aus. Die ausgewählten Bibliotheken werden aus der DD VTL gelöscht.

CLI-Entsprechung

```
# vtl del OldVTL
```

Suchen nach Bändern

Für die Suche nach Bändern können verschiedene Kriterien wie Speicherort, Pool und/oder Strichcode verwendet werden.

Vorgehensweise

1. Wählen Sie **Virtual Tape Libraries** oder **Pools**.
2. Wählen Sie den zu durchsuchenden Bereich aus (Bibliothek, Vault, Pool).
3. Wählen Sie **More Tasks** > **Tapes** > **Search**.
4. Geben Sie im Dialogfeld „Search Tapes“ Informationen über die die Bänder ein, nach denen gesucht werden soll.

Tabelle 139 Dialogfeld „Search Tapes“

Feld	Benutzereingabe
Location	Geben Sie einen Speicherort ein oder behalten Sie den Standardwert („All“) bei.
Pools bilden	Wählen Sie den Namen des Pools aus, der nach dem Band durchsucht werden soll. Wenn keine Pools erstellt wurden, verwenden Sie den Standardpool.
Strichcode	Geben Sie einen eindeutigen Strichcode an oder behalten Sie den Standardwert (*) bei, damit eine Gruppe von Bändern zurückgegeben wird. Für Strichcodes können Sie die Platzhalter ? und * verwenden, wobei ? mit einem einzigen Zeichen und * mit 0 oder mehr Zeichen übereinstimmt.

Tabelle 139 Dialogfeld „Search Tapes“ (Fortsetzung)

Feld	Benutzereingabe
Count	Geben Sie ein, wie viele Bänder maximal an Sie zurückgegeben werden sollen. Wenn Sie dieses Feld leer lassen, wird der Standardwert (*) für Strichcodes verwendet.

5. Wählen Sie **Search**.

Arbeiten mit einer ausgewählten Bibliothek

Wählen Sie **Virtual Tape Libraries** > **VTL Service** > **Libraries** > *library*, um detaillierte Informationen für eine ausgewählte Bibliothek anzuzeigen.

Tabelle 140 Geräte

Element	Beschreibung
Gerät	Die Elemente in der Bibliothek, wie Laufwerke, Steckplätze und CAPs (Cartridge Access Ports).
Loaded	Die Anzahl der Geräte mit geladenen Medien.
Empty	Die Anzahl der Geräte ohne geladene Medien.
Gesamt	Die Gesamtanzahl der geladenen und leeren Geräte.

Tabelle 141 Optionen

Eigenschaft	Wert
auto-eject	enabled oder disabled
auto-offline	enabled oder disabled
barcode-length	6 oder 8

Tabelle 142 Bänder

Element	Beschreibung
Pools bilden	Der Name des Pools, in dem die Bänder sich befinden.
Tape Count	Maximale Anzahl der Bänder in diesem Pool.
Kapazität	Die gesamte konfigurierte Datenkapazität der Bänder in diesem Pool in GiB (Gibibyte, der 2er-Potenz-Entsprechung von GB, Gigabyte).
Used	Der belegte Speicherplatz auf den Bändern in diesem Pool.
Average Compression	Der durchschnittliche Komprimierungsbetrag, der mit den Daten auf den Bändern in diesem Pool erreicht wurde.

Im Menü "More Tasks" können Sie Optionen für eine Bibliothek löschen, umbenennen oder festlegen, Bänder erstellen, löschen, importieren, exportieren oder verschieben und Steckplätze und CAPs hinzufügen oder löschen.

Erstellen von Bändern

Sie können Bänder in einer Bibliothek oder in einem Pool erstellen. Wenn die Erstellung über einen Pool initiiert wird, erstellt das System zuerst die Bänder und importiert sie dann in die Bibliothek.

Vorgehensweise

1. Wählen Sie **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library* oder **Vault** oder **Pools** > **Pools >** *pool*.
2. Wählen Sie **More Tasks** > **Tapes** > **Create**.
3. Geben Sie im Dialogfeld „Create Tapes“ die folgenden Informationen über das Band ein:

   Tabelle 143 Dialogfeld „Create Tapes“

Feld	Benutzereingabe
Library (wenn von einer Bibliothek initiiert)	Wenn ein Drop-down-Menü aktiviert ist, wählen Sie die Bibliothek aus oder behalten Sie die Standardauswahl bei.
Poolname	Wählen Sie in der Drop-down-Liste den Namen des Pools, in dem sich das Band befindet. Wenn keine Pools erstellt wurden, verwenden Sie den Pool "Default".
Number of Tapes	Wählen Sie für eine Bibliothek eine Zahl zwischen 1 und 20 aus. Wählen Sie für einen Pool eine Zahl zwischen 1 und 100.000 aus oder behalten Sie den Standardwert (20) bei. [Obwohl die Anzahl der unterstützten Bänder unbegrenzt ist, können Sie nicht mehr als 100.000 Bänder gleichzeitig erstellen.]
Starting Barcode	Geben Sie die anfängliche Strichcodenummer ein (im Format A99000LA).
Tape Capacity	(Optional) Geben Sie die Anzahl der GiB von 1 bis 4.000 für jedes Band ein (diese Einstellung setzt die Strichcodekapazitätseinstellung außer Kraft). Für die effiziente Nutzung von Festplattenspeicherplatz verwenden Sie 100 GiB oder weniger.

4. Wählen Sie **OK** und **Close**.

CLI-Entsprechung

```
 # vtl tape add A00000L1 capacity 100 count 5 pool VTL_Pool ...
added 5 tape(s)...
```

Hinweis

Sie müssen dafür sorgen, dass Band-Volume-Namen im Basis-10-Format automatisch inkrementiert werden.

Löschen von Bändern

Sie können Bänder in einer Bibliothek oder in einem Pool löschen. Wenn es aus einer Bibliothek initiiert wird, exportiert das System zuerst die Bänder und löscht sie dann. Die Bänder müssen sich im Vault befinden, nicht in einer Bibliothek. Auf einem DD-System, das als Replikationsziel dient, ist das Löschen von Bändern nicht zulässig.

Vorgehensweise

1. Wählen Sie **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library* oder **Vault** oder **Pools** > **Pools >** *pool*.
2. Wählen Sie **More Tasks** > **Tapes** > **Delete**.
3. Geben Sie im Dialogfeld „Delete Tapes“ Suchinformationen über die zu löschenden Bänder ein und wählen Sie **Search**:

Tabelle 144 Dialogfeld „Delete Tapes“

Feld	Benutzereingabe
Location	Wenn eine Drop-down-Liste angezeigt wird, wählen Sie eine Bibliothek aus, oder behalten Sie die Standardauswahl **Vault** bei.
Pools bilden	Wählen Sie den Namen des Pools aus, der nach dem Band durchsucht werden soll. Wenn keine Pools erstellt wurden, verwenden Sie den Pool "Default".
Barcode	Geben Sie einen eindeutigen Strichcode an oder behalten Sie den Standardwert (*) bei, um eine Gruppe von Bändern zu suchen. Für Strichcodes können Sie die Platzhalter ? und * verwenden, wobei ? mit einem einzigen Zeichen und * mit 0 oder mehr Zeichen übereinstimmt.
Count	Geben Sie ein, wie viele Bänder maximal an Sie zurückgegeben werden sollen. Wenn Sie dieses Feld leer lassen, wird der Standardwert (*) für Strichcodes verwendet.
Tapes Per Page	Wählen Sie die maximale Anzahl von Bändern aus, die pro Seite angezeigt werden. Mögliche Werte sind 15, 30 und 45.
Select All Pages	Wählen Sie das Kontrollkästchen **Select All Pages** aus, um alle Bänder auswählen, die durch die Suchanfrage zurückgegeben werden.
Items Selected	Zeigt die Anzahl der Bänder an, die auf mehreren Seiten ausgewählt sind. Dieser Wert wird automatisch für jede Bandauswahl aktualisiert.

4. Aktivieren Sie das Kontrollkästchen des Bands, das gelöscht werden soll, oder das Kontrollkästchen für die Spaltenüberschrift, um alle Bänder zu entfernen, und klicken Sie auf **Next**.
5. Wählen Sie im Bestätigungsfenster **Submit** und dann **Close**.

Hinweis

Nachdem ein Band entfernt wurde, wird der für das Band verwendete physische Laufwerksspeicherplatz erst nach einem Dateisystem-Bereinigungsvorgang zurückgewonnen.

CLI-Entsprechung

```
# vtl tape del barcode [count count] [pool pool]
```

Beispiel:

```
# vtl tape del A00000L1
```

Hinweis

Sie können die Aktion für Bereiche ausführen. Wenn in dem Bereich jedoch ein Band fehlt, wird die Aktion beendet.

Bänder importieren

Beim *Importieren von Bändern* werden vorhandene Bänder aus dem Vault zu einem Bibliothekssteckplatz, Laufwerk oder Cartridge Access Port (CAP) verschoben.

Die Anzahl der Bänder, die Sie gleichzeitig importieren können, wird von der Anzahl der leeren Steckplätze in der Bibliothek begrenzt, d. h. Sie können nicht mehr Bänder als die Anzahl der derzeitig leeren Steckplätze importieren.

Um die verfügbaren Steckplätze für eine Bibliothek anzuzeigen, wählen Sie im Stapelmenü die Bibliothek aus. Im Informationsbereich für die Bibliothek wird die Zahl in der Spalte „Empty“ angezeigt.

- Wenn sich ein Band in einem Laufwerk befindet und als Bandursprung ein Steckplatz bekannt ist, wird ein Steckplatz reserviert.
- Wenn sich ein Band in einem Laufwerk befindet und der Bandursprung unbekannt (Steckplatz oder CAP) ist, wird ein Steckplatz reserviert.
- Wenn sich ein Band in einem Laufwerk befindet und als Bandursprung ein CAP bekannt ist, wird kein Steckplatz reserviert. (Das Band kehrt zum CAP zurück, wenn es aus dem Laufwerken entfernt wird.)
- Informationen dazu, wie Sie ein Band in ein Laufwerk verschieben, finden Sie im folgenden Abschnitt zum Verschieben von Bändern.

Vorgehensweise

1. Bänder können mithilfe von Schritt a. oder Schritt b. importiert werden.

   a. Wählen Sie **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library* aus. Wählen Sie anschließend **More Tasks** > **Tapes** > **Import**. Geben Sie im Dialogfeld „Import Tapes“ Suchinformationen über die zu importierenden Bänder ein und wählen Sie **Search**:

   Tabelle 145 Dialogfeld „Import Tapes“

Feld	Benutzereingabe
Location	Wenn eine Drop-down-Liste angezeigt wird, wählen Sie den Bandspeicherort aus, oder behalten Sie die Standardauswahl **Vault** bei.
Pools bilden	Wählen Sie den Namen des Pools aus, der nach dem Band durchsucht werden soll. Wenn keine Pools erstellt wurden, verwenden Sie den Pool „Default“.
Barcode	Geben Sie einen eindeutigen Strichcode an oder behalten Sie den Standardwert (*) bei, damit eine Gruppe von Bändern zurückgegeben wird. Für Strichcodes können Sie die Platzhalter ? und * verwenden, wobei ? mit einem einzigen Zeichen und * mit 0 oder mehr Zeichen übereinstimmt.
Count	Geben Sie ein, wie viele Bänder maximal an Sie zurückgegeben werden sollen. Wenn Sie dieses Feld leer lassen, wird der Standardwert (*) für Strichcodes verwendet.
Tapes Per Page	Wählen Sie die maximale Anzahl der Bänder aus, die pro Seite angezeigt werden sollen. Die möglichen Werte sind 15, 30 und 45.

Tabelle 145 Dialogfeld „Import Tapes“ (Fortsetzung)

Feld	Benutzereingabe
Items Selected	Zeigt die Anzahl der Bänder an, die auf mehreren Seiten ausgewählt sind. Dieser Wert wird automatisch für jede Bandauswahl aktualisiert.

Basierend auf den bisherigen Bedingungen wird ein Standardsatz Bänder durchsucht, um die zu importierenden Bänder auszuwählen. Wenn Pool, Strichcode oder Anzahl geändert wird, wählen Sie „Search“ aus, um die Gruppe der Bänder zu aktualisieren, die zur Auswahl verfügbar sind.

b. Wählen **Virtual Tape Libraries** > **VTL Service** > **Libraries** > *Bibliothek* > **Changer** > **Drives** > *Laufwerk* > **Tapes** aus. Wählen Sie die zu importierenden Bänder aus, indem Sie das Kontrollkästchen neben Folgendem aktivieren:

- Einem einzelnen Band oder
- Der Spalte **Barcode**, um alle Bänder auf der aktuellen Seite auszuwählen oder
- Das Kontrollkästchen **Select All Pages**, um alle Bänder auszuwählen, die durch die Suchanfrage zurückgegeben werden.

Nur Bänder mit Vault als Speicherort können importiert werden.

Klicken Sie auf **Import from Vault**. Diese Schaltfläche ist standardmäßig deaktiviert und nur aktiviert, wenn alle ausgewählten Bänder vom Vault sind.

2. Überprüfen Sie in der Bibliotheksansicht „Import Tapes“ die Zusammenfassungsinformationen und die Bandliste und wählen Sie **OK**.
3. Wählen Sie im Statusfenster **Close** aus.

CLI-Entsprechung

```
# vtl tape show pool VTL_Pool
Processing tapes....
Barcode  Pool     Location State    Size    Used (%)           Comp ModTime
-------- -------- -------- ----- ------- --------------- ---- -------------------
A00000L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
A00001L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
A00002L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
A00003L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
A00004L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
-------- -------- -------- ----- ------- --------------- ---- -------------------
VTL Tape Summary
----------------
Total number of tapes:     5
Total pools:               1
Total size of tapes:       500 GiB
Total space used by tapes: 0.0 GiB
Average Compression:       0.0x

# vtl import NewVTL barcode A00000L3 count 5 pool VTL_Pool
... imported 5 tape(s)...

# vtl tape show pool VTL_Pool
Processing tapes....

VTL Tape Summary
----------------
Total number of tapes:     5
Total pools:               1
Total size of tapes:       500 GiB
```

```
Total space used by tapes: 0.0 GiB
Average Compression:       0.0x
```

Exportieren von Bändern

Exporting a tape entfernt dieses Band aus einem Steckplatz, Laufwerk oder Kassettenzugriffsport (Cartridge Access Port, CAP) und sendet es an den Vault.

Vorgehensweise

1. Bänder können mithilfe von Schritt a. oder Schritt b. exportiert werden.

   a. Wählen Sie **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library*. Wählen Sie dann **More Tasks** > **Tapes** > **Export**. Geben Sie im Dialogfeld „Export Tapes“ Suchinformationen über die zu exportierenden Bänder ein und wählen Sie **Search**:

   Tabelle 146 Dialogfeld „Export Tapes“

Feld	Benutzereingabe
Location	Wenn eine Drop-down-Liste angezeigt wird, wählen Sie den Namen der Bibliothek aus, in der sich das Band befindet, oder behalten Sie die ausgewählte Bibliothek bei.
Pools bilden	Wählen Sie den Namen des Pools aus, der nach dem Band durchsucht werden soll. Wenn keine Pools erstellt wurden, verwenden Sie den Pool "Default".
Barcode	Geben Sie einen eindeutigen Strichcode an oder behalten Sie den Standardwert (*) bei, damit eine Gruppe von Bändern zurückgegeben wird. Für Strichcodes können Sie die Platzhalter ? und * verwenden, wobei ? mit einem einzigen Zeichen und * mit 0 oder mehr Zeichen übereinstimmt.
Count	Geben Sie ein, wie viele Bänder maximal an Sie zurückgegeben werden sollen. Wenn Sie dieses Feld leer lassen, wird der Standardwert (*) für Strichcodes verwendet.
Tapes Per Page	Wählen Sie die maximale Anzahl der Bänder aus, die pro Seite angezeigt werden sollen. Die möglichen Werte sind 15, 30 und 45.
Select All Pages	Wählen Sie das Kontrollkästchen **Select All Pages** aus, um alle Bänder auswählen, die durch die Suchanfrage zurückgegeben werden.
Items Selected	Zeigt die Anzahl der Bänder an, die auf mehreren Seiten ausgewählt sind. Dieser Wert wird automatisch für jede Bandauswahl aktualisiert.

   b. Wählen Sie **Virtual Tape Libraries** > **VTL Service** > **Libraries***> library***> Changer** > **Drives >** *drive* **> Tapes**. Wählen Sie die zu exportierenden Bänder aus, indem Sie das Kontrollkästchen neben Folgendem aktivieren:

   - Einem einzelnen Band oder
   - Der Spalte **Barcode**, um alle Bänder auf der aktuellen Seite auszuwählen oder
   - Das Kontrollkästchen **Select All Pages**, um alle Bänder auszuwählen, die durch die Suchanfrage zurückgegeben werden.

   Nur Bänder mit einem Bibliotheksnamen in der Spalte „Location“ können exportiert werden.

Wählen Sie **Export from Library** aus. Diese Schaltfläche ist standardmäßig deaktiviert und nur aktiviert, wenn für alle ausgewählten Bänder in der Spalte „Location“ ein Bibliotheksname angegeben ist.

2. Überprüfen Sie in der Bibliotheksansicht „Export Tapes“ die Zusammenfassungsinformationen und die Bandliste und wählen Sie **OK**.
3. Wählen Sie im Statusfenster **Close** aus.

Verschieben von Bändern zwischen Geräten innerhalb einer Bibliothek

Bänder können zwischen physischen Geräten innerhalb einer Bibliothek zu mimischen Backupsoftwareverfahren für physische Bandbibliotheken verschoben werden. (Dabei wird ein Band in einer Bibliothek von einem Steckplatz zu einem Laufwerk, von einem Steckplatz zu einem CAP, von einem CAP zu einem Laufwerk und umgekehrt verschoben.) In einer physischen Bandbibliothek verschiebt die Backupsoftware ein Band niemals außerhalb der Bibliothek. Daher kann die Zielbibliothek nicht geändert werden und wird nur zur Klärung dargestellt.

Vorgehensweise

1. Wählen Sie **Virtual Tape Libraries** > **VTL Service** > **Libraries** > ***library***.

   Wenn dieser Vorgang von einer Bibliothek gestartet wird, beachten Sie, dass im Bereich „Tapes“ Bänder nur zwischen Geräten verschoben werden können.

2. Wählen Sie **More Tasks** > **Tapes** > **Move**.

   Wenn dieser Vorgang von einer Bibliothek gestartet wird, beachten Sie, dass im Bereich „Tapes“ Bänder nur zwischen Geräten verschoben werden können.

3. Geben Sie im Dialogfeld „Move Tape“ Suchinformationen über die zu verschiebenden Bänder ein und wählen Sie **Search**:

   Tabelle 147 Dialogfeld „Move Tape“

Feld	Benutzereingabe
Location	Der Speicherort kann nicht geändert werden.
Pools bilden	-
Barcode	Geben Sie einen eindeutigen Strichcode an oder behalten Sie den Standardwert (*) bei, damit eine Gruppe von Bändern zurückgegeben wird. Für Strichcodes können Sie die Platzhalter ? und * verwenden, wobei ? mit einem einzigen Zeichen und * mit 0 oder mehr Zeichen übereinstimmt.
Count	Geben Sie ein, wie viele Bänder maximal an Sie zurückgegeben werden sollen. Wenn Sie dieses Feld leer lassen, wird der Standardwert (*) für Strichcodes verwendet.
Tapes Per Page	Wählen Sie die maximale Anzahl der Bänder aus, die pro Seite angezeigt werden sollen. Die möglichen Werte sind 15, 30 und 45.
Items Selected	Zeigt die Anzahl der Bänder an, die auf mehreren Seiten ausgewählt sind. Dieser Wert wird automatisch für jede Bandauswahl aktualisiert.

4. Wählen Sie in der Liste mit den Suchergebnissen das Band oder die Bänder für das Verschieben aus.
5. Führen Sie einen der folgenden Schritte aus:

a. Wählen Sie das Gerät in der Liste „Devices“ aus (z. B. einen Steckplatz, ein Laufwerk oder einen CAP) und geben Sie eine Startadresse mithilfe der sequenziellen Zahlen für das zweite und die nachfolgenden Bänder ein. Für jedes zu verschiebende Band wird, wenn die angegebene IP-Adresse belegt ist, die nächste verfügbare IP-Adresse verwendet.

b. Lassen Sie die Adresse leer, wenn das Band in einem Laufwerk ursprünglich von einem Steckplatz stammt und zu diesem Steckplatz zurückgegeben werden soll; oder wenn das Band zu dem nächsten verfügbaren Steckplatz verschoben werden soll.

6. Klicken Sie auf **Next**.
7. Überprüfen Sie im Dialogfeld „Move Tape“ die Zusammenfassungsinformationen und die Bandliste und wählen Sie **Submit**.
8. Wählen Sie im Statusfenster **Close** aus.

Hinzufügen von Steckplätzen

Sie können Steckplätze von einer konfigurierten Bibliothek hinzufügen, um die Anzahl der Speicherelemente zu ändern.

Hinweis

Einige Backupanwendungen erkennen nicht automatisch, dass Steckplätze einer DD VTL hinzugefügt wurden. In Ihrer Anwendungsdokumentation finden Sie Informationen dazu, wie Sie die Anwendung konfigurieren, um diese Art der Änderung zu erkennen.

Vorgehensweise

1. Wählen Sie **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library* aus.
2. Wählen Sie **More Tasks** > **Slots** > **Add**.
3. Geben Sie im Dialogfeld "Add Slots" die Anzahl der Steckplätze ein, die Sie hinzufügen möchten. Die Gesamtzahl der Steckplätze in einer Bibliothek oder in allen Bibliotheken auf einem System darf 32.000 für eine Bibliothek und 64.000 für ein System nicht überschreiten.
4. Wählen Sie **OK** und **Close**, wenn der Status `Completed` anzeigt.

Löschen von Steckplätzen

Sie können Steckplätze aus einer konfigurierten Bibliothek löschen, um die Anzahl der Speicherelemente zu ändern.

Hinweis

Einige Backupanwendungen erkennen nicht automatisch, dass Steckplätze aus einer DD VTL gelöscht wurden. In Ihrer Anwendungsdokumentation finden Sie Informationen dazu, wie Sie die Anwendung konfigurieren, um diese Art der Änderung zu erkennen.

Vorgehensweise

1. Wenn der Steckplatz, den Sie löschen möchten, Kassetten enthält, verschieben Sie diese Kassetten in den Vault. Das System löscht nur leere, nicht übernommene Steckplätze.
2. Wählen Sie **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library* aus.

3. Wählen Sie **More Tasks** > **Slots** > **Delete**.
4. Geben Sie im Dialogfeld „Delete Pools“ die „Number of Slots“ ein, die gelöscht werden sollen:
5. Wählen Sie **OK** und **Close**, wenn der Status `Completed` anzeigt.

Hinzufügen von CAPs

Sie können CAPs (Cartridge Access Ports) von einer konfigurierten Bibliothek aus hinzufügen, um die Anzahl der Speicherelemente zu ändern.

Hinweis

CAPs werden von einer begrenzten Anzahl von Backupanwendungen verwendet. In Ihrer Anwendungsdokumentation können Sie nachsehen, ob CAPs unterstützt werden.

Vorgehensweise

1. Wählen Sie **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library* aus.
2. Wählen Sie **More Tasks** > **CAPs** > **Add**.
3. Geben Sie im Dialogfeld „Add CAPs“ die Anzahl der hinzuzufügenden CAPs ein. Sie können zwischen 1 und 100 CAPs pro Bibliothek und zwischen 1 und 1.000 CAPs pro System hinzufügen.
4. Wählen Sie **OK** und **Close**, wenn der Status `Completed` anzeigt.

Löschen von CAPs

Sie können CAPs (Cartridge Access Ports) aus einer konfigurierten Bibliothek löschen, um die Anzahl der Speicherelemente zu ändern.

Hinweis

Einige Backupanwendungen erkennen nicht automatisch, dass CAPs aus einer DD VTL entfernt wurden. In Ihrer Anwendungsdokumentation finden Sie Informationen dazu, wie Sie die Anwendung konfigurieren, um diese Art der Änderung zu erkennen.

Vorgehensweise

1. Wenn der CAP, den Sie entfernen möchten, Kassetten enthält, verschieben Sie diese Kassetten in den Vault oder dies wird automatisch durchgeführt.
2. Wählen Sie **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library* aus.
3. Wählen Sie **More Tasks** > **CAPs** > **Delete**.
4. Geben Sie im Dialogfeld „Delete CAPs“ die Anzahl der zu löschenden CAPs ein. Sie können maximal 100 CAPs pro Bibliothek oder 1.000 CAPs pro System löschen.
5. Wählen Sie **OK** und **Close**, wenn der Status `Completed` anzeigt.

Anzeigen von Wechslerinformationen

Es darf nur ein Wechsler pro DD VTL vorhanden sein. Welches Wechslermodell Sie auswählen, hängt von Ihrer jeweiligen Konfiguration ab.

Vorgehensweise

1. Wählen Sie **Virtual Tape Libraries** > **VTL Service** > **Libraries** aus.

2. Wählen Sie eine bestimmte Bibliothek aus.
3. Falls nicht erweitert, wählen Sie das Pluszeichen (+) auf der linken Seite aus, um die Bibliothek zu öffnen und wählen Sie ein Wechslerelement aus, um den Informationsbereich „Changer“ anzuzeigen, der die folgenden Informationen enthält.

Tabelle 148 Informationsbereich „Changer“

Element	Beschreibung
Anbieter	Name des Anbieters, der den Wechsler hergestellt hat
Produkt	Name des Modells
Version	Versionsstufe
Serial Number	Seriennummer des Wechslers

Arbeiten mit Laufwerken

Wenn Sie **Virtual Tape Libraries** > **VTL Service** > **Libraries** > *Bibliothek*> **Drives** auswählen, werden detaillierte Informationen zu allen Laufwerken für eine ausgewählte Bibliothek angezeigt.

Tabelle 149 Informationsbereich „Drives“

Spalte	Beschreibung
Laufwerk	Die Liste der Laufwerke nach Name, wobei der Name „Drive #“ und # eine Zahl zwischen 1 und n ist, die die Adresse oder den Speicherort des Laufwerks in der Liste der Laufwerke darstellt
Vendor	Hersteller oder Anbieter des Laufwerks, z. B. IBM
Product	Produktname des Laufwerks, z. B. ULTRIUM-TD5
Revision	Versionsnummer des Laufwerkprodukts
Serial Number	Seriennummer des Laufwerkprodukts
Status	Gibt an, ob das Laufwerk leer, offen, gesperrt oder geladen ist. Ein Band muss vorhanden sein, damit das Laufwerk gesperrt oder geladen werden kann.
Tape	Der Strichcode des Bands im Laufwerk (falls vorhanden)
Pool	Der Pool des Bands im Laufwerk (falls vorhanden)

Tape and Library Drivers: Zum Arbeiten mit Laufwerken müssen Sie die von Ihrem Backupsoftwareanbieter bereitgestellten Band- und Bibliothekstreiber verwenden, die die Laufwerke IBM LTO-1, IBM LTO-2, IBM LTO-3, IBM LTO-4, IBM LTO-5 (Standard), HP-LTO-3 oder HP-LTO-4 sowie die Bibliotheken StorageTek L180 (Standard), RESTORER-L180, IBM TS3500, I2000, I6000 oder DDVTL unterstützen. Weitere Informationen finden Sie in den *Anwendungskompatibilitätsmatrizen und Integrationsleitfäden* für Ihre Anbieter. Denken Sie beim Konfigurieren von Laufwerken auch an die Grenzwerte für Backupdatenstreams, die von der verwendeten Plattform bestimmt werden.

LTO Drive Capacities: Da das DD-System LTO-Laufwerke als virtuelle Laufwerke behandelt, können Sie die maximale Kapazität für jeden Laufwerkstyp auf 4 TiB

(4.000 GiB) festlegen. Die Standardkapazitäten für jeden LTO-Laufwerkstyp lauten wie folgt:

- LTO-1-Laufwerk: 100 GiB
- LTO-2-Laufwerk: 200 GiB
- LTO-3-Laufwerk: 400 GiB
- LTO-4-Laufwerk: 800 GiB
- LTO-5-Laufwerk: 1,5 TiB

Migrating LTO-1 Tapes: Sie können Bänder von vorhandenen LTO-1-VTLs zu VTLs migrieren, die Bänder und Laufwerke anderer unterstützter LTO-Typen beinhalten. Die Migrationsoptionen sind für jede Backupanwendung unterschiedlich, deshalb sollten Sie die Anweisungen im jeweiligen für Ihre Anwendung spezifischen LTO-Bandmigrationsleitfaden befolgen. Sie finden den entsprechenden Leitfaden, indem Sie die Onlinesupport-Website aufrufen und in das Suchtextfeld **LTO-Bandmigration für VTLs** eingeben.

Tape full: Early Warning: Sie erhalten eine Warnung, wenn der verbleibende Bandspeicherplatz fast vollständig aufgebraucht ist, das heißt, bei mehr als 99,9, aber weniger als 100 Prozent liegt. Die Anwendung kann bis zum Ende des Bands weiterschreiben, bis die Kapazität von 100 Prozent erreicht ist. Der letzte Schreibvorgang ist allerdings nicht wiederherstellbar.

Sie können über das Menü „More Tasks“ ein Laufwerk erstellen oder löschen.

Erstellen von Laufwerken

Mithilfe des Abschnitts *Anzahl der von einer DD VTL unterstützten Laufwerke* können Sie die maximale Anzahl von Laufwerken ermitteln, die speziell von Ihrer DD VTL unterstützt werden.

Vorgehensweise

1. Wählen Sie **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library***> Changer** > **Drives** aus.
2. Wählen Sie **More Tasks** > **Drives** > **Create**.
3. Geben Sie im Dialogfeld „Create Drive“ die folgenden Informationen ein:

Tabelle 150 Dialogfeld „Create Drive“

Feld	Benutzereingabe
Location	Wählen Sie einen Bibliotheksnamen aus oder behalten Sie den ausgewählten Namen bei.
Number of Drives	Informationen hierzu finden Sie im Abschnitt *Anzahl der von einer DD VTL unterstützten Laufwerke* weiter oben in diesem Kapitel.
Vorlagenname	Wählen Sie das Modell aus der Drop-down-Liste aus. Wenn ein anderes Laufwerk bereits vorhanden ist, ist diese Option inaktiv und der vorhandene Laufwerkstyp muss verwendet werden. Sie können Laufwerkstypen in derselben Bibliothek nicht mischen. • IBM-LTO-1 • IBM-LTO-2 • IBM-LTO-3 • IBM-LTO-4

Tabelle 150 Dialogfeld „Create Drive“ (Fortsetzung)

Feld	Benutzereingabe
	• IBM-LTO-5 (Standard) • HP-LTO-3 • HP-LTO-4

4. Wählen Sie **OK** aus und wählen Sie dann, wenn der Status `Completed` angezeigt wird, **OK** aus.

   Das hinzugefügte Laufwerk wird in der Liste „Drives“ angezeigt.

Löschen von Laufwerken

Ein Laufwerk muss leer sein, damit es gelöscht werden kann.

Vorgehensweise

1. Wenn sich ein Band in dem Laufwerk befindet, das Sie löschen möchten, entfernen Sie das Band.
2. Wählen Sie **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library***>** **Changer** > **Drives**.
3. Wählen Sie **More Tasks** > **Drives** > **Delete**.
4. Aktivieren Sie im Dialogfeld „Delete Drives“ die Kontrollkästchen der Laufwerke, die Sie löschen möchten oder wählen Sie das Kontrollkästchen **Drive** aus, um alle Laufwerke zu löschen.
5. Wählen Sie **Next** aus und nachdem Sie überprüft haben, ob die richtigen Laufwerke zum Löschen ausgewählt sind, wählen Sie **Submit** aus.
6. Wenn im Dialogfeld „Delete Drive Status“ `Completed` angezeigt wird, wählen Sie **Close** aus.

   Das Laufwerk wurde aus der Liste „Drives“ entfernt.

Arbeiten mit einem ausgewählten Laufwerk

Wenn Sie **Virtual Tape Libraries** > **VTL Service** > **Libraries** > *library***> Drives >***drive* auswählen, werden detaillierte Informationen zu einem ausgewählten Laufwerk angezeigt.

Tabelle 151 Registerkarte „Drive“

Spalte	Beschreibung
Laufwerks-	Die Liste der Laufwerke nach Name, wobei der Name „Drive #“ und # eine Zahl zwischen 1 und n ist, die die Adresse oder den Speicherort des Laufwerks in der Liste der Laufwerke darstellt
Anbieter	Hersteller oder Anbieter des Laufwerks, z. B. IBM
Produkt	Produktname des Laufwerks, z. B. ULTRIUM-TD5
Version	Versionsnummer des Laufwerkprodukts

Tabelle 151 Registerkarte „Drive“ (Fortsetzung)

Spalte	Beschreibung
Serial Number	Seriennummer des Laufwerkprodukts
Status	Gibt an, ob das Laufwerk leer, offen, gesperrt oder geladen ist. Ein Band muss vorhanden sein, damit das Laufwerk gesperrt oder geladen werden kann.
Band	Der Strichcode des Bands im Laufwerk (falls vorhanden)
Pools bilden	Der Pool des Bands im Laufwerk (falls vorhanden)

Tabelle 152 Registerkarte „Statistics“

Spalte	Beschreibung
Endpunkt	Der spezifische Name des Endpunkts
Operationen/s	Die Vorgänge pro Sekunde
Read KiB/s	Die Geschwindigkeit von Lesevorgängen in KiB pro Sekunde
Write KiB/s	Die Geschwindigkeit von Schreibvorgängen in KiB pro Sekunde

Über das Menü „More Tasks“ können Sie das Laufwerk löschen oder eine Aktualisierung durchführen.

Arbeiten mit Bändern

Ein Band wird als Datei dargestellt. Bänder können aus einem Vault in eine Bibliothek importiert werden. Bänder können aus einer Bibliothek in den Vault exportiert werden. Bänder können innerhalb einer Bibliothek zwischen Laufwerken, Steckplätzen (Kassettensteckplätzen) und CAPs (Bandzugriffsports) verschoben werden.

Wenn Bänder erstellt werden, werden diese im Vault platziert. Nachdem die Bänder zum Vault hinzugefügt wurden, können sie importiert, exportiert, verschoben, durchsucht oder entfernt werden.

Wählen Sie **Virtual Tape Libraries** > **VTL Service** > **Libraries** > *Library* > **Tapes** aus, um detaillierte Informationen zu allen Bändern für die ausgewählte Bibliothek anzuzeigen.

Tabelle 153 Bandbeschreibung

Element	Beschreibung
Barcode	Der eindeutige Barcode für das Band.
Pool	Der Name des Pools, der das Band enthält. Der Pool „Default“ enthält alle Bänder, die keinem benutzererstellten Pool zugewiesen sind.
Location	Der Speicherort des Bands: eine Bibliothek (mit Angabe der Laufwerks, CAP- oder Steckplatznummer) oder ein virtueller Vault.
State	Der Status des Bands:

Tabelle 153 Bandbeschreibung (Fortsetzung)

Element	Beschreibung
	• RW: les- und beschreibbar • RL: Retention Lock • RO: nur lesbar • WP: schreibgeschützt • RD: Replikationsziel
Capacity	Die Gesamtkapazität des Bands.
Used	Der verwendete Speicherplatz des Bands.
Compression	Der Umfang der Komprimierung, die für Daten auf einem Band durchgeführt wird.
Last Modified	Das Datum der letzten Änderung der Informationen auf dem Band. Die Änderungszeit, die vom System für altersbasierte Policies verwendet wird, kann von der Zeit der letzten Änderung abweichen, die im Abschnitt mit den Bandinformationen in DD System Manager angezeigt wird.
Locked Until	Wenn eine DD Retention Lock-Frist festgelegt wurde, wird die festgelegte Uhrzeit angezeigt. Wenn kein DD Retention Lock vorhanden ist, lautet dieser Wert `Not specified`.

Im Informationsbereich können Sie ein Band aus dem Vault importieren, Bänder in die Bibliothek exportieren, den Status eines Bands festlegen, ein Band erstellen oder ein Band löschen.

Über das Menü „More Tasks“ können Sie ein Band verschieben.

Ändern des Schreib- oder Retention Lock-Status eines Bands

Bevor Sie den Schreib- oder Retention Lock-Status eines Bands ändern können, muss das Band erstellt und importiert worden sein. Für DD VTL-Bänder wird die Data Domain Retention Lock-Standard-Policy verwendet. Nach Ablauf der Aufbewahrungsfrist für ein Band kann dieses nicht mehr beschrieben oder geändert werden; kann es jedoch gelöscht werden.

Vorgehensweise

1. Wählen Sie **Virtual Tape Libraries** > **VTL Service** > **Libraries** > ***Bibliothek*** > **Tapes** aus.
2. Wählen Sie das Band, das geändert werden soll, aus der Liste und anschließend die Option **Set State** aus (über der Liste).
3. Wählen Sie im Dialogfeld „Set Tape State“ die Option **Read-Writeable**, **Write-Protected** oder **Retention-Lock** aus.
4. Für den Status „Retention-Lock“ gehen Sie folgendermaßen vor:
   - Geben Sie das Ablaufdatum des Bands in Tagen, Wochen, Monaten oder Jahren ein.
   - Wählen Sie das Kalendersymbol und anschließend ein Datum aus dem Kalender aus. Die Aufbewahrungssperre läuft am ausgewählten Datum um 12 Uhr mittags ab.

5. Wählen Sie **Next** aus und klicken Sie auf **Submit**, um den Status zu ändern.

Arbeiten mit dem Vault

Der Vault enthält Bänder, die von keiner Bibliothek verwendet werden. Bänder befinden sich entweder in einer Bibliothek oder im Vault.

Durch Auswahl von **Virtual Tape Libraries** > **VTL Service** > **Vault** werden detaillierte Informationen für den Standardpool und alle anderen vorhandenen Pools im Vault angezeigt.

Systeme mit DD Cloud-Tier und DD VTL bieten die Möglichkeit, den Vault auf Cloudspeicher zu speichern.

Tabelle 154 Poolübersicht

Element	Beschreibung
Pool Count	Die Anzahl der VTL-Pools.
Tape Count	Die Anzahl der Bänder in den Pools.
Size	Der Gesamtspeicherplatz in den Pools.
Logical Used	Der in den Pools verwendete Speicherplatz.
Compression	Das durchschnittliche Ausmaß der Komprimierung in den Pools.

Der Bereich **Protection Distribution** enthält die folgenden Informationen.

Tabelle 155 Schutzverteilung

Element	Beschreibung
Speichertyp	Vault oder Cloud.
Cloudanbieter	Bei Systemen mit Bändern in DD Cloud-Tier gibt es eine Spalte für jeden Cloudanbieter.
Logical Used	Der in den Pools verwendete Speicherplatz.
Pool Count	Die Anzahl der VTL-Pools.
Tape Count	Die Anzahl der Bänder in den Pools.

Über das Menü „More Tasks“ können Sie Bänder im Vault erstellen, löschen und suchen.

Arbeiten mit dem cloudbasierten Vault

DD VTL unterstützt mehrere Parameter, die einzigartig für Konfigurationen sind, bei denen der Vault in DD Cloud Tier-Speicher gespeichert ist.

Die folgenden Vorgänge sind für die Arbeit mit cloudbasiertem Vault-Speicher verfügbar.

- Konfigurieren Sie die Datenverschiebungs-Policy und Cloudeinheitinformationen für den angegebenen VTL-Pool. Führen Sie den Befehl **`vtl pool modify <pool-name> data-movement-policy {user-managed | age-threshold <days> | none} to-tier {cloud} cloud-unit <cloud-unit-name>`** aus.
  Die verfügbaren Datenverschiebungs-Policies sind:

  - User-managed: Der Administrator kann diese Policy für einen Pool festlegen, um manuell Bänder aus dem Pool für die Migration zum Cloud-Tier auszuwählen. Die Bänder werden beim ersten Datenverschiebungsvorgang nach der Auswahl der Bänder migriert.
  - Age-threshold: Der Administrator kann diese Policy für einen Pool festlegen, um DD VTL die automatische Auswahl von Bändern aus dem Pool für die Migration zum Cloud-Tier basierend auf dem Alter des Bandes zu erlauben. Die Bänder werden innerhalb von sechs Stunden ausgewählt, nachdem sie den Altersschwellenwert erreicht haben, und bei der ersten Datenverschiebungsoperation nach der Auswahl der Bänder migriert.
- Wählen Sie ein angegebenes Band für die Migration zum Cloud-Tier aus. Führen Sie den Befehl **`vtl tape select-for-move barcode <barcode> [count <count>] pool <pool> to-tier {cloud}`** aus.
- Heben Sie die Auswahl eines angegebenen Bandes für die Migration zum Cloud-Tier auf. Führen Sie den Befehl **`vtl tape deselect-for-move barcode <barcode> [count <count>] pool <pool> to-tier {cloud}`** aus.
- Rufen Sie ein Band vom Cloud-Tier ab. Führen Sie den Befehl **`vtl tape recall start barcode <barcode> [count <count>] pool <pool>`** aus.
  Nach dem Rückruf befindet sich das Band in einem lokalen DD VTL-Vault und muss zum Zugriff in die Bibliothek importiert werden.

Hinweis

Sie können den Befehl `vtl tape show` jederzeit ausführen, um den aktuellen Speicherort eines Bandes zu prüfen. Der Bandspeicherort wird innerhalb von 1 Stunde nach dem Verschieben des Bandes in den oder aus dem Cloud-Tier aktualisiert.

Vorbereiten des VTL-Pools für Datenverschiebung

Festlegen der Datenverschiebungs-Policy auf dem VTL-Pool, um die Migration von VTL-Daten aus dem lokalen Vault auf DD Cloud-Tier zu managen.

Die Datenverschiebung für VTL erfolgt auf Band-Volume-Ebene. Einzelne Band-Volumes oder Sammlungen von Band-Volumes können in den Cloud-Tier verschoben werden, aber nur vom Vault-Speicherort. Bänder in anderen Elementen einer VTL können nicht verschoben werden.

Hinweis

Der standardmäßige VTL-Pool und Vault sowie `/data/col1/backup`-Verzeichnisse oder Legacy-Bibliothekskonfigurationen können nicht für Band-zu-Cloud verwendet werden.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD VTL** aus.
2. Erweitern Sie die Liste der Pools und wählen Sie einen Pool aus, auf dem die Migration von Bändern zu DD Cloud-Tier aktiviert werden soll.
3. Klicken Sie im Bereich **Cloud Data Movement** auf die Option **Create** unter **Cloud Data Movement Policy**.
4. Wählen Sie in der Drop-down-Liste **Policy** eine Datenverschiebungs-Policy aus:
   - **Alter der Bänder in Tagen**

- **Manuelle Auswahl**

5. Legen Sie die Details der Datenverschiebung Policy fest.
   - Wählen Sie für **Age of tapes in days** einen Altersschwellenwert fest, nach dem Bänder in DD Cloud-Tier migriert werden, und geben Sie eine Zielcloudeinheit fest.
   - Legen Sie für **Manual selection** eine Zielcloudeinheit fest.
6. Klicken Sie auf **Create**.

Hinweis

Nach der Erstellung der Datenverschiebungs-Policy können die Schaltflächen **Edit** und **Clear** verwendet werden, um die Datenverschiebungs-Policy zu ändern oder zu löschen.

CLI-Entsprechung

Vorgehensweise

1. Legen Sie die Datenverschiebungs-Policy auf „user-managed“ oder „age-threshold“ fest.

Hinweis

Bei den Namen von VTL-Pool und Cloudeinheit wird Groß-/Kleinschreibung beachtet und Befehle schlagen fehl, wenn die Schreibweise nicht korrekt ist.

- Um die Datenverschiebungs-Policy auf „user-managed“ festzulegen, führen Sie den folgenden Befehl aus:
  ```
  vtl pool modify cloud-vtl-pool data-movement-policy
  user-managed to-tier cloud cloud-unit ecs-unit1
  ```

```
**   Any tapes that are already selected will be migrated on the next data-movement
run.
VTL data-movement policy is set to "user-managed" for VTL pool "cloud-vtl-pool".
```

- Um die Datenverschiebungs-Policy auf „age-threshold“ festzulegen, führen Sie den folgenden Befehl aus:

Hinweis

Das Minimum sind 14 Tage und das Maximum sind 182.250 Tage.

```
vtl pool modify cloud-vtl-pool data-movement-policy age-
threshold 14 to-tier cloud cloud-unit ecs-unit1
```

```
**   Any tapes that are already selected will be migrated on the next data-movement
run.
VTL data-movement policy "age-threshold" is set to 14 days for the VTL pool "cloud-
vtl-pool".
```

2. Überprüfen Sie die Datenverschiebungs-Policy für den VTL-Pool.

   Führen Sie den folgenden Befehl aus:
   ```
   vtl pool show all
   ```

```
VTL Pools
Pool                    Status   Tapes   Size (GiB)   Used (GiB)   Comp   Cloud Unit
Cloud Policy
---------------------   ------   -----   ----------   ----------   ----   ----------
------------
```

```
cloud-vtl-pool          RW          50          250           41    45x   ecs-unit1
user-managed
Default                 RW           0            0            0     0x   -
none
---------------------   ------   -----   ----------   ----------   ----   ----------
------------
8080 tapes in 5 pools

 RO  : Read Only
 RD  : Replication Destination
 BCM : Backwards-Compatibility
```

3. Überprüfen Sie, ob die Policy für den VTL-Pool-MTree `app-managed` ist.

   Führen Sie den folgenden Befehl aus:
   `data-movement policy show all`

```
Mtree                       Target(Tier/Unit Name)   Policy        Value
-------------------------   ----------------------   -----------   -------
/data/col1/cloud-vtl-pool   Cloud/ecs-unit1          app-managed   enabled
-------------------------   ----------------------   -----------   -------
```

Entfernen von Bändern aus dem Backupanwendungsbestand

Verwenden Sie die Backupanwendung, um zu überprüfen, ob die Band-Volumes, die in die Cloud verschoben werden, gemäß den Backupanwendungsanforderungen markiert und im Bestand erfasst sind.

Auswählen von Band-Volumes für die Datenverschiebung

Wählen Sie manuell die Bänder für die Migration auf DD Cloud-Tier aus (sofort oder bei der nächsten geplanten Datenmigration) oder entfernen Sie Bänder manuell aus dem Migrationsplan.

Bevor Sie beginnen

Überprüfen Sie, ob die Backupanwendung über die Statusänderungen für Volumes informiert ist, die in Cloudspeicher verschoben wurden. Führen Sie die notwendigen Schritte durch, damit die Backupanwendung ihren Bestand entsprechend dem neuesten Volume-Status aktualisiert.

Wenn das Band nicht im Vault ist, kann es nicht zu DD Cloud-Tier migriert werden.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD VTL** aus.
2. Erweitern Sie die Liste der Pools und wählen Sie den Pool aus, der für die Migration von Bändern zu DD Cloud-Tier konfiguriert ist.
3. Klicken Sie im Bereich „Pool“ auf die Registerkarte **Tape**.
4. Wählen Sie die Bänder für die Migration auf DD Cloud-Tier aus.
5. Klicken Sie auf **Select for Cloud Move**, um das Band bei der nächsten geplanten Migration zu migrieren, oder auf **Move to Cloud Now**, um das Band sofort zu migrieren.

   Hinweis

   Wenn die Datenverschiebungs-Policy auf Bandalter basiert, steht die Option **Select for Cloud Move** nicht zur Verfügung, da das Data Domain-System automatisch Bänder für die Migration auswählt.

6. Klicken Sie im Bestätigungsdialogfeld auf **Yes**.

Aufheben der Auswahl von Band-Volumes für die Datenverschiebung

Für die Migration auf DD Cloud-Tier ausgewählte Bänder können von der Migrationsplanung entfernt werden.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD VTL** aus.
2. Erweitern Sie die Liste der Pools und wählen Sie den Pool aus, der für die Migration von Bändern zu DD Cloud-Tier konfiguriert ist.
3. Klicken Sie im Bereich „Pool“ auf die Registerkarte **Tape**.
4. Wählen Sie die Bänder für die Migration auf DD Cloud-Tier aus.
5. Klicken Sie auf **Unselect Cloud Move**, um das Band aus der Migrationsplanung zu entfernen.
6. Klicken Sie im Bestätigungsdialogfeld auf **Yes**.

CLI-Entsprechung

Vorgehensweise

1. Identifizieren Sie den Steckplatzspeicherort des Band-Volume, das verschoben werden soll.

   Führen Sie den folgenden Befehl aus:
   `vtl tape show cloud-vtl`

```
Processing tapes....
Barcode    Pool             Location            State    Size           Used (%)
Comp   Modification Time
--------   --------------   -----------------   -----   -----   ----------------
----   ------------------
T00001L3   cloud-vtl-pool   cloud-vtl slot 1    RW      5 GiB   5.0 GiB (99.07%)
205x   2017/05/05 10:43:43
T00002L3   cloud-vtl-pool   cloud-vtl slot 2    RW      5 GiB   5.0 GiB (99.07%)
36x   2017/05/05 10:45:10
T00003L3   cloud-vtl-pool   cloud-vtl slot 3    RW      5 GiB   5.0 GiB (99.07%)
73x   2017/05/05 10:45:26
```

2. Geben Sie den numerischen Steckplatzwert ein, um das Band aus der DD-VTL zu exportieren.

   Führen Sie den folgenden Befehl aus:
   `vtl export cloud-vtl-pool slot 1 count 1`

3. Überprüfen Sie, ob sich das Band im Vault befindet.

   Führen Sie den folgenden Befehl aus:
   `vtl tape show vault`

4. Wählen Sie das Band für die Datenverschiebung aus.

   Führen Sie den folgenden Befehl aus:
   `vtl tape select-for-move barcode T00001L3 count 1 pool cloud-vtl-pool to-tier cloud`

Hinweis

Wenn die Datenverschiebungs-Policy „age-threshold“ ist, werden die Daten automatisch nach 15-20 Minuten verschoben.

5. Zeigen Sie die Liste der Bänder an, die während der nächsten Datenverschiebung in den Cloudspeicher verschoben werden sollen. Die für die Verschiebung ausgewählten Bänder weisen ein `(S)` in der Speicherortspalte auf.

   Führen Sie den folgenden Befehl aus:
   `vtl tape show vault`

```
Processing tapes.....
Barcode    Pool               Location    State      Size           Used (%)   Comp
Modification Time
--------   ----------------   ---------   ------   ------   ----------------   ----
-------------------
T00003L3   cloud-vtl-pool      vault (S)   RW        5 GiB   5.0 GiB (99.07%)    63x
2017/05/05 10:43:43
T00006L3   cloud-vtl-pool      ecs-unit1   n/a       5 GiB   5.0 GiB (99.07%)    62x
2017/05/05 10:45:49
--------   ----------------   ---------   ------   ------   ----------------   ----
-------------------
* RD : Replication Destination
(S) Tape selected for migration to cloud. Selected tapes will move to cloud on the next
data-movement run.
(R) Recall operation is in progress for the tape.

VTL Tape Summary
----------------
Total number of tapes:     4024
Total pools:               3
Total size of tapes:       40175 GiB
Total space used by tapes: 39.6 GiB
Average Compression:       9.7x
```

6. Wenn die Datenverschiebungs-Policy „user-managed“ ist, initiieren Sie die Datenverschiebung.

   Führen Sie den folgenden Befehl aus:
   `data-movement start`

7. Beobachten Sie den Status der Datenverschiebung.

   Führen Sie den folgenden Befehl aus:
   `data-movement watch`

8. Überprüfen Sie, ob die Band-Volumes erfolgreich in den Cloudspeicher verschoben wurden.

   Führen Sie den folgenden Befehl aus:
   `vtl tape show all cloud-unit ecs-unit1`

```
Processing tapes.....
Barcode  Pool           Location  State  Size         Used (%) Comp Modification Time
-------- -------------- --------- ----- ----- ---------------- ---- -------------------
T00001L3 cloud-vtl-pool ecs-unit1 n/a   5 GiB 5.0 GiB (99.07%)  89x 2017/05/05 10:41:41
T00006L3 cloud-vtl-pool ecs-unit1 n/a   5 GiB 5.0 GiB (99.07%)  62x 2017/05/05 10:45:49
-------- -------------- --------- ----- ----- ---------------- ---- -------------------
(S) Tape selected for migration to cloud. Selected tapes will move to cloud on the next
data-movement run.
(R) Recall operation is in progress for the tape.

VTL Tape Summary
----------------
Total number of tapes:     4
Total pools:               2
Total size of tapes:       16 GiB
Total space used by tapes: 14.9 GiB
Average Compression:       59.5x
```

Wiederherstellen von Daten in der Cloud

Wenn ein Client Daten für die Wiederherstellung vom Backupanwendungsserver anfordert, sollte die Backupanwendung eine Warnmeldung oder Mitteilung generieren, in der die erforderlichen Volumes bei der Cloudeinheit angefordert werden.

Das Volume muss von der Cloud abgerufen und in die Data Domain VTL-Bibliothek eingecheckt werden, bevor die Backupanwendung über das Vorhandensein der Volumes informiert werden kann.

Hinweis

Überprüfen Sie, ob die Backupanwendung über die Statusänderungen für Volumes informiert ist, die in Cloudspeicher verschoben wurden. Führen Sie die notwendigen Schritte durch, damit die Backupanwendung ihren Bestand entsprechend dem neuesten Volume-Status aktualisiert.

Manuelles Abrufen eines Band-Volume vom Cloudspeicher

Rufen Sie ein Band aus DD Cloud-Tier in den lokalen VTL-Vault ab.

Vorgehensweise

1. Wählen Sie **Protocols** > **DD VTL** aus.
2. Erweitern Sie die Liste der Pools und wählen Sie den Pool aus, der für die Migration von Bändern zu DD Cloud-Tier konfiguriert ist.
3. Klicken Sie im Bereich „Pool“ auf die Registerkarte **Tape**.
4. Wählen Sie ein Band oder mehrere Bänder aus, das bzw. die sich in einer Cloudeinheit befinden.
5. Klicken Sie auf **Recall Cloud Tapes**, um Bänder von DD Cloud-Tier abzurufen.

Ergebnisse

Nach der nächsten geplanten Datenmigration werden die Bänder von der Cloudeinheit in den Vault abgerufen. Vom Vault können die Bänder in eine Bibliothek zurückgegeben werden.

CLI-Entsprechung

Vorgehensweise

1. Identifizieren Sie das Volume, das zum Wiederherstellen der Daten erforderlich ist.
2. Rufen Sie das Band-Volume vom Vault ab.

   Führen Sie den folgenden Befehl aus:
   ```
   vtl tape recall start barcode T00001L3 count 1 pool cloud-vtl-pool
   ```
3. Überprüfen Sie, ob die Abrufoperation gestartet wurde.

   Führen Sie den folgenden Befehl aus:
   ```
   data-movement status
   ```
4. Überprüfen Sie, ob die Abrufoperation erfolgreich abgeschlossen wurde.

   Führen Sie den folgenden Befehl aus:
   ```
   vtl tape show all barcode T00001L3
   ```

```
Processing tapes....
Barcode    Pool             Location           State    Size           Used (%)
Comp   Modification Time
--------   --------------   ----------------   -----   -----   ----------------
----   -------------------
T00001L3   cloud-vtl-pool   cloud-vtl slot 1   RW      5 GiB   5.0 GiB (99.07%)
239x   2017/05/05 10:41:41
--------   --------------   ----------------   -----   -----   ----------------
----   -------------------
(S) Tape selected for migration to cloud. Selected tapes will move to cloud on the next
data-movement run.
(R) Recall operation is in progress for the tape.

VTL Tape Summary
----------------
Total number of tapes:     1
Total pools:               1
Total size of tapes:       5 GiB
Total space used by tapes: 5.0 GiB
Average Compression:       239.1x
```

5. Validieren Sie den Speicherort der Datei.

   Führen Sie den folgenden Befehl aus:
   `filesys report generate file-location path /data/col1/cloud-vtl-pool`

```
filesys report generate file-location path /data/col1/cloud-vtl-pool
------------------------------      --------------------------
File Name                           Location(Unit Name)
------------------------------      --------------------------
/data/col1/cloud-vtl-pool/.vtl_pool     Active
/data/col1/cloud-vtl-pool/.vtc/T00001L3 Active
-----------------------------------------------------------------
```

6. Importieren Sie das abgerufene Band in die DD VTL.

   Führen Sie den folgenden Befehl aus:
   `vtl import cloud-vtl barcode T00001L3 count 1 pool cloud-vtl-pool element slot`

```
imported 1 tape(s)...sysadmin@ddbeta70# vtl tape show cloud-vtlProcessing tapes.....
```

7. Checken Sie das Volume in den Backupanwendungsbestand ein.
8. Stellen Sie Daten über die Backupanwendung wieder her.
9. Wenn die Wiederherstellung abgeschlossen ist, checken Sie das Band-Volume aus dem Backupanwendungsbestand aus.
10. Exportieren Sie das Band-Volume aus der Data Domain-VTL in den Data Domain-Vault.
11. Verschieben Sie das Band wieder in die Cloudeinheit.

Arbeiten mit Zugriffsgruppen

Zugriffsgruppen enthalten eine Sammlung von Initiator-WWPNs (weltweite Portnamen) oder Aliasnamen sowie die Laufwerke und Wechsler, auf die sie zugreifen dürfen. Eine DD VTL-Standardgruppe namens *TapeServer* ermöglicht es Ihnen, Geräte hinzuzufügen, die NDMP-basierte (Network Data Management Protocol) Backupanwendungen unterstützen.

Die Zugriffsgruppenkonfiguration ermöglicht es Initiatoren (in den allgemeinen Backupanwendungen), Daten auf Geräte in die gleiche Zugriffsgruppe zu schreiben oder sie zu lesen.

Zugriffsgruppen ermöglichen Clients, nur auf ausgewählte LUNs (Medienwechsler oder virtuelle Bandlaufwerke) auf einem System zuzugreifen. Eine Clienteinrichtung für eine Zugriffsgruppe kann nur auf Geräte in der Zugriffsgruppe zugreifen.

Vermeiden Sie Änderungen an der Zugriffsgruppe in einem DD-System während aktiven Backups oder Wiederherstellungen. Eine Änderung kann dazu führen, dass ein aktiver Job fehlschlägt. Die Auswirkungen von Änderungen während aktiver Jobs hängen von der Kombination aus Backupsoftware und Hostkonfigurationen ab.

Durch Auswahl von **Access Groups** > **Groups** werden die folgenden Informationen für alle Zugriffsgruppen angezeigt.

Tabelle 156 Informationen zu Zugriffsgruppen

Element	Beschreibung
Group Name	Der Name der Gruppe
Initiators	Die Anzahl der Initiatoren in der Gruppe
Geräte	Die Anzahl der Geräte in der Gruppe

Wenn Sie **View All Access Groups** auswählen, wechseln Sie zur Ansicht „Fibre Channel“.

Über das Menü „More Tasks“ können Sie eine Gruppe erstellen oder löschen.

Erstellen einer Zugriffsgruppe

Zugriffsgruppen managen den Zugriff zwischen Geräten und Initiatoren. Verwenden Sie die TapeServer-Standardgruppe nur, wenn NDMP verwendet wird.

Vorgehensweise

1. Wählen Sie **Access Groups** > **Groups**.
2. Wählen Sie **More Tasks** > **Group** > **Create** aus.
3. Geben Sie im Dialogfeld „Create Access Group“ einen Namen mit 1 bis 128 Zeichen ein und wählen Sie **Next** aus.
4. Fügen Sie Geräte hinzu und wählen Sie **Next** aus.
5. Überprüfen Sie die Zusammenfassung und wählen Sie **Finish** bzw. **Back** aus.

   CLI-Entsprechung

   ```
   # scsitarget group create My_Group service My_Service
   ```

Hinzufügen eines Zugriffsgruppengeräts

Die Zugriffsgruppenkonfiguration ermöglicht es Initiatoren (in den allgemeinen Backupanwendungen), Daten auf Geräte in die gleiche Zugriffsgruppe zu schreiben oder sie zu lesen.

Vorgehensweise

1. Wählen Sie **Access Groups** > **Groups**. Sie können auch eine spezifische *Gruppe* auswählen.
2. Wählen Sie **More Tasks** > **Group** > **Create** oder **Group** > **Configure** aus.
3. Geben im Dialogfeld „Create or Modify Access Group“ den **Group Name** ein oder ändern Sie ihn, wenn gewünscht. (Dieses Feld muss ausgefüllt werden.)

4. Um Initiatoren für die Zugriffsgruppe zu konfigurieren, aktivieren Sie das Kontrollkästchen neben dem Initiator. Sie können Initiatoren auch zu einem späteren Zeitpunkt zu der Gruppe hinzufügen.
5. Klicken Sie auf **Next**.
6. Wählen Sie in der Anzeige „Devices“ die Option „Add“ (**+**), um das Dialogfeld „Add Devices“ anzuzeigen.
   a. Überprüfen Sie, ob die korrekte Bibliothek in der Drop-down-Liste „Library Name“ ausgewählt ist, oder wählen Sie eine andere Bibliothek aus.
   b. Aktivieren Sie im Bereich „Device“ die Kontrollkästchen der Geräte (Wechsler und Laufwerke), die in die Gruppe aufgenommen werden sollen.
   c. Optional geben Sie eine Start-LUN im Textfeld „LUN Start Address“ an.

      Dies ist die LUN, die ein DD-System zum Initiator zurückgibt. Jedes Gerät wird durch die Bibliothek und den Gerätenamen eindeutig identifiziert. (Beispielsweise ist es möglich, Laufwerk 1 in Bibliothek 1 und Laufwerk 1 in Bibliothek 2 zu haben.) Daher ist eine LUN mit einem Gerät verknüpft, das von der Bibliothek und dem Gerätenamen identifiziert wird.

      Beim Bereitstellen von LUNs über angeschlossene FC-Ports auf FC-HBAs/SLICs kann für Ports „primary“, „secondary“ oder „none“ festgelegt werden. Ein primärer Port (Primary) für LUNs ist der Port, der diese LUNs aktuell in einer Fabric verfügbar macht. Ein sekundärer Port (Secondary) ist ein Port, der LUNs bei einem Ausfall des primären Pfads sendet (manuelle Intervention erforderlich). Die Einstellung „None“ wird verwendet, wenn ausgewählte LUNs nicht verfügbar gemacht werden sollen. Inwiefern LUNs verfügbar gemacht werden, ist von der jeweiligen SAN-Topologie abhängig.

      Die Initiatoren in der Zugriffsgruppe interagieren mit den LUN-Geräten, die der Gruppe hinzugefügt werden sollen.

      Die maximale akzeptierte LUN beim Erstellen einer Zugriffsgruppe ist 16383.

      Eine LUN kann nur einmal für eine einzelne Gruppe verwendet werden. Dieselbe LUN kann mit mehreren Gruppen verwendet werden.

      Einige Initiatoren (Clients) haben spezifische Regeln für die LUN-Nummerierung des Ziels; z. B. sind LUN 0 oder zusammenhängende LUNs erforderlich. Wenn diese Regeln nicht eingehalten werden, ist ein Initiator u. U. nicht in der Lage, auf einige oder alle LUNs zuzugreifen, die einem DD VTL-Zielport zugewiesen sind.

      Überprüfen Sie Ihre Initiatordokumentation auf spezielle Regeln und ändern Sie die Geräte-LUNs auf dem DD VTL-Zielport bei Bedarf, um die Regeln einzuhalten. Wenn beispielsweise ein Initiator erfordert, dass LUN 0 auf dem DD VTL-Zielport zugewiesen wird, überprüfen Sie die LUNs für Geräte, die Ports zugewiesen sind. Wenn nicht ausreichend Geräte LUN 0 zugewiesen sind, ändern Sie die LUN eines Geräts so, dass es LUN 0 zugewiesen wird.

   d. Im Bereich „Primary and Secondary Endpoints“ wählen Sie eine Option aus, um zu bestimmen, von welchen Ports das ausgewählte Gerät erkannt wird. Die folgenden Bedingungen gelten für angegebene Ports:
      - all: Das geprüften Gerät wird von allen Ports erkannt.
      - none: Das geprüfte Gerät wird von keinem Port erkannt.
      - select: Das geprüfte Gerät wird von den ausgewählten Ports erkannt. Aktivieren Sie die Kontrollkästchen für die entsprechenden Ports. Wenn nur Primärports ausgewählt werden, ist das geprüfte Gerät nur von Primärports aus sichtbar.

Wenn nur Sekundärports ausgewählt werden, ist das geprüfte Gerät nur von Sekundärports aus sichtbar. Sekundärports können verwendet werden, wenn die Primärports nicht verfügbar sind.

Der Switchover zu einem sekundären Port ist kein automatischer Vorgang. Sie müssen das DD VTL-Gerät manuell auf den sekundären Port umschalten, wenn die primären Ports nicht mehr verfügbar sind.

Die Portliste ist eine Liste mit physischen Portnummern. Eine Portnummer gibt den PCI-Steckplatz und ein Buchstabe den Port auf einer PCI-Karte an. Beispiele sind 1a, 1b oder 2a, 2b.

Ein Laufwerk wird mit derselben LUN auf allen Ports angezeigt, die Sie konfiguriert haben.

e. Wählen Sie **OK** aus.

Sie wechseln zurück zum Dialogfeld „Devices“, in dem die neue Gruppe aufgeführt ist. Um mehr Geräte hinzuzufügen, wiederholen Sie diese fünf Unterschritte.

7. Klicken Sie auf **Next**.
8. Klicken Sie auf **Close**, wenn die Statusmeldung `Completed` angezeigt wird.

CLI-Entsprechung

```
# vtl group add VTL_Group vtl NewVTL changer lun 0 primary-port all secondary-port all#
vtl group add VTL_Group vtl NewVTL drive 1 lun 1 primary-port all secondary-port all#
vtl group add SetUp_Test vtl SetUp_Test drive 3 lun 3 primary-port endpoint-fc-0
secondary-port endpoint-fc-1

# vtl group show Setup_Test
Group: SetUp_Test

Initiators:
Initiator Alias   Initiator WWPN
---------------   ----------------------
tsm6_p23          21:00:00:24:ff:31:ce:f8
---------------   ----------------------

Devices:
Device Name          LUN   Primary Ports   Secondary Ports    In-use Ports
------------------   ---   -------------   ---------------   -------------
SetUp_Test changer     0             all               all             all
SetUp_Test drive 1     1             all               all             all
SetUp_Test drive 2     2              5a                5b              5a
SetUp_Test drive 3     3   endpoint-fc-0     endpoint-fc-1   endpoint-fc-0
------------------   ---   -------------   ---------------   -------------
```

Ändern oder Löschen eines Zugriffsgruppengeräts

Möglicherweise müssen Sie ein Gerät in einer Zugriffsgruppe ändern oder löschen.

Vorgehensweise

1. Wählen Sie **Protocols** > **VTL** > **Access Groups** > **Groups**> *group* aus.
2. Wählen Sie **More Tasks** > **Group** > **Configure** aus.
3. Geben Sie im Dialogfeld „Modify Access Group“ in das Feld **Group Name** den Gruppennamen ein oder ändern Sie ihn. (Dieses Feld muss ausgefüllt werden.)
4. Um Initiatoren für die Zugriffsgruppe zu konfigurieren, aktivieren Sie das Kontrollkästchen neben dem Initiator. Sie können Initiatoren auch zu einem späteren Zeitpunkt zu der Gruppe hinzufügen.

5. Klicken Sie auf **Next**.
6. Wählen Sie ein Gerät aus und klicken Sie dann auf das Stiftsymbol für die Bearbeitung, um das Dialogfeld „Modify Devices“ anzuzeigen. Führen Sie anschließend die Schritte a bis e durch. Wenn Sie das Gerät einfach löschen möchten, wählen Sie das Löschsymbol (X) aus und fahren Sie mit Schritt e fort.
   a. Überprüfen Sie, dass in der Drop-down-Liste „Library“ die korrekte Bibliothek ausgewählt ist, oder wählen Sie eine andere Bibliothek aus.
   b. Aktivieren Sie im Bereich „Devices to Modify“ die Kontrollkästchen der Geräte (Changer und Laufwerke), die geändert werden sollen.
   c. Ändern Sie optional die Start-LUN (Logical Unit Number) im Feld „LUN Start Address“.

      Dies ist die LUN, die ein DD-System zum Initiator zurückgibt. Jedes Gerät wird durch die Bibliothek und den Gerätenamen eindeutig identifiziert. (Beispielsweise ist es möglich, Laufwerk 1 in Bibliothek 1 und Laufwerk 1 in Bibliothek 2 zu haben.) Daher ist eine LUN mit einem Gerät verknüpft, das von der Bibliothek und dem Gerätenamen identifiziert wird.

      Die Initiatoren in der Zugriffsgruppe interagieren mit den LUN-Geräten, die der Gruppe hinzugefügt werden sollen.

      Die maximale akzeptierte LUN beim Erstellen einer Zugriffsgruppe ist 16383.

      Eine LUN kann nur einmal für eine einzelne Gruppe verwendet werden. Dieselbe LUN kann mit mehreren Gruppen verwendet werden.

      Einige Initiatoren (Clients) haben spezifische Regeln für die LUN-Nummerierung des Ziels; z. B. sind LUN 0 oder zusammenhängende LUNs erforderlich. Wenn diese Regeln nicht eingehalten werden, ist ein Initiator u. U. nicht in der Lage, auf einige oder alle LUNs zuzugreifen, die einem DD VTL-Zielport zugewiesen sind.

      Überprüfen Sie Ihre Initiatordokumentation auf spezielle Regeln und ändern Sie die Geräte-LUNs auf dem DD VTL-Zielport bei Bedarf, um die Regeln einzuhalten. Wenn beispielsweise ein Initiator erfordert, dass LUN 0 auf dem DD VTL-Zielport zugewiesen wird, überprüfen Sie die LUNs für Geräte, die Ports zugewiesen sind. Wenn nicht ausreichend Geräte LUN 0 zugewiesen sind, ändern Sie die LUN eines Geräts so, dass es LUN 0 zugewiesen wird.

   d. Ändern Sie im Bereich „Primary and Secondary Ports“ die Option, mit der festgelegt wird, welchen Ports das ausgewählte Gerät angezeigt wird. Die folgenden Bedingungen gelten für angegebene Ports:
      - all: Das geprüften Gerät wird von allen Ports erkannt.
      - none: Das geprüfte Gerät wird von keinem Port erkannt.
      - select: Das geprüfte Gerät wird ausgewählten Ports angezeigt. Aktivieren Sie die Kontrollkästchen der Ports, denen das Gerät angezeigt wird. Wenn nur Primärports ausgewählt werden, ist das geprüfte Gerät nur von Primärports aus sichtbar.

        Wenn nur Sekundärports ausgewählt werden, ist das geprüfte Gerät nur von Sekundärports aus sichtbar. Sekundäre Ports können verwendet werden, wenn die primären Ports nicht mehr verfügbar sind.

      Der Switchover zu einem sekundären Port ist kein automatischer Vorgang. Sie müssen das DD VTL-Gerät manuell auf den sekundären Port umschalten, wenn die primären Ports nicht mehr verfügbar sind.

Die Portliste ist eine Liste mit physischen Portnummern. Eine Portnummer gibt den PCI-Steckplatz und ein Buchstabe den Port auf einer PCI-Karte an. Beispiele sind 1a, 1b oder 2a, 2b.

Ein Laufwerk wird auf allen Ports, die Sie konfiguriert haben, mit derselben LUN angezeigt.

e. Wählen Sie **OK** aus.

Löschen einer Zugriffsgruppe

Bevor Sie eine Zugriffsgruppe löschen können, müssen Sie alle zugehörigen Initiatoren und LUNs entfernen.

Vorgehensweise

1. Entfernen Sie alle Initiatoren und LUNs aus der Gruppe.
2. Wählen Sie **Access Groups** > **Groups**.
3. Wählen Sie **More Tasks** > **Group** > **Delete** aus.
4. Aktivieren Sie im Dialogfeld „Delete Group“ das Kontrollkästchen der zu entfernenden Gruppe und wählen Sie **Next** aus.
5. Überprüfen Sie im Gruppenbestätigungsdialogfeld den Löschvorgang und wählen Sie **Submit** aus.
6. Wählen Sie **Close** aus, wenn unter „Delete Groups Status“ `Completed` angezeigt wird.

CLI-Entsprechung

```
# scsitarget group destroy My_Group
```

Arbeiten mit einer ausgewählten Zugriffsgruppe

Durch Auswahl von **Access Groups** > **Groups** > *group* werden die folgenden Informationen für eine ausgewählte Zugriffsgruppe angezeigt.

Tabelle 157 Registerkarte „LUNs“

Element	Beschreibung
LUN	Geräteadresse, deren höchste Zahl 16383 ist. Eine LUN kann innerhalb einer Gruppe nur einmal verwendet werden, kann jedoch in einer anderen Gruppe erneut verwendet werden. DD VTL-Geräte, die einer Gruppe hinzugefügt werden, müssen zusammenhängende LUNs verwenden.
Library	Name der Bibliothek, die mit der LUN verknüpft ist
Gerät	Wechsler und Laufwerke
In-Use Endpoints	Der derzeit verwendete Satz von Endpunkten: primär oder sekundär
Primary Endpoints	Erster (oder Standard-)Endpunkt, der von der Backupanwendung verwendet wird. Bei einem Ausfall auf diesem Endpunkt werden die sekundären Endpunkte verwendet, sofern verfügbar.

Tabelle 157 Registerkarte „LUNs“ (Fortsetzung)

Element	Beschreibung
Secondary Endpoints	Satz von Failover-Endpunkten, der verwendet wird, wenn ein primärer Endpunkt ausfällt

Tabelle 158 Registerkarte „Initiators“

Element	Beschreibung
Name	Name des Initiators, entweder der WWPN oder der Alias, der dem Initiator zugewiesen ist
WWPN	Eindeutiger weltweiter Portname, eine 64-Bit-Kennung (ein 60-Bit-Wert nach einer 4-Bit-*Network Address-Authority*-Kennung) des Fibre Channel-Ports

Im Menü „More Tasks“ können Sie eine ausgewählte Gruppe konfigurieren oder die verwendeten Endpunkte festlegen.

Auswählen von Endpunkten für ein Gerät

Da Endpunkte ein Gerät mit einem Initiator verbinden, müssen Sie die Endpunkte mit diesem Prozess einrichten, bevor Sie das Gerät anschließen.

Vorgehensweise

1. Wählen Sie **Access Groups** > **Groups**> *Gruppe* aus.
2. Wählen Sie **More Tasks** > **Endpoints** > **Set In-Use** aus.
3. Wählen Sie im Dialogfeld „Set In-Use Endpoints“ nur bestimmte Geräte oder die Option **Devices** aus, um alle Geräte in der Liste auszuwählen.
4. Geben Sie an, ob es sich um primäre oder sekundäre Endpunkte handelt.
5. Wählen Sie **OK** aus.

Konfigurieren der TapeServer-Gruppe für das NDMP-Gerät

Die DD VTL-TapeServer-Gruppe enthält Bandlaufwerke, die mit NDMP-basierten (Network Data Management Protocol) Backupanwendungen verbunden sind und die Kontrollinformationen und Datenstreams über IP (Internet Protocol) anstelle von FC (Fibre Channel) senden. Ein vom NDMP-TapeServer verwendetes Gerät muss in der DD VTL-Gruppe „TapeServer“ enthalten sein und ist *nur* für den NDMP-TapeServer verfügbar.

Vorgehensweise

1. Fügen Sie neue Bandlaufwerke zu einer vorhandenen Bibliothek hinzu (in diesem Beispiel mit dem Namen „dd990-16“).
2. Erstellen Sie Steckplätze und CAPs für die Bibliothek.
3. Fügen Sie die erstellten Geräte in einer Bibliothek (in diesem Beispiel „dd990-16“) der TapeServer-Zugriffsgruppe hinzu.
4. Aktivieren Sie den NDMP-Daemon, indem Sie an der Befehlszeile Folgendes eingeben:

```
# ndmpd enable
Starting NDMP daemon, please wait.............
NDMP daemon is enabled.
```

5. Vergewissern Sie sich, dass der NDMP-Daemon die Geräte in der TapeServer-Gruppe erkennt:

```
# ndmpd show devicenames
NDMP Device          Virtual Name        Vendor   Product       Serial Number
-----------------    ----------------    ------   -----------   -------------
/dev/dd_ch_c0t0l0    dd990-16 changer    STK      L180          6290820000
/dev/dd_st_c0t1l0    dd990-16 drive 1    IBM      ULTRIUM-TD3   6290820001
/dev/dd_st_c0t2l0    dd990-16 drive 2    IBM      ULTRIUM-TD3   6290820002
/dev/dd_st_c0t3l0    dd990-16 drive 3    IBM      ULTRIUM-TD3   6290820003
/dev/dd_st_c0t4l0    dd990-16 drive 4    IBM      ULTRIUM-TD3   6290820004
-----------------    ----------------    ------   -----------   -------------
```

6. Fügen Sie einen NDMP-Benutzer (in diesem Beispiel ndmp) mit dem folgenden Befehl hinzu:

```
# ndmpd user add ndmp
Enter password:
Verify password:
```

7. Überprüfen Sie, ob der Benutzer ndmp ordnungsgemäß hinzugefügt wurde:

```
# ndmpd user show
ndmp
```

8. Zeigen Sie die NDMP-Konfiguration an:

```
# ndmpd option show all
Name              Value
--------------    --------
authentication    text
debug             disabled
port              10000
preferred-ip
--------------    --------
```

9. Ändern Sie die Standardbenutzer-Passwortauthentifizierung, um die MD5-Verschlüsselung für erweiterte Sicherheit zu verwenden, und überprüfen Sie die Änderung (beachten Sie, dass der Authentifizierungswert von „text“ in „md5“ geändert wurde):

```
# ndmpd option set authentication md5
# ndmpd option show all
Name              Value
--------------    --------
authentication    md5
debug             disabled
port              10000
preferred-ip
--------------    --------
```

Ergebnisse

NDMP ist nun konfiguriert und die TapeServer-Zugriffsgruppe zeigt die Gerätekonfiguration. Informationen zu allen Befehlen und Optionen finden Sie im Kapitel `ndmpd` im *Data Domain Operating System Command Reference Guide*.

Arbeiten mit Ressourcen

Wenn Sie **Resources** > **Resources** auswählen, werden Informationen über Initiatoren und Endpunkte angezeigt. Ein *Initiator* ist ein Backupclient, der mit einem System verbunden ist, um Daten mithilfe des FC-Protokolls (Fibre Channel) zu lesen und schreiben. Ein bestimmter Initiator kann DD Boost über Fibre Channel oder DD VTL

unterstützen, aber nicht beides. Ein *Endpunkt* ist das logische Ziel auf einem DD-System, mit dem der Initiator verbunden ist.

Tabelle 159 Registerkarte „Initiators“

Element	Beschreibung
Name	Name des Initiators, entweder der WWPN oder der Alias, der dem Initiator zugewiesen ist
WWPN	Eindeutiger weltweiter Portname, eine 64-Bit-Kennung (ein 60-Bit-Wert nach einer 4-Bit-*Network Address-Authority*-Kennung) des FC-Ports (Fibre Channel)
WWNN	Eindeutiger weltweiter Node-Name, eine 64-Bit-Kennung (ein 60-Bit-Wert nach einer 4-Bit-*Network Address-Authority*-Kennung) des FC-Node
Online Endpoints	Der Name der Gruppe, in dem Initiator Ports angezeigt werden. Hier wird `None` oder `Offline` angezeigt, wenn der Initiator nicht verfügbar ist.

Tabelle 160 Registerkarte „Endpoints“

Element	Beschreibung
Name	Der Name des Endpunkts
WWPN	Eindeutiger weltweiter Portname, eine 64-Bit-Kennung (ein 60-Bit-Wert nach einer 4-Bit-*Network Address-Authority*-Kennung) des FC-Ports (Fibre Channel)
WWNN	Eindeutiger weltweiter Node-Name, eine 64-Bit-Kennung (ein 60-Bit-Wert nach einer 4-Bit-*Network Address-Authority*-Kennung) des FC-Node
Systemadresse	Systemadresse für den Endpunkt.
Aktiviert	Der Portbetriebszustand des HBA (Hostbusadapters), der entweder `Yes` (aktiviert) oder `No` (nicht aktiviert) sein kann.
Status	Status des DD VTL-Links, entweder `Online` (kann Datenverkehr verarbeiten) oder `Offline`.

Configure Resources
Wenn Sie **Configure Resources** auswählen, gelangen Sie zum Fibre Channel-Bereich, in dem Sie Endpunkte und Initiatoren konfigurieren können.

Arbeiten mit Initiatoren

Durch Auswahl von **Resources** > **Resources** > **Initiators** werden Informationen über Initiatoren angezeigt. Ein *Initiator* ist der WWPN (weltweite Portname) eines Clientsystem-FC-HBA (Fibre Channel-Hostbusadapter), mit dem das DD-System verbunden ist. Ein *Initiatorname* ist ein Alias für den WWPN des Clients, der die Anwenderfreundlichkeit erhöht.

Während ein Client als Initiator zugeordnet ist, aber bevor eine Zugriffsgruppe hinzugefügt wurde, kann der Client auf keine Daten auf einem DD-System zugreifen.

Nachdem Sie eine Zugriffsgruppe für den Initiator oder den Client hinzugefügt haben, kann der Client nur auf die Geräte in dieser Zugriffsgruppe zugreifen. Ein Client kann Zugriffsgruppen für mehrere Geräte haben.

Eine Zugriffsgruppe kann mehrere Initiatoren aufweisen, ein Initiator kann jedoch nur in einer Zugriffsgruppe existieren.

Hinweis

Maximal 1024 Initiatoren können für ein DD-System konfiguriert werden.

Tabelle 161 Initiatorinformationen

Element	Beschreibung
Name	Name des Initiators
Gruppe	Gruppe, die dem Initiator zugewiesen ist
Online Endpoints	Endpunkte, die dem Initiator angezeigt werden. Hier wird `none` oder `offline` angezeigt, wenn der Initiator nicht verfügbar ist.
WWPN	Eindeutiger weltweiter Portname, eine 64-Bit-Kennung (ein 60-Bit-Wert nach einer 4-Bit-*Network Address-Authority*-Kennung) des FC-Ports (Fibre Channel)
WWNN	Eindeutiger weltweiter Node-Name, eine 64-Bit-Kennung (ein 60-Bit-Wert nach einer 4-Bit-*Network Address-Authority*-Kennung) des FC-Node
Vendor Name	Name des Anbieters für den Initiator

Wenn Sie **Configure Initiators** auswählen, gelangen Sie zum Fibre Channel-Bereich, in dem Sie Endpunkte und Initiatoren konfigurieren können.

CLI-Entsprechung

```
# vtl initiator show
Initiator  Group      Status  WWNN                    WWPN                    Port
---------  ---------  ------  ----------------------  ----------------------  ----
tsm6_p1    tsm3500_a  Online  20:00:00:24:ff:31:ce:f8  21:00:00:24:ff:31:ce:f8 10b
---------  ---------  ------  ----------------------  ----------------------  ----

Initiator  Symbolic Port Name                          Address Method
---------  ------------------------------------------  --------------
tsm6_p1    QLE2562 FW:v5.06.03 DVR:v8.03.07.15.05.09-k  auto
---------  ------------------------------------------  --------------
```

Arbeiten mit Endpunkten

Wählen Sie **Resources** > **Resources** > **Endpoints** aus, um Informationen über Hardware und Verbindungen von Endpunkten anzuzeigen.

Tabelle 162 Registerkarte „Hardware“

Element	Beschreibung
Systemadresse	Systemadresse des Endpunkts.
WWPN	Eindeutiger weltweiter Portname, eine 64-Bit-Kennung (ein 60-Bit-Wert nach einer 4-Bit-*Network Address-Authority*-Kennung) des FC-Ports (Fibre Channel)

Tabelle 162 Registerkarte „Hardware“ (Fortsetzung)

Element	Beschreibung
WWNN	Eindeutiger weltweiter Node-Name, eine 64-Bit-Kennung (ein 60-Bit-Wert nach einer 4-Bit-*Network Address-Authority*-Kennung) des FC-Node
Enabled	Der Portbetriebszustand des HBA (Hostbusadapters), der entweder `Yes` (aktiviert) oder `No` (nicht aktiviert) sein kann.
NPIV	NPIV-Status dieses Endpunkts: entweder „Enabled“ oder „Disabled“
Link Status	Verknüpfungsstatus dieses Endpunkts: entweder „Online“ oder „Offline“
Operation Status	Betriebsstatus dieses Endpunkts: entweder „Normal“ oder „Marginal“
# of Endpoints	Anzahl der Endpunkte, die diesem Endpunkt zugeordnet sind

Tabelle 163 Registerkarte „Endpoints“

Element	Beschreibung
Name	Der Name des Endpunkts
WWPN	Eindeutiger weltweiter Portname, eine 64-Bit-Kennung (ein 60-Bit-Wert nach einer 4-Bit-*Network Address-Authority*-Kennung) des FC-Ports (Fibre Channel)
WWNN	Eindeutiger weltweiter Node-Name, eine 64-Bit-Kennung (ein 60-Bit-Wert nach einer 4-Bit-*Network Address-Authority*-Kennung) des FC-Node
Systemadresse	Systemadresse des Endpunkts.
Enabled	Der Portbetriebszustand des HBA (Hostbusadapters), der entweder `Yes` (aktiviert) oder `No` (nicht aktiviert) sein kann.
Link Status	Verknüpfungsstatus dieses Endpunkts: entweder „Online“ oder „Offline“.

Configure Endpoints

Durch Auswahl von **Configure Endpoints** gelangen Sie zum Bereich „Fibre Channel“, wo Sie alle der obigen Informationen für den Endpunkt ändern können.

CLI-Entsprechung

```
# scsitarget endpoint show list
Endpoint       System Address  Transport     Enabled  Status
--------       --------------  ---------     -------  ------
endpoint-fc-0  5a              FibreChannel  Yes      Online
endpoint-fc-1  5b              FibreChannel  Yes      Online
```

Arbeiten mit einem ausgewählten Endpunkt

Wählen Sie **Resources** > **Resources** > **Endpoints** > *endpoint*, um Informationen über die Hardware und Verbindungen sowie Statistiken von Endpunkten anzuzeigen.

Tabelle 164 Registerkarte „Hardware“

Element	Beschreibung
Systemadresse	Systemadresse des Endpunkts
WWPN	Eindeutiger weltweiter Portname, eine 64-Bit-Kennung (ein 60-Bit-Wert nach einer 4-Bit-*Network Address-Authority*-Kennung) des Fibre-Channel-Ports
WWNN	Eindeutiger weltweiter Node-Name, eine 64-Bit-Kennung (ein 60-Bit-Wert nach einer 4-Bit-*Network Address-Authority*-Kennung) des FC-Node
Aktiviert	Der Portbetriebszustand des HBA (Hostbusadapters), der entweder `Yes` (aktiviert) oder `No` (nicht aktiviert) sein kann.
NPIV	NPIV-Status dieses Endpunkts: entweder „Enabled“ oder „Disabled“
Link Status	Verknüpfungsstatus dieses Endpunkts: entweder „Online“ oder „Offline“
Operation Status	Betriebsstatus dieses Endpunkts: entweder „Normal“ oder „Marginal“
# of Endpoints	Anzahl der Endpunkte, die diesem Endpunkt zugeordnet sind

Tabelle 165 Registerkarte „Summary“

Element	Beschreibung
Name	Der Name des Endpunkts
WWPN	Eindeutiger weltweiter Portname, eine 64-Bit-Kennung (ein 60-Bit-Wert nach einer 4-Bit-*Network Address-Authority*-Kennung) des Fibre-Channel-Ports
WWNN	Eindeutiger weltweiter Node-Name, eine 64-Bit-Kennung (ein 60-Bit-Wert nach einer 4-Bit-*Network Address-Authority*-Kennung) des FC-Node
Systemadresse	Systemadresse des Endpunkts
Aktiviert	Der Portbetriebszustand des HBA (Hostbusadapters), der entweder `Yes` (aktiviert) oder `No` (nicht aktiviert) sein kann.
Link Status	Verknüpfungsstatus dieses Endpunkts: entweder „Online“ oder „Offline“

Tabelle 166 Registerkarte „Statistics“

Element	Beschreibung
Endpoint	Der Name des Endpunkts
Library	Name der Bibliothek, die den Endpunkt enthält
Gerät	Nummer des Geräts
Ops/s	Vorgänge pro Sekunde

Tabelle 166 Registerkarte „Statistics“ (Fortsetzung)

Element	Beschreibung
Read KiB/s	Geschwindigkeit der Lesevorgänge in KiB pro Sekunde
Write KiB/s	Geschwindigkeit der Schreibvorgänge in KiB pro Sekunde

Tabelle 167 Registerkarte „Detailed Statistics“

Element	Beschreibung
Endpoint	Der Name des Endpunkts
# of Control Commands	Anzahl der Steuerbefehle
# of Read Commands	Anzahl der Lesebefehle
# of Write Commands	Anzahl der Schreibbefehle
In (MiB)	Anzahl der geschriebenen MIB (das binäre Äquivalent von MB)
Out (MiB)	Anzahl der gelesenen MIB
# of Error Protocol	Anzahl der Fehlerprotokolle
# of Link Fail	Anzahl der Linkausfälle
# of Invalid Crc	Anzahl der ungültigen CRCs (zyklische Redundanzprüfungen)
# of Invalid TxWord	Anzahl der ungültigen tx-Wörter (Übertragung)
# of Lip	Anzahl der LIPs (Loopinitialisierungsprimitive)
# of Loss Signal	Anzahl der verlorenen Signale oder Verbindungen
# of Loss Sync	Anzahl der Signale oder Verbindungen, die die Synchronisation verloren haben

Arbeiten mit Pools

Wählen Sie **Pools** > **Pools** aus, um detaillierte Informationen über den Standardpool und alle anderen vorhandenen Pools anzuzeigen. Ein *Pool* ist eine Sammlung von Bändern, die einem Verzeichnis auf einem Dateisystem zugeordnet ist. Pools werden verwendet, um Bänder an ein Ziel zu replizieren. Sie können verzeichnisbasierte Pools in MTree-basierte Pools konvertieren, um die zahlreicheren Funktionen von MTrees zu nutzen.

Beachten Sie folgende Hinweise zu Pools:

- Es gibt zwei Arten von Pools: MTree (empfohlen) oder Verzeichnis für Abwärtskompatibilität.
- Ein Pool kann unabhängig davon repliziert werden, wo sich einzelne Bänder befinden. Bänder können sich im Vault oder in einer Bibliothek (Steckplatz, CAP oder Laufwerk) befinden.
- Sie können Bänder von einem Pool zu einem anderen kopieren und verschieben.
- Auf Pools kann nicht mit Backupsoftware zugegriffen werden.
- Beim Replizieren von Pools ist keine DD VTL-Konfiguration oder -Lizenz auf einem Replikationsziel erforderlich.

- Sie müssen Bänder mit eindeutigen Strichcodes erstellen. Das Duplizieren von Strichcodes kann zu unvorhersehbarem Verhalten in Backupanwendungen führen und für Benutzer verwirrend sein.
- Wenn zwei Bänder in zwei verschiedenen Pools auf einem DD-System denselben Namen haben, kann keins der Bänder an den Pool des anderen Bands verschoben werden. Ebenso muss ein Pool, der an ein Replikationsziel gesendet wird, einen Namen haben, der für das Ziel eindeutig ist.

Tabelle 168 Registerkarte „Pools“

Element	Beschreibung
Location	Standort des Pools
Typ	Verzeichnis- oder MTree-Pool
Tape Count	Die Anzahl der Bänder im Pool
Kapazität	Die gesamte konfigurierte Datenkapazität von Bändern im Pool, in GiB (Gibibyte, das Base-2-Äquivalent von GB, Gigabyte)
Belegt	Der belegte Speicherplatz, der im Pool für virtuelle Bänder verwendet wird
Average Compression	Das durchschnittliche Ausmaß der Komprimierung, die für Daten auf Bändern im Pool erreicht wird

Tabelle 169 Registerkarte „Replication“

Element	Beschreibung
Name	Der Name des Pools
Configured	Zeigt an, ob die Replikation für diesen Pool konfiguriert ist: „yes“ oder „no“
Remotequelle	Enthält nur einen Eintrag, wenn der Pool aus einem anderen DD-System repliziert wird.
Remote Destination	Enthält nur einen Eintrag, wenn der Pool in ein anderes DD-System repliziert wird.

Über das Menü „More Tasks“ können Sie Pools erstellen und löschen sowie nach Bändern suchen.

Erstellen von Pools

Falls erforderlich, können Sie für Ihre Konfiguration Pools mit Abwärtskompatibilität erstellen, beispielsweise für die Replikation mit einem DD OS-System älter als Version 5.2.

Vorgehensweise

1. Wählen Sie **Pools** > **Pools**.
2. Wählen Sie **More Tasks** > **Pool** > **Create**.
3. Geben Sie im Dialogfeld „Create Pool“ einen Poolnamen ein und beachten Sie Folgendes:
   - „all,“„vault“ oder „summary“ darf nicht verwendet werden.

- Ein Poolname kann nicht mit einem Leerzeichen oder Punkt beginnen oder enden.
- Die Groß-/Kleinschreibung muss beachtet werden.

4. Wenn Sie einen Verzeichnispool erstellen möchten (welcher mit der vorherigen Version von DD System Manager abwärtskompatibel ist), wählen Sie die Option „Create a directory backwards compatibility mode pool“ aus. Beachten Sie jedoch, dass die Verwendung eines MTree-Pools folgende Vorteile bietet:
   - Erstellung individueller Snapshots und Planung von Snapshots
   - Anwendung von Aufbewahrungssperren
   - Festlegung einer individuellen Aufbewahrungs-Policy
   - Abruf von Komprimierungsinformationen
   - Abruf von Datenmigrations-Policies für den Aufbewahrungs-Tier
   - Festlegung einer Policy für die Speicherplatznutzung (Quota-Unterstützung) durch Festlegen von harten und weichen Limits
5. Klicken Sie auf **OK**, um das Statusdialogfeld „Create Pool“ anzuzeigen.
6. Nachdem im Statusdialogfeld „Create Pool“ der Status `Completed` angezeigt wird, wählen Sie **Close** aus. Der Pool wird zum Unterverzeichnis „Pools“ hinzugefügt und Sie können nun virtuelle Bänder hinzufügen.

CLI-Entsprechung

```
# vtl pool add VTL_Pool
A VTL pool named VTL_Pool is added.
```

Löschen von Pools

Bevor ein Pool gelöscht werden kann, müssen Sie alle Bänder gelöscht haben, die darin enthalten sind. Wenn die Replikation für den Pool konfiguriert ist, muss das Replikationspaar ebenfalls gelöscht werden. Das Löschen eines Pools entspricht der Umbenennung des MTree und dem anschließenden Löschen, was beim nächsten Bereinigungsprozess auftritt.

Vorgehensweise

1. Wählen Sie **Pools** > **Pools** > ***pool***.
2. Wählen Sie **More Tasks** > **Pool** > **Delete**.
3. Aktivieren Sie im Dialogfeld „Delete Pools“ das Kontrollkästchen der zu löschenden Elemente:
   - Der Name jedes Pools oder
   - **Pool Names**, um alle Pools zu löschen.
4. Wählen Sie **Submit** in den Bestätigungsdialogfeldern aus.
5. Wenn im Dialogfeld „Delete Pool Status“ `Completed` angezeigt wird, wählen Sie **Close** aus.

   Der Pool wurde im Unterverzeichnis „Pools“ entfernt.

Arbeiten mit einem ausgewählten Pool

Sowohl **Virtual Tape Libraries** > **VTL Service** > **Vault** > *Pool* als auch **Pools** > **Pools** > *Pool* zeigen Information für einen ausgewählten Pool an. Beachten Sie, dass der Pool „Default“ immer vorhanden ist.

Registerkarte „Pool“

Tabelle 170 Zusammenfassung

Element	Beschreibung
Convert to MTree Pool	Wählen Sie diese Schaltfläche aus, um einen Verzeichnispool in einen MTree-Pool zu konvertieren.
Typ	Verzeichnis- oder MTree-Pool
Tape Count	Die Anzahl der Bänder im Pool
Kapazität	Die gesamte konfigurierte Datenkapazität von Bändern im Pool, in GiB (Gibibyte, das Base-2-Äquivalent von GB, Gigabyte)
Logical Used	Der belegte Speicherplatz, der im Pool für virtuelle Bänder verwendet wird
Compression	Das durchschnittliche Ausmaß der Komprimierung, die für Daten auf Bändern im Pool erreicht wird

Tabelle 171 Registerkarte „Pool“ Clouddatenverschiebung – Schutzverteilung

Element	Beschreibung
Pool type (%)	VTL-Pool und -Cloud (falls zutreffend) mit dem aktuellen Prozentsatz der Daten in Klammern.
Name	Name des lokalen VTL-Pool oder Cloudanbieter.
Logical Used	Der belegte Speicherplatz, der im Pool für virtuelle Bänder verwendet wird
Tape Count	Die Anzahl der Bänder im Pool

Tabelle 172 Registerkarte „Pool“ Clouddatenverschiebung – Clouddatenverschiebungs-Policy

Element	Beschreibung
Policy	Alter der Bänder in Tagen oder manuelle Auswahl.
Older Than	Altersschwellenwert für eine alterbasierte Datenverschiebungs-Policy.
Cloud Unit	Zielcloudeinheit.

Registerkarte „Tape“

Tabelle 173 Bandsteuerelemente

Element	Beschreibung
Create	Erstellen eines neuen Bands.
Delete	Löschen der ausgewählten Bänder.
Copy	Erstellen einer Kopie von einem Band.
Move between Pool	Verschieben der ausgewählten Bänder zu einem anderen Pool.
Select for Cloud Move	Planen der ausgewählten Bänder zur Migration auf DD Cloud-Tier.
Unselect from Cloud Move	Entfernen der ausgewählten Bänder aus dem Plan zur Migration auf DD Cloud-Tier.
Recall Cloud Tapes	Abrufen der ausgewählten Bänder vom DD Cloud-Tier.
Move to Cloud Now	Migrieren der ausgewählten Bänder in DD Cloud-Tier, ohne bis zur nächsten geplanten Migration zu warten.

Tabelle 174 Bandinformationen

Element	Beschreibung
Barcode	Bandbarcode
Size	Maximale Größe des Bands.
Physical Used	Vom Band verwendete physische Speicherkapazität.
Compression	Komprimierungsverhältnis auf dem Band.
Location	Speicherort des Bands
Änderungszeit	Der Zeitpunkt der letzten Änderung des Bands.
Recall Time	Der Zeitpunkt des letzten Aufrufs des Bands.

Registerkarte „Replication“

Tabelle 175 Replikation

Element	Beschreibung
Name	Der Name des Pools
Configured	Zeigt an, ob die Replikation für diesen Pool konfiguriert ist: „yes“ oder „no“
Remotequelle	Enthält nur einen Eintrag, wenn der Pool aus einem anderen DD-System repliziert wird.
Remote Destination	Enthält nur einen Eintrag, wenn der Pool in ein anderes DD-System repliziert wird.

Sie können auch die Schaltfläche **Replication Detail** rechts oben auswählen, um direkt zum Bereich „Replication information“ für den ausgewählten Pool zu wechseln.

Im Bereich „Virtual Tape Libraries or Pools“ über das Menü „More Tasks“ können Sie ein Band im Pool erstellen, löschen, verschieben, kopieren oder suchen.

Im Bereich „Pools“ können Sie über das Menü „More Tasks“ einen Pool umbenennen oder löschen.

Konvertieren eines Verzeichnispools in einen MTree-Pool

MTree-Pools haben gegenüber Verzeichnispools zahlreiche Vorteile. Weitere Informationen hierzu finden Sie im Abschnitt *Erstellen von Pools*.

Vorgehensweise

1. Stellen Sie sicher, dass alle der folgenden Voraussetzungen erfüllt wurden:
   - Die Quell- und Zielpools müssen synchronisiert worden sein, damit die Anzahl der Bänder und die Daten auf jeder Seite unverändert bleiben.
   - Der Verzeichnispool darf keine Replikationsquelle oder ein Replikationsziel sein.
   - Das Dateisystem darf nicht voll sein.
   - Das Dateisystem darf die maximal zulässige Anzahl von MTrees (100) nicht erreichen.
   - Es darf kein MTree mit demselben Namen bereits vorhanden sein.
   - Wenn der Verzeichnispool auf mehreren Systemen repliziert wird, müssen die replizierenden Systeme dem Managementsystem bekannt sein.
   - Wenn der Verzeichnispool für eine ältere DD OS-Version repliziert wird (z. B. von DD OS 5.5 zu DD OS 5.4), kann er nicht konvertiert werden. Nutzen Sie folgenden Workaround:
     - Replizieren Sie den Verzeichnispool in einem zweiten DD-System.
     - Replizieren Sie den Verzeichnispool aus dem zweiten DD-System in ein drittes DD-System.
     - Entfernen Sie das zweite und dritte DD-System aus dem Data Domain-Netzwerk des DD-Managementsystems.
     - Wählen Sie auf einem der Systeme unter DD OS 5.5 aus dem Untermenü „Pools“ die Option **Pools** und dann einen Verzeichnispool aus. Wählen Sie auf der Registerkarte „Pools“ die Option **Convert to MTree Pool**.
2. Markieren Sie den Verzeichnispool, den Sie konvertieren möchten, und wählen Sie **Convert to MTree Pool**.
3. Wählen Sie im Dialogfeld „Convert to MTree Pool“ **OK**.
4. Beachten Sie, dass die Konvertierung sich wie folgt auf die Replikation auswirkt:
   - DD VTL ist während der Konvertierung vorübergehend auf dem replizierten System deaktiviert.
   - Die Zieldaten werden auf dem Zielsystem in einen neuen Pool kopiert, um die Daten zu erhalten, bis die neue Replikation initialisiert und synchronisiert wurde. Anschließend können Sie diesen vorübergehend kopierten Pool sicher entfernen. Der Pool trägt den Namen **CONVERTED-***pool*, wobei *pool* der Name des Pools ist, der aktualisiert wurde (oder die ersten 18 Zeichen bei längeren Poolnamen). [Dies gilt nur für DD OS 5.4.1.0 und höher.]
   - Das Zielreplikationsverzeichnis wird in das MTree-Format konvertiert. [Dies gilt nur für DD OS 5.2 und höher.]

- Replikationspaare werden vor der Poolkonvertierung getrennt und danach wiederhergestellt, wenn keine Fehler auftreten.
- DD Retention Lock kann nicht auf Systemen aktiviert werden, die an der MTree-Poolkonvertierung beteiligt sind.

Verschieben von Bändern zwischen Pools

Bänder im Vault können zum Durchführen von Replikationsaktivitäten zwischen Pools verschoben werden. Beispielsweise sind Pools erforderlich, wenn alle Bänder im Standardpool erstellt wurden, aber Sie später unabhängige Gruppen für die Replikation von Gruppen von Bändern benötigen. Sie können benannte Pools erstellen und die Gruppen von Bändern in neue Pools neu organisieren.

Hinweis

Sie können keine Bänder von einem Bandpool verschieben, der eine Verzeichnisreplikationsquelle ist. Als Workaround ist Folgendes möglich:

- Kopieren Sie das Band an einen neuen Pool und löschen Sie das Band dann aus dem alten Pool.
- Verwenden Sie einen Mtree-Pool, mit dem Sie Bänder von einem Bandpool verschieben können, der eine Verzeichnisreplikationsquelle ist.

Vorgehensweise

1. Wählen Sie mit einem hervorgehobenen Pool**More Tasks** > **Tapes** > **Move**.

   Beachten Sie, dass beim Starten von einem Pool Bänder im Bereich „Tapes“ nur zwischen Pools verschoben werden können.

2. Geben Sie im Dialogfeld „Move Tapes“ Informationen ein, um die zu verschiebenden Bänder zu suchen und wählen Sie **Search** aus:

Tabelle 176 Dialogfeld „Move Tapes“

Feld	Benutzereingabe
Location	Der Speicherort kann nicht geändert werden.
Pools bilden	Wählen Sie den Namen des Pools aus, in dem sich die Bänder befinden. Wenn keine Pools erstellt wurden, verwenden Sie den Pool "Default".
Barcode	Geben Sie einen eindeutigen Strichcode an oder behalten Sie den Standardwert (*) bei, um eine Gruppe von Bändern zu importieren. Für Strichcodes können Sie die Platzhalter ? und * verwenden, wobei ? mit einem einzigen Zeichen und * mit 0 oder mehr Zeichen übereinstimmt.
Count	Geben Sie ein, wie viele Bänder maximal an Sie zurückgegeben werden sollen. Wenn Sie dieses Feld leer lassen, wird der Standardwert (*) für Strichcodes verwendet.
Tapes Per Page	Wählen Sie die maximale Anzahl der Bänder aus, die pro Seite angezeigt werden sollen. Die möglichen Werte sind 15, 30 und 45.
Items Selected	Zeigt die Anzahl der Bänder an, die auf mehreren Seiten ausgewählt sind. Dieser Wert wird automatisch für jede Bandauswahl aktualisiert.

3. Wählen Sie in der Liste mit den Suchergebnissen die zu verschiebenden Bänder aus.
4. Wählen Sie in der Liste „Select Destination“: „Location“ den Standort des Pools aus, an den Bänder verschoben werden sollen. Diese Option ist nur verfügbar, wenn aus der (benannten) Ansicht „Pool“ gestartet wird.
5. Klicken Sie auf **Next**.
6. Überprüfen Sie in der Ansicht „Move Tapes“ die Zusammenfassungsinformationen und die Bandliste und wählen Sie **Submit**.
7. Wählen Sie im Statusfenster **Close** aus.

Kopieren von Bändern zwischen Pools

Bänder können zwischen Pools oder vom Vault an einen Pool kopiert werden, um die Replikationsaktivitäten zu beherbergen. Diese Option ist nur verfügbar, wenn aus der (benannten) Ansicht „Pool“ gestartet wird.

Vorgehensweise

1. Wählen Sie mit einem hervorgehobenen Pool**More Tasks** > **Tapes** > **Copy**.
2. Aktivieren Sie im Dialogfeld „Copy Tapes Between Pools“ die Kontrollkästchen der zu kopierenden Bänder oder geben Sie Informationen ein, um nach den zu kopierenden Bändern zu suchen und wählen Sie „**Search**“:

Tabelle 177 Dialogfeld „Copy Tapes Between Pools“

Feld	Benutzereingabe
Location	Wählen Sie entweder eine Bibliothek oder den **Vault** für die Suche nach den Bändern aus. Obwohl Bänder immer in einem Pool (unter dem Menü „Pools“) angezeigt werden, befinden sie sich technisch in einer Bibliothek oder im Vault, aber nicht in beiden, und sind niemals in zwei Bibliotheken gleichzeitig. Verwenden Sie die Optionen zum Importieren/Exportieren, um Bänder zwischen dem Vault und einer Bibliothek zu verschieben.
Pools bilden	Wählen Sie zum Kopieren von Bändern zwischen Pools den Namen des Pools aus, in dem sich die Bänder derzeit befinden. Wenn keine Pools erstellt wurden, verwenden Sie den Pool **Default**.
Barcode	Geben Sie einen eindeutigen Strichcode an oder behalten Sie den Standardwert (*) bei, um eine Gruppe von Bändern zu importieren. Für Strichcodes können Sie die Platzhalter ? und * verwenden, wobei ? mit einem einzigen Zeichen und * mit 0 oder mehr Zeichen übereinstimmt.
Count	Geben Sie ein, wie viele Bänder maximal importiert werden sollen. Wenn Sie dieses Feld leer lassen, wird der Standardwert (*) für Strichcodes verwendet.
Tapes Per Page	Wählen Sie die maximale Anzahl der Bänder aus, die pro Seite angezeigt werden sollen. Die möglichen Werte sind 15, 30 und 45.
Items Selected	Zeigt die Anzahl der Bänder an, die auf mehreren Seiten ausgewählt sind. Dieser Wert wird automatisch für jede Bandauswahl aktualisiert.

3. Wählen Sie in der Liste mit den Suchergebnissen die zu kopierenden Bänder aus.
4. Wählen Sie in der Liste „Select Destination“: „Pool“ den Pool aus, in dem Bänder kopiert werden sollen. Wenn sich ein Band mit einem übereinstimmendem Strichcode bereits im Zielpool befindet, wird ein Fehler angezeigt und der Kopiervorgang wird abgebrochen.

5. Klicken Sie auf **Next**.
6. Überprüfen Sie im Dialogfeld „Copy Tapes Between Pools“ die Zusammenfassungsinformationen und die Bandliste und wählen Sie **Submit** aus.
7. Wählen Sie im Fenster „Copy Tapes Between Pools“ die Option **Close** aus.

Umbenennen von Pools

Ein Pool kann nur umbenannt werden, wenn keines seiner Bänder in einer Bibliothek ist.

Vorgehensweise

1. Wählen Sie**Pools** > **Pools** > ***pool***.
2. Wählen Sie **More Tasks** > **Pool** > **Rename**.
3. Geben Sie im Dialogfeld „Rename Pool“ den neuen Poolnamen unter Beachtung der folgenden Einschränkungen ein:
   - „all,“„vault“ oder „summary“ darf nicht verwendet werden.
   - Ein Poolname kann nicht mit einem Leerzeichen oder Punkt beginnen oder enden.
   - Die Groß-/Kleinschreibung muss beachtet werden.
4. Klicken Sie auf **OK**, um das Statusdialogfeld „Rename Pool“ anzuzeigen.
5. Nachdem im Statusdialogfeld „Rename Pool“ der Status `Completed` angezeigt wird, wählen Sie **OK**.

   Der Pool wird im Unterverzeichnis „Pools“ in den Bereichen „Pools“ und „Virtual Tape Libraries“ umbenannt.

KAPITEL 16

DD Replicator

Inhalt dieses Kapitels:

Überblick über DD Replicator

Data Domain Replicator (DD Replicator) ermöglicht eine automatisierte, Policy-basierte, netzwerkeffiziente und verschlüsselte Replikation für die Disaster Recovery (DR) und für die Konsolidierung von Backup und Archivierung über mehrere Standorte. DD Replicator repliziert nur komprimierte, deduplizierte Daten asynchron über das WAN (Wide Area Network).

DD Replicator führt zwei Stufen der Deduplizierung durch, um die Bandbreitenanforderungen erheblich zu reduzieren: *lokale* und *standortübergreifende* Deduplizierung. Die lokale Deduplizierung bestimmt die eindeutigen Segmente, die über ein WAN repliziert werden sollen. Wenn die Replikation von mehreren Standorten aus zum selben Zielsystem erfolgt, wird die erforderliche Bandbreite durch die standortübergreifende Deduplizierung weiter reduziert. Bei der standortübergreifenden Deduplizierung werden redundante Segmente, die bereits von einem anderen Standort übertragen wurden oder infolge eines lokalen Backups oder einer lokalen Archivierung vorliegen, nicht noch einmal repliziert. Dies verbessert die Netzwerkeffizienz aller Standorte und verringert die täglich benötigte Netzwerkbandbreite um bis zu 99 %, wodurch die netzwerkbasierte Replikation zu einer schnellen, zuverlässigen und kosteneffizienten Methode wird.

Zur Erfüllung eines breiten Spektrums von Disaster-Recovery-Anforderungen ermöglicht DD Replicator flexible Replikationstopologien wie die vollständige Systemspiegelung oder bidirektionale, n:1-, 1:n- oder kaskadierte Replikation. Außerdem können Sie festlegen, ob die Replikation auf Ihrem DD-System alle Daten oder nur einen Teil der Daten betreffen soll. Um höchsten Sicherheitsansprüchen gerecht zu werden, kann DD Replicator die zwischen DD-Systemen replizierten Daten mit dem SSL-Standardprotokoll (Secure Socket Layer) verschlüsseln.

Zur Unterstützung von größeren Unternehmensumgebungen skaliert DD Replicator die Performance und die unterstützten Fan-in-Verhältnisse.

Beachten Sie for dem Start von DD Replicator die folgenden allgemeinen Anforderungen:

- DD Replicator ist ein lizenziertes Produkt. Wenden Sie sich an Ihren Data Domain-Vertriebsmitarbeiter, um Lizenzen zu erwerben.
- Sie können in der Regel nur zwischen Computern replizieren, die maximal zwei Versionen auseinanderliegen, beispielsweise von 5.6 auf 6.0. Es gibt jedoch Ausnahmen dieser Regel (durch die atypische Versionsnummerierung). Sehen Sie sich hierzu die Tabellen im Abschnitt *Replikationsversionskompatibilität* an oder erkundigen Sie sich bei Ihrem Data Domain-Vertriebsmitarbeiter.
- Falls Sie DD Replicator nicht über die aktuelle Version von DD System Manager managen und überwachen können, verwenden Sie die `replication`-Befehle, die im *Data Domain Operating System Command Reference Guide* beschrieben werden.

Voraussetzungen für die Replikationskonfiguration

Prüfen Sie vor dem Konfigurieren einer Replikation die folgenden Voraussetzungen, um die für die erstmalige Datenübertragung benötigte Zeit zu verkürzen, um zu verhindern, dass Daten überschrieben werden usw.

- **Kontexte**: Ermitteln Sie die maximale Anzahl von Kontexten für Ihre DD-Systeme anhand der Replikationsstreams in der folgenden Tabelle.

  Tabelle 178 An ein Data Domain-System gesendete Datenstreams

Modell	RAM/NVRAM	Backupschreibstreams	Backuplesestreams	Repl[a]-Quellstreams	Repl[a]-Zielstreams	Gemischt
DD140, DD160, DD610	4 GB oder 6 GB/0,5 GB	16	4	15	20	w<= 16 ; r<= 4 ReplSrc<=15; ReplDest<=20; ReplDest+w<=16; w+r+ReplSrc <=16;Total<=20
DD620, DD630, DD640	8 GB/0,5 GB oder 1 GB	20	16	30	20	w<=20; r<=16; ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; Total<=30
DD640, DD670	16 GB oder 20 GB/1 GB	90	30	60	90	w<=90; r<=30; ReplSrc<=60; ReplDest<=90; ReplDest+w<=90; Total<=90
DD670, DD860	36 GB/1 GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD860	72 GB[b]/1 GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD890	96 GB/2 GB	180	50	90	180	w<=180; r<=50; ReplSrc <=90;ReplDest<=180; ReplDest +w<=180; Total<=180
DD990	128 oder 256 GB[b]/4 GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD2200	8 GB	20	16	16	20	w<=20; r<=16; ReplSrc<=16; ReplDest<=20; ReplDest+w<=20; Total<=20
DD2200	16 GB	60	16	30	60	w<=60; r<=16; ReplSrc<=30; ReplDest<=60; ReplDest+w<=60; Total<=60
DD2500	32 GB oder 64 GB/2 GB	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; Total<=180
DD4200	128 GB[b]/4 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270

Tabelle 178 An ein Data Domain-System gesendete Datenstreams (Fortsetzung)

Modell	RAM/NVRAM	Backupschreibstreams	Backuplesestreams	Repl[a]-Quellstreams	Repl[a]-Zielstreams	Gemischt
DD4500	192 GB[b]/4 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD7200	128 oder 256 GB[b]/4 GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD9500	256/512 GB	1.885	300	540	1.080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest +w<=1080; Total<=1885
DD9800	256/768 GB	1.885	300	540	1.080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest +w<=1080; Total<=1885
DD6300	48/96 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD6800	192 GB	400	110	220	400	w<=400; r<=110; ReplSrc<=220; ReplDest<=400; ReplDest +w<=400; Total<=400
DD9300	192/384 GB	800	220	440	800	w<=800; r<=220; ReplSrc<=440; ReplDest<=800; ReplDest +w<=800; Total<=800
Data Domain Virtual Edition (DD VE)	6 TB oder 8 TB oder 16 TB/ 0,5 TB oder 32 TB oder 48 TB oder 64 TB oder 96 TB	16	4	15	20	w<= 16 ; r<= 4 ReplSrc<=15; ReplDest<=20; ReplDest+w<=16; w+r+ReplSrc <=16;Total<=20

a. DirRepl, OptDup, MTreeRepl-Streams
b. Die Data Domain Extended Retention-Softwareoption ist für diese Geräte nur mit erweitertem (maximalem) Arbeitsspeicher verfügbar.

- **Kompatibilität**: Wenn auf Ihren DD-Systemen unterschiedliche Versionen von DD OS ausgeführt werden, lesen Sie den nachfolgenden Abschnitt über die Versionskompatibilität bei der Replikation.
- **Erste Replikation**: Wenn in der Quelle viele Daten gespeichert werden, kann der Replikationsvorgang mehrere Stunden in Anspruch nehmen. Überlegen Sie, ob es sinnvoll ist, beide DD-Systeme über eine schnelle Verbindung mit niedriger Latenz an denselben Speicherort zu verschieben. Nach der ersten Replikation können Sie die Systeme an die geplanten Speicherorte verschieben, da dann nur noch neue Daten gesendet werden.
- **Einstellungen für die Bandbreitenverzögerung**: Quelle und Ziel müssen über dieselben Bandbreitenverzögerungseinstellungen verfügen. Diese Tuningkontrollen verbessern die Replikationsperformance über Verbindungen mit höherer Latenz

durch Festlegen der entsprechenden TCP-Puffergröße (Transmission Control Protocol). Das Quellsystem kann dann genügend Daten an das Ziel senden, während es auf eine Bestätigung wartet.

- **Nur ein Kontext für Verzeichnisse/Unterverzeichnisse**: Ein Verzeichnis (und die entsprechenden Unterverzeichnisse) kann sich immer jeweils nur in einem Kontext befinden. Achten Sie daher darauf, dass ein Unterverzeichnis in einem Quellverzeichnis nicht in einem anderen Verzeichnisreplikationskontext verwendet wird.
- **Genügend Speicherplatz**: Das Ziel muss mindestens über *genauso viel Speicherplatz* verfügen wie die Quelle.
- **Leeres Ziel für Verzeichnisreplikation**: Bei einer Verzeichnisreplikation muss das Zielverzeichnis leer sein oder die Inhalte dürfen nicht mehr benötigt werden, da sie überschrieben werden.
- **Sicherheit** – DD OS erfordert, dass Port 3009 offen ist, damit eine sichere Replikation über eine Ethernetverbindung konfiguriert werden kann.

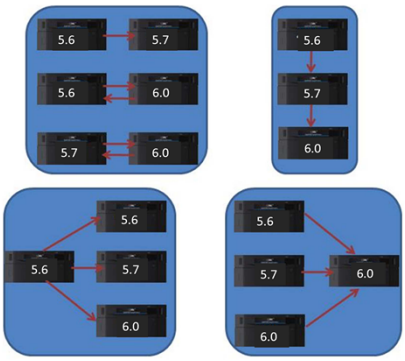
Replikationsversionskompatibilität

Für die Verwendung von DD-Systemen mit unterschiedlichen DD OS-Versionen auf Quelle und Ziel finden Sie in den folgenden Tabellen Informationen zur Kompatibilität für folgende Replikationen: Single Node, DD Extended Retention, DD Retention Lock, MTree, Verzeichnis, Sammlung, Delta (Optimierung bei geringer Bandbreite) und kaskadiert.

Allgemein gilt:

- Unterstützte Konfigurationen für DD Boost oder OST finden Sie unter „Optimized Duplication Version Compatibility“ im *Data Domain Boost for Partner Integration Administration Guide* oder im *Data Domain Boost for OpenStorage Administration Guide*.
- MTree- und Verzeichnisreplikation können nicht gleichzeitig für die Replikation derselben Daten verwendet werden.
- Das Recovery-Verfahren gilt für alle unterstützten Replikationskonfigurationen.
- Die Dateimigration wird unterstützt, wenn die Sammelreplikation unterstützt wird.
- Die MTree-Replikation zwischen einem DD-Quellsystem, auf dem DD OS 5.2.x ausgeführt wird, und einem DD-Zielsystem, auf dem DD OS 5.4.x oder DD OS 5.5.x ausgeführt wird, wird nicht unterstützt, wenn DD Retention Lock Governance auf dem Quell-MTree aktiviert ist.
- Bei einer MTree-Replikation von einem DD-Quellsystem mit DD OS 6.0 auf ein DD-Zielsystem mit einer früheren Version von DD OS verhält sich der Replikationsprozess gemäß der älteren Version von DD OS auf dem DD-Zielsystem. Wenn ein Wiederherstellungsvorgang oder eine kaskadierte Replikation vom DD-Zielsystem durchgeführt wird, werden keine virtuellen synthetischen Backups angewendet.
- Bei kaskadierten Konfigurationen beträgt die maximale Anzahl Hops zwei, d. h. drei DD-Systeme.
  Die Verzeichnis-zu-MTree-Replikation unterstützt Abwärtskompatibilität für bis zu zwei frühere Versionen. Weitere Informationen zur Verzeichnis-zu-Mtree-Migration finden Sie unter Replikationsmigration (Verzeichnis zu MTree) auf Seite 475.
- 1:n-, n:1- und kaskadierte Replikationen unterstützen bis zu drei aufeinander folgende DD OS-Versionsreihen (wie in den folgenden Abbildungen dargestellt).

Abbildung 9 Gültige Replikationskonfigurationen



Für die nachfolgenden Tabellen gilt Folgendes:

- Jede DD OS-Version beinhaltet alle Versionen in dieser Reihe. Beispiel: DD OS 5.7 beinhaltet 5.7.1, 5.7.x, 6.0 usw.
- S = Sammelreplikation
- Verz = Verzeichnisreplikation
- M = MTree-Replikation
- Del = Delta-Replikation (Optimierung bei geringer Bandbreite)
- Ziel = Ziel
- Quell = Quelle
- NA = nicht zutreffend

Tabelle 179 Konfiguration: Single-Node zu Single-Node

	5.0 (Ziel)	5.1 (Ziel)	5.2 (Ziel)	5.3 (Ziel)	5.4 (Ziel)	5.5 (Ziel)	5.6 (Ziel)	5.7 (Ziel)	6.0 (Ziel)	6.1 (Ziel)
5.0 (Quell)	S, Verz, Del	Verz, Del	Verz, Del	NA	NA	NA	NA	NA	NA	NA
5.1 (Quell)	Verz, Del	C, Verz, Del, M[a]	Verz, Del, M[a]	Verz, Del, M[a]	Verz, Del, M[a]	NA	NA	NA	NA	NA
5.2 (Quell)	Verz, Del	Verz, Del, M[a]	C, Verz, Del, M[b]	Verz, Del, M	Verz, Del, M	Verz, Del, M	NA	NA	NA	NA
5.3 (Quell)	NA	Verz, Del, M[a]	Verz, Del, M	S, Verz, Del, M	Verz, Del, M	Verz, Del, M	NA	NA	NA	NA
5.4 (Quell)	NA	Verz, Del, M[a]	Verz, Del, M	Verz, Del, M	S, Verz, Del, M	Verz, Del, M	Verz, Del, M	NA	NA	NA
5.5 (Quell)	NA	NA	Verz, Del, M	Verz, Del, M	Verz, Del, M	S, Verz, Del, M	Verz, Del, M	Verz, Del, M	NA	NA
5.6 (Quell)	NA	NA	NA	NA	Verz, Del, M	Verz, Del, M	S, Verz, Del, M	Verz, Del, M	Verz, Del, M	NA
5.7 (Quell)	NA	NA	NA	NA	NA	Verz, Del, M	Verz, Del, M	S, Verz, Del, M	Verz, Del, M	Verz, Del, M
6.0 (Quelle)	NA	NA	NA	NA	NA	NA	Verz, Del, M	Verz, Del, M	S, Verz, Del, M	Verz, Del, M
6.1 (Quell)	NA	NA	NA	NA	NA	NA	NA	Verz, Del, M	Verz, Del, M	S, Verz, Del, M

a. MTree-Replikation wird für DD VTL nicht unterstützt.
b. Sammelreplikation wird nur für Compliancedaten unterstützt.

Tabelle 180 Konfiguration: DD Extended Retention zu DD Extended Retention

	5.0 (Ziel)	5.1 (Ziel)	5.2 (Ziel)	5.3 (Ziel)	5.4 (Ziel)	5.5 (Ziel)	5.6 (Ziel)	5.7 (Ziel)	6.0 (Ziel)	6.1 (Ziel)
5.0 (Quell)	c	NA	NA	NA	NA	NA	NA	NA	NA	NA
5.1 (Quell)	NA	c	M[a]	M[b]	M[b]	NA	NA	NA	NA	NA
5.2 (Quell)	NA	M[a]	S, M[a]	M[a]	M[a]	M[a]	NA	NA	NA	NA
5.3 (Quell)	NA	M[c]	M[c]	S, M	m	m	NA	NA	NA	
5.4 (Quell)	NA	M[c]	M[c]	m	S, M	m	m	NA	NA	NA
5.5 (Quell)	NA	NA	M[c]	m	m	S, M	m	m	NA	NA

Tabelle 180 Konfiguration: DD Extended Retention zu DD Extended Retention (Fortsetzung)

	5.0 (Ziel)	5.1 (Ziel)	5.2 (Ziel)	5.3 (Ziel)	5.4 (Ziel)	5.5 (Ziel)	5.6 (Ziel)	5.7 (Ziel)	6.0 (Ziel)	6.1 (Ziel)
5.6 (Quell)	NA	NA	NA	NA	m	m	S, M	m	m	
5.7 (Quell)	NA	NA	NA	NA	NA	m	m	S, M	m	m
6.0 (Quelle)	NA	NA	NA	NA	NA	NA	m	m	S, M	m
6.1 (Quell)	NA	NA	NA	NA	NA	NA	NA	m	m	S, M

a. Dateimigration wird bei MTree-Replikation auf der Quelle oder auf dem Ziel in dieser Konfiguration nicht unterstützt.
b. Dateimigration wird bei MTree-Replikation auf der Quelle in dieser Konfiguration nicht unterstützt.
c. Dateimigration wird bei MTree-Replikation auf dem Ziel in dieser Konfiguration nicht unterstützt.

Tabelle 181 Konfiguration: Single-Node zu DD Extended Retention

	5.0 (Ziel)	5.1 (Ziel)	5.2 (Ziel)	5.3 (Ziel)	5.4 (Ziel)	5.5 (Ziel)	5.6 (Ziel)	5.7 (Ziel)	6.0 (Ziel)	6.1 (Ziel)
5.0 (Quell)	Verz	Verz	NA	NA	NA	NA	NA	NA	NA	NA
5.1 (Quell)	Verz	Verz, M[a]	Verz, M[a]	Verz, M	Verz, M	NA	NA	NA	NA	NA
5.2 (Quell)	Verz	Verz, M[a]	Verz, M[a]	Verz, M	Verz, M	Verz, M	NA	NA	NA	NA
5.3 (Quell)	NA	Verz, M[a]	Verz, M[a]	Verz, M	Verz, M	Verz, M	NA	NA	NA	NA
5.4 (Quell)	NA	Verz, M[a]	Verz, M[a]	Verz, M	Verz, M	Verz, M	Verz, M	NA	NA	NA
5.5 (Quell)	NA	NA	Verz, M[a]	Verz, M	Verz, M	Verz, M	Verz, M	Verz, M	NA	NA
5.6 (Quell)	NA	NA	NA	NA	Verz, M	Verz, M	Verz, M	Verz, M	Verz, M	NA
5.7 (Quell)	NA	NA	NA	NA	NA	Verz, M	Verz, M	Verz, M	Verz, M	Verz, M
6.0 (Quell)	NA	NA	NA	NA	NA	NA	Verz, M	Verz, M	Verz, M	Verz, M
6.1 (Quell)	NA	NA	NA	NA	NA	NA	NA	Verz, M	Verz, M	Verz, M

a. Dateimigration wird in dieser Konfiguration nicht unterstützt.

Replikationstypen

Die Replikation umfasst in der Regel ein DD-*Quell*system (das Daten von einem Backupsystem empfängt) und ein oder mehrere DD-*Ziel*systeme. Jedes DD-System kann als Quelle und/oder Ziel für Replikationskontexte dienen. Während der Replikation kann jedes DD-System auch normale Backup- und Wiederherstellungsvorgänge ausführen.

Jeder Replikationstyp legt einen *Kontext* fest, der einem vorhandenen Verzeichnis oder MTree auf der Quelle zugeordnet ist. Der replizierte Kontext wird auf dem Ziel erstellt, sobald ein Kontext festgelegt ist. Der Kontext legt ein Replikationspaar fest, das immer aktiv ist. Alle bei der Quelle eingehenden Daten werden so bald wie möglich in das Ziel kopiert. In Replikationskontexten konfigurierte Pfade sind absolute Verweise, die sich nicht basierend auf dem System, auf dem sie konfiguriert sind, ändern.

Ein Data Domain-System kann für die Replikation von Verzeichnissen, Sammlungen oder MTrees eingerichtet werden.

- *Verzeichnisreplikation* findet auf Ebene der einzelnen Verzeichnisse statt.
- Bei der *Sammelreplikation* wird der gesamte Datenspeicher auf der Quelle kopiert und an das Ziel übertragen. Dabei ist das replizierte Volume schreibgeschützt.

- Bei der *MTree-Replikation* werden ganze MTrees (d. h. eine virtuelle Dateistruktur, die ein erweitertes Management ermöglicht) repliziert. Medienpools können ebenfalls repliziert werden. Ab DD OS 5.3 wird standardmäßig ein MTree erstellt, der repliziert wird. (Ein Medienpool kann auch im Abwärtskompatibilitätsmodus erstellt werden, der bei der Replikation als Verzeichnisreplikationskontext dient.)

Für alle Replikationstypen gelten die folgenden Anforderungen:

- Auf einem Data Domain-Zielsystem muss mindestens so viel Speicherkapazität verfügbar sein, dass sie der Größe der erwarteten maximalen Quellverzeichnisgröße entspricht. Vergewissern Sie sich, dass auf dem Data Domain-Zielsystem genügend Netzwerkbandbreite und Speicherplatz für den Datenverkehr von den Replikationsquellen vorhanden ist.
- Das Dateisystem muss aktiviert sein oder es wird je nach Replikationstyp im Rahmen der Replikationsinitialisierung aktiviert.
- Die Quelle muss vorhanden sein.
- Das Ziel darf nicht bereits vorhanden sein.
- Das Ziel wird beim Erstellen oder Initialisieren eines Kontexts erstellt.
- Nach Beginn der Replikation sind Eigentumsrechte und Berechtigungen des Ziels immer mit denen der Quelle identisch.
- In den Replikationsbefehlsoptionen wird das jeweilige Replikationspaar immer durch das Ziel identifiziert.
- Beide Systeme müssen eine aktive, sichtbare Route durch das IP-Netzwerk aufweisen, sodass jedes System den Hostnamen seines Partners auflösen kann.

Die Wahl des Replikationstyps hängt von Ihren spezifischen Anforderungen ab. Die nachfolgenden Abschnitte enthalten Beschreibungen und Funktionen der drei Typen sowie eine kurze Einführung in die gemanagte Dateireplikation, die von DD Boost verwendet wird.

Managed File Replication

Managed File Replication, die von DD Boost verwendet wird, ist eine Art der Replikation, die von Backupsoftware verwaltet und gesteuert wird.

Mit Managed File Replication werden Backup-Images einzeln direkt von einem DD-System auf ein anderes übertragen, auf Anfrage von der Backupsoftware.

Die Backupsoftware verfolgt sämtliche Kopien und ermöglicht so ein einfaches Monitoring des Replikationsstatus und eine Recovery von mehreren Kopien.

Manged File Replication bietet flexible Replikationstopologien, einschließlich einer vollständigen Systemspiegelung, bidirektional, n: 1 und kaskadiert, und ermöglicht so eine effiziente Deduplizierung zwischen verschiedenen Standorten.

Hier sind einige weitere Aspekte, die bei der Managed File Replication zu beachten sind:

- Replikationskontexte müssen nicht konfiguriert werden.
- Lebenszyklusrichtlinien steuern die Replikation von Informationen ohne Benutzereingriff.
- DD Boost erstellt und entfernt Kontexte bei Bedarf im laufenden Betrieb.

Weitere Informationen finden Sie unter den `ddboost file-replication`-Befehlen im *Data Domain Operating System Command Reference Guide*.

Verzeichnisreplikation

Bei der *Verzeichnisreplikation* werden deduplizierte Daten innerhalb eines DD-Dateisystemverzeichnisses als Replikationsquelle in ein Verzeichnis übertragen, das als Replikationsziel auf einem anderen System konfiguriert wurde.

Bei der Verzeichnisreplikation kann ein DD-System gleichzeitig die Quelle einiger Replikationskontexte und das Ziel für andere Kontexte sein. Außerdem kann dieses DD-System bei der Datenreplikation Daten von Backup- und Archivierungsanwendungen empfangen.

Die Verzeichnisreplikation hat dieselben flexiblen Topologien für die Netzwerkbereitstellung und verfügt über dieselben standortübergreifenden Deduplizierungseffekte wie die gemanagte Dateireplikation (der von DD Boost verwendete Typ).

Hier sind einige zusätzliche zu beachtende Aspekte, wenn die Verzeichnisreplikation verwendet wird:

- CIFS- und NFS-Daten dürfen nicht im selben Verzeichnis abgelegt sein. Ein einzelnes Data Domain-Zielsystem kann Backups von CIFS- und NFS-Clients empfangen, solange hierzu für CIFS und NFS separate Verzeichnisse verwendet werden.
- Ein Verzeichnis kann nur jeweils in einem Kontext vorliegen. Ein übergeordnetes Verzeichnis darf in einem Replikationskontext nicht verwendet werden, wenn ein untergeordnetes Verzeichnis dieses Verzeichnisses bereits repliziert wird.
- Das Umbenennen (Verschieben) von Dateien oder Bändern *in oder aus* ein(em) Verzeichnisreplikations-Quellverzeichnis heraus ist *nicht* zulässig. Das Umbenennen von Dateien oder Bändern *innerhalb* eines Verzeichnisreplikations-Quellverzeichnisses *ist* zulässig.
- Auf einem DD-Zielsystem muss mindestens so viel Speicherkapazität verfügbar sein, dass sie der nachkomprimierten Größe der erwarteten maximalen nachkomprimierten Größe des Quellverzeichnisses entspricht.
- Beim Start der Replikation wird ein Zielverzeichnis automatisch erstellt.
- Nach Beginn der Replikation sind Eigentumsrechte und Berechtigungen im Zielverzeichnis mit denen im Quellverzeichnis identisch. Solange der Kontext vorhanden ist, wird das Zielverzeichnis im schreibgeschützten Status aufbewahrt und kann nur Daten vom Quellverzeichnis empfangen.
- Aufgrund von Unterschieden bei der globalen Komprimierung können sich Quell- und Zielverzeichnis in der Größe voneinander unterscheiden.

Empfehlungen zum Erstellen von Ordnern

Bei der Verzeichnisreplikation werden Daten auf dem Level der einzelnen Unterverzeichnisse unter `/data/col1/backup` repliziert.

Um eine fein abgestimmte Trennung von Daten zu ermöglichen, müssen Sie auf einem Hostsystem andere Verzeichnisse (DirA, DirB usw.) im MTree „/backup“ erstellen. Jedes Verzeichnis muss auf Ihrer Umgebung basieren und diese Verzeichnisse müssen an einen anderen Speicherort repliziert werden. Es wird nicht der gesamte MTree „/backup“ repliziert. Stattdessen richten Sie in jedem Unterverzeichnis unterhalb von „/data/col1/backup/ (Bsp. /data/col1/backup/DirC) Replikationskontexte ein. Damit werden drei Zwecke erfüllt:

- Es ermöglicht die Kontrolle der Zielspeicherorte, das DirA an einen Standort geht und DirB an einen anderen.

- Durch dieses Maß an Feinabstimmung sind Management, Monitoring und Fehlerisolierung möglich. Jeder Replikationskontext kann angehalten, beendet, gelöscht oder gemeldet werden.
- Die Performance ist in einem einzelnen Kontext begrenzt. Durch die Erstellung mehrerer Kontexte kann die Performance der gesamten Replikation verbessert werden.
- Generell wird empfohlen, etwa fünf bis zehn Kontexte zu erstellen, um die Replikationslast auf mehrere Replikationsstreams zu verteilen. Dies muss mit dem Standortdesign, dem Volume und der Zusammensetzung der Daten am Standort abgestimmt werden.

Hinweis

Die Empfehlung einer bestimmten Anzahl von Kontexten ist eine Frage des Designs und in einigen Fällen sind mit der Entscheidung für die Trennung von Daten zur Optimierung der Replikation erhebliche Beeinträchtigungen verbunden. Daten sind in der Regel für die Art und Weise, wie sie gespeichert werden, optimiert, und nicht für die Art und Weise, wie sie repliziert werden. Beachten Sie dies, wenn Sie eine Backupumgebung ändern.

MTree-Replikation

Die *MTree-Replikation* wird für die Replikation von MTrees zwischen DD-Systemen verwendet. Es werden an der Quelle regelmäßige Snapshots erstellt. Die Unterschiede werden an das Ziel übertragen, indem derselbe standortübergreifende Deduplizierungsmechanismus wie bei der Verzeichnisreplikation verwendet wird. Diese Vorgehensweise sorgt dafür, dass die Daten auf dem Ziel immer eine Point-in-Time-Kopie der Quelle mit Dateikonsistenz sind. Hierdurch werden außerdem Replikationsprobleme in den Daten reduziert und eine effizientere WAN-Auslastung erzielt.

Bei der MTree-Replikation kann ein DD-System gleichzeitig die Quelle einiger Replikationskontexte und das Ziel für andere Kontexte sein. Außerdem kann dieses DD-System bei der Datenreplikation Daten von Backup- und Archivierungsanwendungen empfangen.

Die MTree-Replikation verfügt über dieselben flexiblen Topologien für die Netzwerkbereitstellung und standortübergreifenden Deduplizierungseffekte wie die verwaltete Dateireplikation (der von DD Boost verwendete Typ).

Hier sind einige weitere Aspekte, die bei der Verwendung der MTree-Replikation zu beachten sind:

- Beim Start der Replikation wird automatisch ein schreibgeschütztes Ziel-MTree erstellt.
- Daten können zur Optimierung der Replikationsperformance logisch in mehrere MTrees getrennt werden.
- Snapshots müssen in Quellkontexten erstellt werden.
- Snapshots können nicht an einem Replikationsziel erstellt werden.
- Snapshots werden mit einer fixen Aufbewahrungsfrist von einem Jahr erstellt. Die Aufbewahrungsfrist kann und muss jedoch auf dem Ziel angepasst werden.
- Replikationskontexte müssen sowohl auf der Quelle als auch auf dem Ziel konfiguriert werden.
- Bei der Replikation von DD VTL-Bandkassetten (oder Pools) werden lediglich MTrees oder Verzeichnisse repliziert, die DD VTL-Bandkassetten enthalten.

Medienpools werden standardmäßig mittels MTree-Replikation repliziert. Ein Medienpool kann im Abwärtskompatibilitätsmodus erstellt und anschließend mittels verzeichnisbasierter Replikation repliziert werden. Beim Erstellen von Replikationskontexten über die Befehlszeile kann die Syntax „pool://“ nicht verwendet werden. Beim Festlegen einer poolbasierten Replikation in DD System Manager wird je nach Medienpooltyp eine Verzeichnis- oder MTree-Replikation erstellt.

- Die Replikation von Verzeichnissen unter einem MTree ist nicht zulässig.
- Auf einem DD-Zielsystem muss mindestens so viel Speicherkapazität verfügbar sein, dass sie der nachkomprimierten Größe der erwarteten maximalen nachkomprimierten Größe des Quell-MTree entspricht.
- Nach Beginn der Replikation sind Eigentumsrechte und Berechtigungen des Ziel-MTree immer mit denen des Quell-MTree identisch. Wenn der Kontext konfiguriert ist, ist der Ziel-MTree schreibgeschützt und kann nur Daten vom Quell-MTree empfangen.
- Aufgrund von Unterschieden bei der globalen Komprimierung können sich Quell- und Ziel-MTree in der Größe voneinander unterscheiden.
- Die MTree-Replikation von DD Extended Retention-Systemen auf Nicht-DD Extended Retention-Systeme wird unterstützt, wenn auf beiden Systemen DD OS 5.5 oder höher ausgeführt wird.
- DD Retention Lock Compliance wird mit der MTree-Replikation standardmäßig unterstützt. Wenn DD Retention Lock auf einer Quelle lizenziert ist, muss das Ziel ebenfalls über eine DD Retention Lock-Lizenz verfügen, da sonst bei der Replikation ein Fehler auftritt (Zur Vermeidung dieser Situation müssen Sie DD Retention Lock deaktivieren). Wenn DD Retention Lock in einem Replikationskontext aktiviert ist, enthält ein replizierter Zielkontext immer mit einer Aufbewahrungssperre versehene Daten.

Automatic Multi-Streaming (AMS)

Automatic Multi-Streaming (AMS) verbessert die Performance der MTree-Replikation. Es nutzt mehrere Streams für die Replikation einer einzigen großen Datei (32 GB oder größer) zur Verbesserung der Auslastung der Netzwerkbandbreite während der Replikation. Durch die Erhöhung der Replikationsgeschwindigkeit für individuelle Dateien verbessert AMS auch die Pipeline-Effizienz der Replikationswarteschlange und sorgt für einen besseren Replikationsdurchsatz und eine reduzierte Replikationsverzögerung.

Wenn die Workload mehrere Optimierungsoptionen bietet, wählt AMS automatisch die beste Option für die Workload aus. Wenn die Workload beispielsweise eine große Datei mit Fastcopy-Attributen ist, verwendet die Replikation Fastcopy-Optimierung, um den Overhead für das Scannen der Datei zu vermeiden und so eindeutige Segmente zwischen dem Replikationspaar zu identifizieren. Wenn die Workload Synthetics verwendet, nutzt die Replikation synthetische Replikation zusätzlich zu AMS, um lokale Vorgänge auf dem Zielsystem für jeden Replikationsstream zu nutzen und so die Datei zu erzeugen.

AMS ist immer aktiviert und kann nicht deaktiviert werden.

Sammelreplikation

Bei der *Sammelreplikation*wird das gesamte System in einer 1:1-Topologie gespiegelt, indem kontinuierlich Änderungen in der zugrunde liegenden Sammlung (einschließlich sämtlicher logischer Verzeichnisse und Dateien im DD-Dateisystem) übertragen werden.

Die Sammelreplikation verfügt nicht über die Flexibilität der anderen Arten, kann jedoch einen höheren Durchsatz bieten und unterstützt mehr Objekte mit weniger Overhead, was sich u. U. besser für geschäftliche Fälle mit hoher Skalierung eignet.

Bei der Sammelreplikation wird der gesamte Bereich `/data/col1` von einem DD-Quellsystem an ein DD-Zielsystem repliziert.

Hinweis

Sammelreplikation wird für Systeme nicht unterstützt, die für Cloud-Tier aktiviert sind.

Hier sind einige zusätzliche zu beachtende Aspekte bei Verwendung der Sammelreplikation:

- Eine fein abgestimmte Replikationssteuerung ist nicht möglich. Alle Daten werden von der Quelle auf das Ziel kopiert, wobei eine schreibgeschützte Kopie erstellt wird.
- Bei der Sammelreplikation muss die Kapazität des Zielspeichers größer oder gleich der Kapazität des Quellsystems sein. Wenn die Zielkapazität kleiner als die Quellkapazität ist, wird die verfügbare Kapazität der Quelle auf die Kapazität des Ziels reduziert.
- Das als Sammelreplikationsziel zu verwendende DD-System muss leer sein, bevor die Replikation konfiguriert wird. Nach der Konfiguration der Replikation empfängt dieses System Daten vom Quellsystem.
- Bei der Sammelreplikation werden sämtliche Benutzerkonten und Passwörter von der Quelle auf das Ziel repliziert. Ab DD OS 5.5.1.0 werden jedoch andere Elemente der Konfiguration und Benutzereinstellungen des DD-Systems nicht auf dem Ziel repliziert. Sie müssen sie nach der Replikation explizit neu konfigurieren.
- Sammelreplikation wird mit DD Secure Multitenancy (SMT) unterstützt. Core-SMT-Informationen, enthalten im Registry Namespace, einschließlich der Mandanten- und Mandanteneinheitdefinitionen mit entsprechenden UUIDs werden automatisch während der Replikation übertragen. Die folgenden SMT-Informationen sind nicht automatisch für die Replikation enthalten und müssen manuell auf dem Zielsystem konfiguriert werden:
  - Warnmeldungsbenachrichtigungslisten für jede Mandanteneinheit
  - Alle Benutzer, die dem DD Boost-Protokoll von SMT-Mandanten zugewiesen sind, wenn DD Boost auf dem System konfiguriert ist
  - Die Standardmandanteneinheit, die mit jedem DD Boost-Benutzer verbunden ist, falls vorhanden, wenn DD Boost auf dem System konfiguriert ist

  Verwenden der Sammelreplikation zur Disaster Recovery mit SMT auf Seite 480 beschreibt, wie diese Elemente manuell auf dem Replikationsziel konfiguriert werden.
- DD Retention Lock Compliance unterstützt die Sammelreplikation.
- Die Sammelreplikation wird in für Cloud-Tier aktivierten Systemen nicht unterstützt.
- Bei Sammelreplikation können Daten in einem Replikationskontext auf dem Quellsystem, die nicht repliziert wurden, nicht für die Dateisystembereinigung verarbeitet werden. Wenn die Dateisystembereinigung nicht abgeschlossen werden kann, da die Quell- und Zielsysteme nicht synchron sind, meldet das System den Status des Bereinigungsvorgangs als `partial`und nur begrenzte Systemstatistiken sind für die Bereinigung verfügbar. Wenn die Sammelreplikation

deaktiviert ist, steigt die Menge an Daten, die für die Dateisystembereinigung nicht verarbeitet werden können, da Quell- und Zielsysteme der Replikation nicht synchron sind. KB-Artikel *Data Domain: An overview of Data Domain File System (DDFS) clean/garbage collection (GC) phases*, verfügbar auf der Online Support-Website unter https://support.emc.com bietet weitere Informationen.

- Um den Durchsatz in einer Umgebung mit hoher Bandbreite zu verbessern, führen Sie den Befehl `replication modify <destination> crepl-gc-gw-optim` aus, um die Bandbreitenoptimierung für die Sammelreplikation zu deaktivieren.

Verwenden von DD Encryption mit DD Replicator

DD Replicator kann mit der optionalen Funktion *DD Encryption* verwendet werden, wodurch verschlüsselte Daten mithilfe der Sammel-, Verzeichnis- oder MTree-Replikation repliziert werden können.

Replikationskontexte werden immer mit einem *gemeinsamen geheimen Schlüssel* authentifiziert. Dieser gemeinsame geheime Schlüssel wird dazu verwendet, mithilfe eines Diffie-Hellman-Schlüsselaustauschprotokolls einen Sitzungsschlüssel zu erstellen. Dieser Sitzungsschlüssel wird dazu verwendet, den Chiffrierschlüssel des Data Domain-Systems zu verschlüsseln und ggf. zu entschlüsseln.

Jeder Replikationstyp funktioniert auf andere Weise mit Verschlüsselung und bietet das gleiche Sicherheitslevel.

- Bei der Sammelreplikation müssen Quelle und Ziel die gleiche Verschlüsselungskonfiguration haben, da die Zieldaten ein exaktes Replikat der Quelldaten sein sollen. Insbesondere muss die Verschlüsselungsfunktion sowohl an der Quelle als auch am Ziel aktiviert oder deaktiviert werden und, wenn die Funktion aktiviert wird, müssen zudem der Verschlüsselungsalgorithmus und die Systempassphrasen übereinstimmen. Die Parameter werden während der Replikationsverknüpfungsphase geprüft.
  Während der Sammelreplikation überträgt die Quelle die Daten in verschlüsselter Form und überträgt außerdem die Chiffrierschlüssel an das Ziel. Die Daten können am Ziel wiederhergestellt werden, da dieses dieselbe Passphrase und denselben Systemchiffrierschlüssel hat.

  Hinweis

  Sammelreplikation wird für Systeme nicht unterstützt, bei denen Cloud-Tiering aktiviert ist.

- Bei der *MTree- und der Verzeichnisreplikation* muss die Verschlüsselungskonfiguration an Quelle und Ziel nicht identisch sein. Stattdessen erfolgt während der Replikationsverknüpfungsphase ein sicherer Austausch des Chiffrierschlüssels des Ziels zwischen Quelle und Ziel. Die Daten werden entschlüsselt und anschließend mithilfe des Chiffrierschlüssels des Ziels erneut an der Quelle verschlüsselt, bevor die Daten an das Ziel übertragen werden.
  Wenn das Ziel eine abweichende Verschlüsselungskonfiguration hat, werden die übertragenen Daten entsprechend vorbereitet. Wenn die Funktion beispielsweise am Ziel deaktiviert ist, werden die Daten an der Quelle entschlüsselt und unverschlüsselt ans Ziel gesendet.
- Bei einer *kaskadierten Replikationstopologie* ist das Replikat mit mindestens drei Data Domain-Systemen verkettet. Das letzte System in der Kette kann als Sammlung, MTree oder Verzeichnis konfiguriert werden. Wenn das letzte System ein Sammelreplikationsziel ist, werden dieselben Chiffrierschlüssel und verschlüsselten Daten wie für die Quelle verwendet. Wenn das letzte System ein

MTree- oder Verzeichnisreplikationsziel ist, werden die Schlüssel dieses Systems verwendet und die Daten an der Quelle verschlüsselt. Für die Verschlüsselung wird der Chiffrierschlüssel für das Ziel an jedem Link verwendet. Die Verschlüsselung für Systeme in den Ketten funktioniert wie in einem Replikationspaar.

Replikationstopologien

DD Replicator unterstützt fünf Replikationstopologien (One-to-One, One-to-One bidirektional, 1:n, n:1 und kaskadiert). In den Tabellen in diesem Abschnitt wird erläutert, (1) wie diese Topologien mit drei Replikationsverfahren (MTree, Verzeichnis und Sammlung) und zwei Arten von DD-Systemen [Single Node (SN) und DD Extended Retention] verwendet werden und (2) wie gemischte Topologien mit kaskadierter Replikation unterstützt werden.

Allgemein gilt:

- SN-Systeme (Single Node) unterstützen alle Replikationstopologien.
- Single Node-to-Single Node (SN -> SN) kann für alle Replikationsverfahren verwendet werden.
- DD Extended Retention-Systeme können nicht als Quelle für die Verzeichnisreplikation verwendet werden.
- Die Sammelreplikation kann nicht von einem System mit einem Node (Single Node, SN) zu einem DD Extended Retention-System und nicht von einem DD Extended Retention-System zu einem System mit einem Node (Single Node, SN) konfiguriert werden.
- Die Sammelreplikation kann weder von einem SN-System auf ein DD-System mit aktivierter hoher Verfügbarkeit noch von einem DD-System mit aktivierter hoher Verfügbarkeit auf ein SN-System konfiguriert werden.
- Für die MTtree- und Verzeichnis-Replikation werden DD-HA-Systeme wie SN-Systeme behandelt.
- Die Sammelreplikation kann nicht konfiguriert werden, wenn für jedes oder beide Systeme Cloud-Tier aktiviert ist.

In dieser Tabelle gelten die folgenden Definitionen:

- SN = DD-System mit einem Node (ohne DD Extended Retention)
- ER = DD Extended Retention-System

Tabelle 182 Topologieunterstützung durch Replikationsverfahren und DD-Systemtyp

Topologien	MTree-Replikation	Verzeichnisreplikation	Sammelreplikation
One-to-One	{SN | ER} -> {SN | ER} ER->SN [unterstützt ab Version 5.5; vor Version 5.5 nur Recovery]	SN -> SN SN -> ER	SN -> SN ER -> ER
One-to-One, bidirektional	{SN | ER} -> {SN | ER}	SN -> SN	Nicht unterstützt
1:n	{SN | ER} -> {SN | ER}	SN -> SN SN -> ER	Nicht unterstützt

Tabelle 182 Topologieunterstützung durch Replikationsverfahren und DD-Systemtyp (Fortsetzung)

Topologien	MTree-Replikation	Verzeichnisreplikation	Sammelreplikation
n:1	{SN | ER} -> {SN | ER}	SN -> SN SN -> ER	Nicht unterstützt
Kaskadiert	{SN | ER } -> {SN | ER} -> {SN | ER}	SN -> SN -> SN SN -> SN -> ER	ER -> ER -> ER SN -> SN -> SN

Die kaskadierte Replikation unterstützt gemischte Topologien, wobei sich die zweite Komponente in einer kaskadierten Verbindung vom ersten Typ in einer Verbindung unterscheidet (Beispiel: A -> B ist eine Verzeichnisreplikation und B -> C ist eine Sammelreplikation).

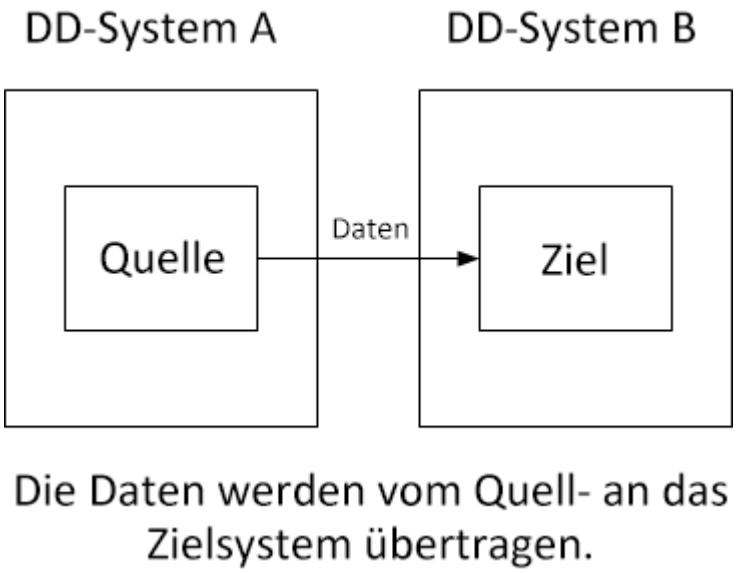
Tabelle 183 Unterstützte Topologien mit kaskadierter Replikation

Gemischte Topologien	
SN – Verz.-Repl. -> ER – MTree-Repl. -> ER – MTree-Repl.	SN – Verz.-Repl. -> ER – Sam.-Repl. -> ER – Sam.-Repl.
SN – MTree-Repl. -> SN – Sam.-Repl. -> SN – Sam.-Repl.	SN – MTree-Repl. -> ER – Sam.-Repl. -> ER – Sam.-Repl.

One-to-One-Replikation

Die einfachste Art der Replikation erfolgt von einem DD-Quellsystem auf ein DD-Zielsystem, auch bekannt als *One-to-One*-Replikationspaar. Diese Replikationstopologie kann mit Verzeichnis, MTree oder Sammelreplikationsarten konfiguriert werden.

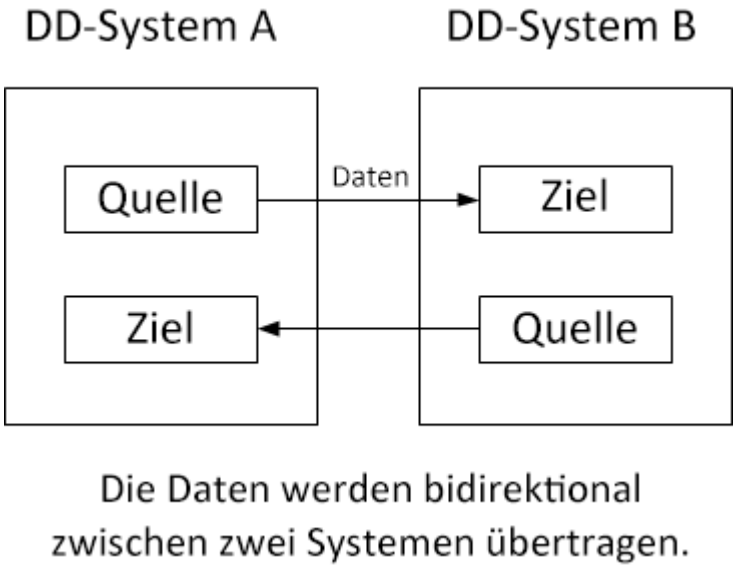
Abbildung 10 One-to-One-Replikationspaar



Bidirektionale Replikation

In einem bidirektionalen Replikationspaar werden die Daten aus einem Verzeichnis oder MTree auf DD-System A an System B und von einem anderen Verzeichnis oder MTree auf DD-System B an DD-System A repliziert.

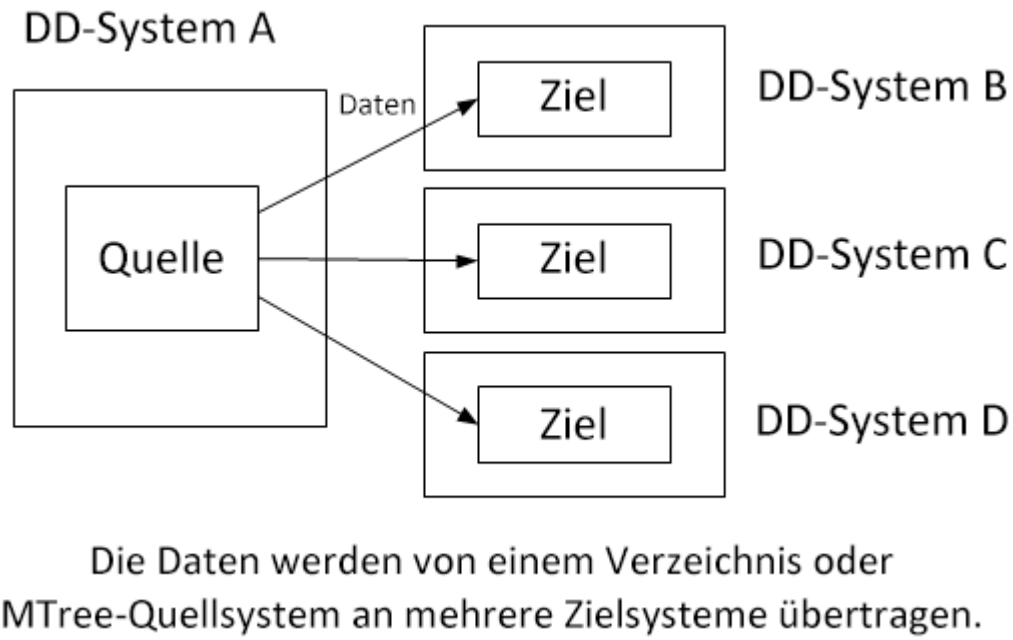
Abbildung 11 Bidirektionale Replikation



1:n-Replikation

Bei einer 1:n-Replikation fließen die Daten von einem Quellverzeichnis oder MTree auf einem DD-System an mehrere Zielsysteme. Mit diesem Replikationstyp könnten Sie mehr als zwei Kopien erstellen, um eine höhere Datensicherheit zu erzielen oder Daten für die Verwendung an mehreren Standorten zu verteilen.

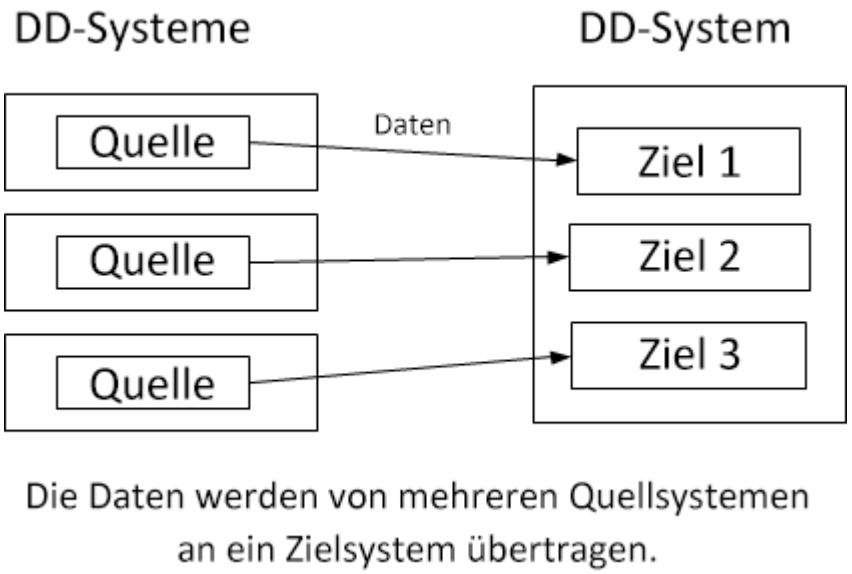
Abbildung 12 1:n-Replikation



Many-to-One-Replikation

Bei der n:1-Replikation (ob mit MTree oder einem Verzeichnis) werden Daten von den verschiedenen DD-Quellsystemen an ein einziges Zielsystem übertragen. Dieser Replikationstyp kann verwendet werden, um die Datenwiederherstellung für verschiedene Zweigstellen im IT-System des Hauptsitzes zu schützen.

Abbildung 13 Many-to-One-Replikation

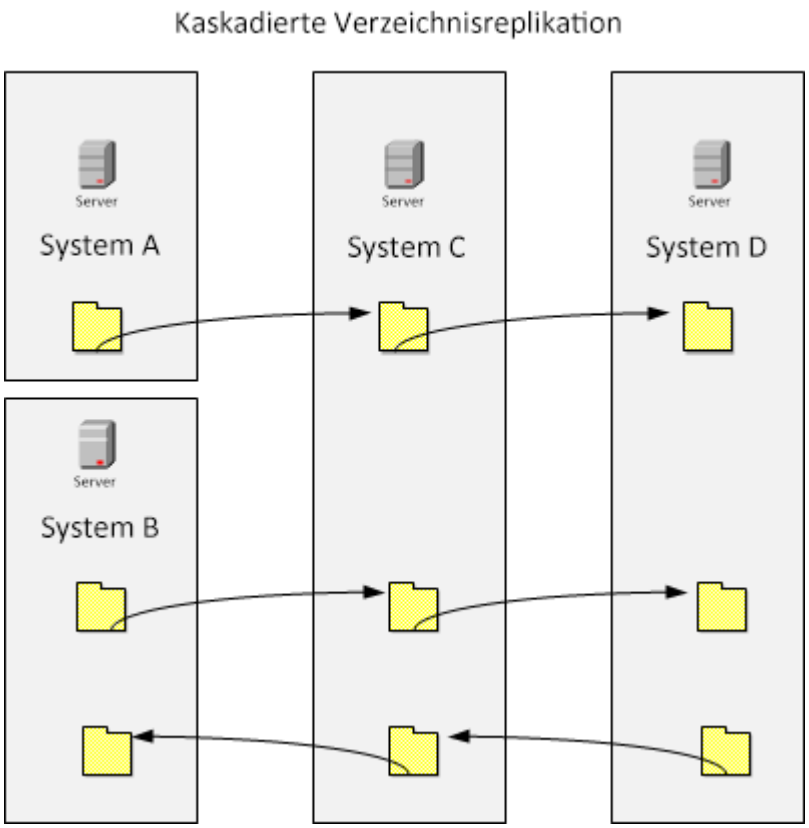


Kaskadierte Replikation

In einer kaskadierten Replikationstopologie wird ein Quellverzeichnis bzw. MTree mit drei DD-Systemen gekettet. Das letzte Glied in der Kette kann als Sammel-, MTree- oder Verzeichnisreplikation konfiguriert werden, je nachdem, ob die Quelle ein Verzeichnis oder MTree ist.

Beispielsweise repliziert DD-System A einen oder mehrere MTrees an DD-System B, das dann diese MTrees an DD-System C repliziert. Die MTrees auf DD-System B sind sowohl ein Ziel (für DD-System A) als auch eine Quelle (für DD-System C).

Abbildung 14 Kaskadierte Verzeichnisreplikation



Die Datenwiederherstellung kann von dem nicht heruntergestuften Replikationspaarkontext durchgeführt werden. Beispiel:

- Falls eine Recovery von DD-System A erforderlich ist, können Daten von DD-System B wiederhergestellt werden.
- Falls eine Recovery von DD-System B erforderlich ist, besteht die einfachste Methode darin, eine erneute Replikationssynchronisierung von DD-System A an DD-System B (Ersatz) durchzuführen. In diesem Fall sollte der Replikationskontext von DD-System B an DD-System C zuerst unterbrochen werden. Nachdem der Replikationskontext von DD-System A zu DD-System die erneute Synchronisierung abgeschlossen hat, sollte ein neuer Kontext von DD-System B zu DD-System C konfiguriert und erneut synchronisiert werden.

Managen der Replikation

Sie können die Replikation über die Data Domain System Manager (DD System Manager)- oder die Data Domain Operating System (DD OS)-Command Line Interface (CLI) managen.

Um eine Graphical User Interface (GUI) für das Managen der Replikation zu verwenden, melden Sie sich beim DD System Manager an.

Vorgehensweise

1. Klicken Sie im Menü links vom DD System Manager auf **Replication**. Wenn Ihre Lizenz noch nicht hinzugefügt wurde, wählen Sie **Add License**.
2. Wählen Sie **Automatic** oder **On-Demand**. (Sie müssen eine DD Boost-Lizenz für den Bedarfsfall haben.)

   CLI-Entsprechung

   Sie können sich auch bei der Befehlszeilenoberfläche anmelden:

   ```
   login as: Sysadmin
   Data Domain OS 6.0.x.x-12345
   Using keyboard-interactive authentication.
   Password:
   ```

Replikationsstatus

Unter „Replication Status“ wird die systemweite Anzahl der Replikationskontexte mit Warnstatus (gelber Text), Fehlerstatus (roter Text) oder normalem Status angezeigt.

Zusammenfassungsansicht

In der Ansicht „Summary“ werden die konfigurierten Replikationskontexte für ein DD-System mit aggregierten Informationen über das ausgewählte DD-System angezeigt – d. h. eine Zusammenfassung zu eingehenden und ausgehenden Replikationspaaren. Der Schwerpunkt ist das DD-System selbst und Eingaben und Ausgaben in das System und aus dem System.

Die Tabelle „Summary“ kann gefiltert werden, indem Sie einen Quell- oder Zielnamen eingeben oder einen Status auswählen (Fehler, Warnung oder Normal).

Tabelle 184 Ansicht „Replication Summary“

Element	Beschreibung
Quelle	System- und Pfadname des Quellkontexts im Format *system.path*. Für das Verzeichnis `dir1` auf `system dd120-22` wird beispielsweise `dd120-22.chaos.local/data/col1/dir1` angezeigt.
Ziel	System- und Pfadname des Zielkontexts im Format *system.path*. Für den MTree `MTree1` auf `system dd120-44` wird beispielsweise `dd120-44.chaos.local/data/col1/MTree1` angezeigt.
Typ	Kontexttyp: MTree, Verzeichnis (Dir) oder Pool
State	Folgende Status sind für Replikationspaare möglich:

Tabelle 184 Ansicht „Replication Summary“ (Fortsetzung)

Element	Beschreibung
	• Normal: Wenn das Replikat initialisiert, repliziert, wiederhergestellt, neu synchronisiert oder migriert wird • Idle: Bei der MTree-Replikation kann dieser Status anzeigen, ob der Replikationsprozess derzeit nicht aktiv ist oder Netzwerkfehler vorliegen (wenn beispielsweise nicht auf das Zielsystem zugegriffen werden kann) • Warning: Wenn eine ungewöhnliche Verzögerung für die ersten fünf Status oder für den Status „Uninitialized“ vorliegt • Error: Alle möglichen Fehlerstatus, z. B. „Disconnected“
Synced As Of Time	Zeitstempel für die neueste automatische Replikationssynchronisierung, die durch die Quelle durchgeführt wurde. Für die MTree-Replikation wird dieser Wert aktualisiert, wenn ein Snapshot auf dem Ziel verfügbar gemacht wird. Bei der Verzeichnisreplikation wird er aktualisiert, wenn ein Synchronisationspunkt, der von der Quelle eingesetzt wurde, angewendet wird. Ein Wert von „unbekannt“ wird während der Replikationsinitialisierung angezeigt.
Pre-Comp Remaining	Menge der vorkomprimierten Daten, die zum Replizieren übrig bleiben
Completion Time (Est.)	Der Wert ist entweder `Completed` oder die geschätzte Zeit, die zum Abschließen der Übertragung von Replikationsdaten erforderlich ist, basierend auf der Übertragungsrate in den letzten 24 Stunden.

Detaillierte Informationen für einen Replikationskontext

Wenn Sie in der Ansicht „Summary“ einen Replikationskontext auswählen, werden in den Bereichen „Detailed Information“, „Performance Graph“, „Completion Stats“ und „Completion Predictor“ die Informationen zu diesem Kontext angezeigt.

Tabelle 185 Detaillierte Informationen

Element	Beschreibung
Statusbeschreibung	Meldung zum Status des Replikats
Source	System- und Pfadname des Quellkontexts im Format `system.path`. Für das Verzeichnis `dir1` auf System `dd120-22` wird beispielsweise `dd120-22.chaos.local/data/col1/dir1` angezeigt.
Destination	System- und Pfadname des Zielkontexts im Format `system.path`. Für den MTree `MTree1` auf System `dd120-44` wird beispielsweise `dd120-44.chaos.local/data/col1/MTree1` angezeigt.
Connection Port	Systemname und Empfangsport, der für die Replikationsverbindung verwendet wird

Tabelle 186 Performance Graph

Element	Beschreibung
Pre-Comp Remaining	Vorkomprimierte Daten, die noch repliziert werden müssen
Pre-Comp Written	Vorkomprimierte Daten, die auf die Quelle geschrieben sind
Post-Comp Replicated	Nachkomprimierte Daten, die repliziert wurden

Tabelle 187 Abschlussstatistiken

Element	Beschreibung
Synced As Of Time	Zeitstempel für die neueste automatische Replikationssynchronisierung, die durch die Quelle durchgeführt wurde. Für die MTree-Replikation wird dieser Wert aktualisiert, wenn ein Snapshot auf dem Ziel verfügbar gemacht wird. Bei der Verzeichnisreplikation wird er aktualisiert, wenn ein Synchronisationspunkt, der von der Quelle eingesetzt wurde, angewendet wird. Ein Wert von „unbekannt“ wird während der Replikationsinitialisierung angezeigt.
Completion Time (Est.)	Der Wert ist entweder`Completed` oder die geschätzte Zeit, die zum Abschließen der Übertragung von Replikationsdaten erforderlich ist, basierend auf der Übertragungsrate in den letzten 24 Stunden.
Pre-Comp Remaining	Menge der noch zu replizierenden Daten
Files Remaining	(Nur Verzeichnisreplikation) Anzahl der Dateien, die noch nicht repliziert worden sind
Status	Für Quell- und Zielendpunkte wird der Status („Enabled", „Disabled", „Not Licensed“ usw.) der wichtigsten Komponenten im System angezeigt, z. B.: • Replikation • Dateisystem • Replikationssperre • Data-at-Rest-Verschlüsselung • Verschlüsselung über Kabel • Verfügbarer Speicherplatz • Optimierung bei geringer Bandbreite • Komprimierungsverhältnis • Optimierungsverhältnis bei geringer Bandbreite

Completion Predictor

„Completion Predictor“ ist ein Widget für die Verfolgung des Fortschritts eines Backupjobs und für Prognosen, wann die Replikation abgeschlossen sein wird, für einen ausgewählten Kontext.

Erstellen eines Replikationspaars

Vergewissern Sie sich vor dem Erstellen eines Replikationspaars, dass das Ziel nicht *vorhanden* ist, da sonst ein Fehler auftritt.

Vorgehensweise

1. Wählen Sie **Replication** > **Automatic** > **Registerkarte "Summary"** > **Create Pair**.
2. Fügen Sie im Dialogfeld "Create Pair" Informationen hinzu, um ein eingehendes oder ausgehendes MTree-, Verzeichnis-, Sammlungs- oder Poolreplikationspaar zu erstellen, wie in den folgenden Abschnitten beschrieben.

Hinzufügen eines DD-Systems für die Replikation

Möglicherweise müssen Sie ein DD-System als Host oder Ziel hinzufügen, bevor Sie ein Replikationspaar erstellen können.

Hinweis

Vergewissern Sie sich, dass das System, das hinzugefügt werden soll, eine kompatible DD OS-Version ausführt.

Vorgehensweise

1. Wählen Sie im Dialogfeld „Create Pair“ die Option „Add System“ aus.
2. Geben Sie für "System" den Hostnamen oder die IP-Adresse des Systems ein, das hinzugefügt werden soll.
3. Geben Sie für "User Name" und "Password" den Benutzernamen und das Passwort des Systemadministrators ein.
4. Klicken Sie optional auf **More Options**, um eine Proxy-IP-Adresse (oder den Systemnamen) eines Systems einzugeben, auf das nicht direkt zugegriffen werden kann. Wenn dies konfiguriert ist, geben Sie einen benutzerdefinierten Port anstelle des Standardports 3009 ein.

   Hinweis

   IPv6-Adressen werden nur unterstützt, wenn ein DD OS 5.5- oder höheres System zu einem Managementsystem mit DD OS 5.5 oder höher hinzugefügt wird.

5. Wählen Sie **OK** aus.

   Hinweis

   Wenn das System nach dem Hinzufügen zu DD System Manager nicht erreichbar ist, sorgen Sie dafür, dass eine Route vom Managementsystem zum System hinzugefügt wird. Wenn ein Hostname (entweder ein vollständig qualifizierter Domainname (FQDN) oder nicht vollständig qualifizierter Domainname) eingegeben wird, sollten Sie sicherstellen, dass er auf dem gemanagten System aufgelöst werden kann. Konfigurieren Sie einen Domainnamen für das gemanagte System und stellen Sie sicher, dass ein DNS-Eintrag für das System vorhanden ist, oder sorgen Sie dafür, dass die Zuordnung einer IP-Adresse zu einem Hostnamen definiert ist.

6. Wenn das Systemzertifikat nicht überprüft wurde, werden im Dialogfeld „Verify Certificate“ Details zum Zertifikat angezeigt. Prüfen Sie die Systemanmeldedaten. Klicken Sie auf **OK**, wenn Sie dem Zertifikat vertrauen, oder klicken Sie auf **Cancel**.

Erstellen eines Sammelreplikationspaars

Allgemeine Informationen über diese Art der Replikation finden Sie im Abschnitt *Sammelreplikation*.

Bevor Sie ein Sammelreplikationspaar erstellen, stellen Sie Folgendes sicher:

- Die Speicherkapazität des Zielsystems ist größer oder gleich der Kapazität des Quellsystems. (Wenn die Zielkapazität kleiner als die der Quelle ist, wird die verfügbare Kapazität auf der Quelle auf die des Ziels reduziert.)
- Das Ziel wurde gelöscht und anschließend erneut erstellt, aber nicht aktiviert.
- Jedes Ziel und jede Quelle befindet sich nur in jeweils einem Kontext gleichzeitig.
- Beim Konfigurieren und Aktivieren der Verschlüsselung auf der Quelle ist das Dateisystem auf dem Replikat deaktiviert.
- Beim Konfigurieren und Aktivieren der Verschlüsselung auf dem Replikat ist das Dateisystem auf der Quelle deaktiviert.

Vorgehensweise

1. Wählen Sie im Dialogfeld „Create Pair“ **Collection** aus dem Menü **Replication Type** aus.
2. Wählen Sie im Menü **Source System** den Hostnamen des Quellsystems aus.
3. Wählen Sie im Menü **Destination System** den Hostnamen des Zielsystems aus. Die Liste enthält nur Hosts in der DD-Netzwerkliste.
4. Wenn Sie Hostverbindungseinstellungen ändern möchten, wählen Sie die Registerkarte **Advanced** aus.
5. Wählen Sie **OK** aus. Die Replikation von der Quelle zum Ziel wird gestartet.

Ergebnisse

Testergebnisse von Data Domain gaben die folgenden Performancerichtlinien für die Replikationsinitialisierung zurück. Hierbei handelt es sich *nur* um Richtlinien und die tatsächliche Performance, die in der Produktionsumgebung beobachtet wird, kann variieren.

- Über ein Gibibit-LAN: Mit einer ausreichenden Anzahl Einschübe, um maximalen Input/Output und Idealbedingungen zu erreichen, kann die Sammelreplikation eine 1-GigE-Verbindung (Modulo 10 % Protokoll-Overhead) sowie 400–900 MB/s auf 10gigE bedienen, abhängig von der Plattform.
- Über ein WAN richtet sich die Performance nach der Leitungsgeschwindigkeit, Bandbreite, Latenz und Paketverlustrate der WAN-Verbindung.

Erstellen eines MTree-, Verzeichnis- oder Poolreplikationspaars

Allgemeine Informationen über diese Arten der Replikation finden Sie in den Abschnitten *MTree-Replikation* und *Verzeichnisreplikation*.

Beachten Sie beim Erstellen eines MTree-, Verzeichnis- oder Poolreplikationspaars Folgendes:

- Stellen Sie sicher, dass die Replikation über die richtige Schnittstelle übertragen wird bzw. die richtige Schnittstelle verlässt. Beim Definieren eines Replikationskontexts müssen die Hostnamen der Quelle und des Ziels mit Forward-

und Reverse-Lookups aufgelöst werden. Damit Daten über andere Schnittstellen im System als über die standardmäßig festgelegte auflösende Schnittstelle übertragen werden, muss der Replikationskontext nach der Erstellung geändert werden. Möglicherweise müssen Hostdateien eingerichtet werden, um sicherzustellen, dass Kontexte in nicht auflösenden (Crossover) Schnittstellen definiert werden.

- Sie können den Kontext für eine MTree-Replikation „umkehren“, z. B. können Sie das Ziel und die Quelle wechseln.
- Unterverzeichnisse in einem MTree können nicht repliziert werden, da der MTree in vollem Umfang repliziert wird.
- Die MTree-Replikation von DD Extended Retention-Systemen auf Nicht-DD Extended Retention-Systeme wird unterstützt, wenn auf beiden Systemen DD OS 5.5 oder höher ausgeführt wird.
- Auf dem DD-Zielsystem muss mindestens so viel Speicherkapazität verfügbar sein, dass sie der nachkomprimierten Größe der erwarteten maximalen nachkomprimierten Größe des Quellverzeichnisses oder MTrees entspricht.
- Beim Start der Replikation wird ein Zielverzeichnis automatisch erstellt.
- Ein DD-System kann gleichzeitig die Quelle eines Kontextes und das Ziel für einen anderen Kontext sein.

Vorgehensweise

1. Wählen Sie im Dialogfeld „Create Pair“ **Directory**, **MTree** (Standard) oder **Pool** aus dem Menü **Replication Type** aus.
2. Wählen Sie im Menü **Source System** den Hostnamen des Quellsystems aus.
3. Wählen Sie im Menü **Destination System** den Hostnamen des Zielsystems.
4. Geben Sie den Quellpfad in das Textfeld **Source Path** ein (beachten Sie, dass der erste Teil des Pfads eine Konstante ist, die sich basierend auf dem ausgewählten Replikationstyp ändert).
5. Geben Sie den Zielpfad in das Textfeld **Destination Directory** ein (beachten Sie, dass der erste Teil des Pfads eine Konstante ist, die sich basierend auf dem ausgewählten Replikationstyp ändert).
6. Wenn Sie die Hostverbindungseinstellungen ändern möchten, wählen Sie die Registerkarte **Advanced** aus.
7. Wählen Sie **OK** aus.

   Die Replikation von der Quelle zum Ziel wird gestartet.

   Testergebnisse aus Data Domain führten zu den folgenden Richtlinien für die Schätzung der Zeit, die für die Replikationsinitialisierung erforderlich ist.

   Hierbei handelt es sich *nur* um Richtlinien, die möglicherweise in der speziellen Produktionsumgebung nicht zutreffen.

   - Bei einer T3-Verbindung mit 100 ms WAN beträgt die Performance für vorkomprimierte Daten ca. 40 MiB/s, was folgende Datenübertragung ergibt:
     1 MiB/s = 25 Sekunden/GiB = 3,456 TiB/Tag
   - Bei der 2er-Potenz-Entsprechung von Gigabit-LAN beträgt die Performance ca. 80 MiB/s für vorkomprimierte Daten, was eine Datenübertragung mit ca. der doppelten Rate für ein T3-WAN ergibt.

   CLI-Entsprechung
   Im Folgenden finden Sie einige Beispiele zum Erstellen von MTree- oder Verzeichnisreplikationspaaren über die Befehlszeilenoberfläche. Im letzten

Beispiel ist die IP-Version angegeben, die als Replikationstransport verwendet wird.

```
# replication add source mtree://ddsource.test.com/data/col1/
examplemtree destination mtree://ddtarget.test.com/data/col1/
examplemtree (Mtree example) # replication add source dir://
ddsource.test.com/data/col1/directorytorep destination dir://
ddtarget.test.com/backup/directorytorep # replication add
source dir://ddsource.test.com/data/col1/directorytorep
destination dir://ddtarget.test.com/backup/directorytorep
ipversion ipv6
```

Um die Replikation zwischen einer Quelle und einem Ziel zu starten, verwenden Sie den Befehl `replication initialize` auf der Quelle. Anhand dieses Befehls wird überprüft, ob die Konfiguration und die Verbindungen korrekt sind. Bei Problemen werden Fehlermeldungen zurückgegeben.

```
# replication initialize mtree://host3.test.com/data/col1/
mtree1/
```

Konfigurieren der bidirektionalen Replikation
Um ein bidirektionales Replikationspaar von Host A zu Host B zu erstellen, verwenden Sie das Verfahren zum Erstellen von Verzeichnis- oder MTree-Replikationspaaren (z. B. mit mtree2). Verwenden Sie das gleiche Verfahren, um ein Replikationspaar (z. B. mit mtree1) von Host B zu Host A zu erstellen. Für diese Konfiguration können Zielpfadnamen nicht identisch sein.

Konfigurieren der 1:n-Replikation
Um ein 1:n-Replikationspaar zu erstellen, verwenden Sie das Verfahren für Verzeichnisse oder MTree-Replikationspaare (z. B. unter Verwendung von „mtree1“) auf Host A zu: (1) mtree1 auf Host B, (2) mtree1 auf Host C und (3) mtree1 auf Host D. Es kann keine Replikations-Recovery für einen Quellkontext durchgeführt werden, dessen Pfad der Quellpfad für andere Kontexte ist. Die anderen Kontexte müssen angehalten und nach der Recovery neu synchronisiert werden.

Konfigurieren der n:1-Replikation
Um ein n:1-Replikationspaar zu erstellen, verwenden Sie das Verfahren für Verzeichnisse oder MTree-Replikationspaare [z. B. (1) mtree1 von Host A zu mtree1 auf Host C und (2) mtree2 von Host B zu mtree2 auf Host C].

Konfigurieren der kaskadierten Replikation
Verwenden Sie zum Erstellen eines kaskadierten Replikationspaars das Verfahren für Verzeichnis- oder MTree-Replikationspaare: (1) mtree1 auf Host A an mtree1 auf Host B und (2) erstellen Sie auf Host B ein Paar für mtree1 an mtree1 auf Host C. Der Kontext des endgültigen Ziels (auf Host C in diesem Beispiel, aber es werden mehr als drei Hops unterstützt) kann ein Sammelreplikat oder ein Verzeichnis- oder MTree-Replikat sein.

Deaktivieren und Aktivieren eines Replikationspaars

Durch Deaktivierung eines Replikationspaars wird die aktive Replikation von Daten zwischen einer Quelle und einem Ziel vorübergehend angehalten. Die Quelle sendet keine weiteren Daten an das Ziel und das Ziel unterbricht die aktive Verbindung zur Quelle.

Vorgehensweise

1. Wählen Sie in der Tabelle „Summary“ eines oder mehrere Replikationspaare und anschließend die Option **Disable Pair** aus.
2. Wählen Sie im Dialogfeld „Display Pair“ erst **Next** und anschließend **OK** aus.
3. Um den Vorgang eines deaktivierten Replikationspaars wieder aufzunehmen, wählen Sie in der Tabelle „Summary“ eines oder mehrere Replikationspaare und

anschließend die Option **Enable Pair** auf, um das Dialogfeld „Enable Pair“ anzuzeigen.

4. Wählen Sie **Next** und anschließend **OK** aus. Die Datenreplikation wird fortgesetzt.

CLI-Entsprechung

```
# replication disable {destination | all}

# replication enable {destination | all}
```

Löschen eines Replikationspaars

Wenn ein Verzeichnis oder ein MTree-Replikationspaar gelöscht wird, wird das Zielverzeichnis bzw. der MTree beschreibbar. Wenn ein Sammelreplikationspaar gelöscht wird, wird aus dem DD-Zielsystem ein eigenständiges Lese-/Schreibsystem und das Dateisystem wird deaktiviert.

Vorgehensweise

1. Wählen Sie ein oder mehrere Replikationspaare in der Übersichtstabelle aus und wählen Sie **Delete Pair**.
2. Wählen Sie im Dialogfeld „Delete Pair“ **Next** und dann **OK**. Die Replikationspaare werden gelöscht.

CLI-Entsprechung

Führen Sie vor dem Ausführen dieses Befehls immer erst den Befehl `filesys disable` aus. Führen Sie anschließend den Befehl `filesys enable` aus.

```
# replication break {destination | all}
```

Ändern von Hostverbindungseinstellungen

Damit Datenverkehr über einen bestimmten Port nach außen weitergeleitet wird, ändern Sie den aktuellen Kontext, indem Sie den Parameter für den Verbindungshost mit einem zuvor in der lokalen Hostdatei definierten Hostnamen so ändern, dass das andere System adressiert wird. Dieser Hostname entspricht dem Zielsystem. Der Hosteintrag gibt für diesen Host eine andere Zieladresse an. Dieser Vorgang muss möglicherweise sowohl auf dem Quell- als auch auf dem Zielsystem durchgeführt werden.

Vorgehensweise

1. Wählen Sie das Replikationspaar in der Tabelle „Summary“ und dann **Modify Settings** aus. Sie können diese Einstellungen auch ändern, wenn Sie „Create Pair“, „Start Resync“ oder „Start Recover“ durchführen, indem Sie die Registerkarte **Advanced** auswählen.
2. Im Dialogfeld „Modify Connection Settings“ können Sie die folgenden Einstellungen ändern:
   a. **Use Low Bandwidth Optimization**: Für Unternehmen mit kleinen Datasets und einer Netzwerkbandbreite von weniger als 6 Mbit/s kann DD Replicator durch Auswahl eines *Optimierungsmodus für geringe Bandbreiten* die zu übertragende Datenmenge zusätzlich verringern. Dadurch können Remotestandorte mit begrenzter Bandbreite weniger Bandbreite verwenden oder mehr Daten über bestehende Netzwerke replizieren und sichern. Die Optimierung bei geringer Bandbreite muss auf dem DD-Quellsystem und auf dem DD-Zielsystem aktiviert werden. Wenn Quelle und Ziel inkompatible Einstellungen hinsichtlich der Optimierung bei niedriger Bandbreite

aufweisen, ist die Optimierung bei niedriger Bandbreite für diesen Kontext inaktiv. Nachdem Sie den Optimierungsmodus für geringe Bandbreiten auf der Quelle und dem Ziel aktiviert haben, müssen beide Systeme einen vollständigen Bereinigungszyklus durchlaufen, um die vorhandenen Daten vorzubereiten. Führen Sie dafür auf beiden Systemen `filesys clean start` aus. Die Dauer des Bereinigungszyklus hängt von der Menge der Daten auf dem DD-System ab, er nimmt aber mehr Zeit in Anspruch als eine normale Bereinigung. Weitere Informationen zu den `filesys`-Befehlen finden Sie im *Data Domain Operating System Command Reference Guide*.

Wichtig: Der Optimierungsmodus für geringe Bandbreiten wird nicht unterstützt, wenn die DD Extended Retention-Softwareoption auf einem DD-System aktiviert ist. Sie wird ebenfalls nicht für die Sammelreplikation unterstützt.

b. **Enable Encryption Over Wire**: DD Replicator unterstützt die Data-in-Flight-Verschlüsselung über die SSL-Standardprotokollversion 1.0.1 (Secure Socket Layer), die die ADH-AES256-GCM-SHA384- und die DHE-RSA-AES256-GCM-SHA384-Cipher-Suite verwendet, um sichere Replikationsverbindungen einzurichten. Diese Funktion muss auf beiden Seiten der Verbindung aktiviert sein, um die Verschlüsselung fortsetzen zu können.

c. **Network Preference**: Sie können IPv4 oder IPv6 auswählen. Ein IPv6-fähiger Replikationsservice kann immer noch Verbindungen von einem IPv4-Replikationsclient akzeptieren, wenn der Service über IPv4 erreichbar ist. Ein IPv6-fähiger Replikationsservice kann immer noch mit einem IPv4-Replikationsservice kommunizieren, wenn der Service über IPv4 erreichbar ist.

d. **Use Non-default Connection Host**: Das Quellsystem überträgt Daten an einen Überwachungsport auf dem Zielsystem. Da auf einem Quellsystem die Replikation für viele Zielsysteme konfiguriert sein kann (von denen jedes über einen anderen Überwachungsport verfügen kann), kann jeder Kontext auf der Quelle den Verbindungsport für den entsprechenden Überwachungsport des Ziels konfigurieren.

3. Wählen Sie **Next** und dann **Close** aus.

   Die Einstellungen für das Replikationspaar werden aktualisiert und die Replikation wird wieder aufgenommen.

CLI-Entsprechung

```
#replication modify <destination> connection-host <new-host-name> [port <port>]
```

Managen von Replikationssystemen

Sie können Data Domain-Systeme, die für die Replikation verwendet werden, über das Dialogfeld "Manage Systems" hinzufügen oder Löschen.

Vorgehensweise

1. Wählen Sie **Modify Settings**.
2. Fügen Sie im Dialogfeld "Manage Systems" Data Domain-Systeme nach Bedarf hinzu und/oder löschen Sie sie.
3. Klicken Sie auf **Close**.

Wiederherstellen von Daten aus einem Replikationspaar

Wenn auf Quellreplikationsdaten nicht mehr zugegriffen werden kann, können diese aus dem Replikationspaarziel *wiederhergestellt* werden. Die Quelle muss leer sein, bevor die Recovery durchgeführt werden kann. Die Recovery kann außer für die die MTree-Replikation für alle Replikationstopologien durchgeführt werden.

Die Recovery von Daten aus einem Verzeichnispool sowie aus Verzeichnis- und Sammelreplikationspaaren wird in den nächsten Abschnitten beschrieben.

Wiederherstellen von Verzeichnispooldaten

Daten können aus einem verzeichnisbasierten Pool, nicht jedoch aus einem MTree-basierten Pool wiederhergestellt werden.

Vorgehensweise

1. Wählen Sie **More** > **Start Recover**.
2. Wählen Sie im Dialogfeld „Start Recovery“ **Pool** aus dem Menü **Replication Type** aus.
3. Wählen Sie im Menü **System to recover to** den Hostnamen des Quellsystems aus.
4. Wählen Sie im Menü **System to recover from** den Hostnamen des Zielsystems aus.
5. Wählen Sie den Kontext auf dem Ziel aus, aus dem Daten wiederhergestellt werden.
6. Wenn Sie Hostverbindungseinstellungen ändern möchten, wählen Sie die Registerkarte **Advanced** aus.
7. Klicken Sie auf **OK**, um die Recovery zu starten.

Wiederherstellen von Daten eines Sammelreplikationspaars

Damit die Daten eines Sammelreplikationspaars wiederhergestellt werden können, muss sich das Quelldateisystem in einem makellosen Zustand befinden und der Zielkontext muss komplett initialisiert sein.

Vorgehensweise

1. Wählen Sie **More** > **Start Recover**, um das Dialogfeld „Start Recover“ anzuzeigen.
2. Wählen Sie aus dem Menü **Replication Type** die Option **Collection** aus.
3. Wählen Sie aus dem Menü **System to recover to** den Hostnamen des Quellsystems aus.
4. Wählen Sie aus dem Menü **System to recover from** den Hostnamen des Zielsystems aus.
5. Wählen Sie den Kontext auf dem Ziel aus, aus dem Daten wiederhergestellt werden sollen. Auf dem Ziel ist nur eine Sammlung vorhanden.
6. Wenn Sie die Host-Verbindungseinstellungen ändern möchten, wählen Sie die Registerkarte **Advanced** aus.
7. Klicken Sie auf **OK**, um die Recovery zu starten.

Wiederherstellen von Daten eines Verzeichnisreplikationspaars

Damit Daten eines Verzeichnisreplikationspaars erfolgreich wiederhergestellt werden können, muss das Verzeichnis erstellt werden (aber leer bleiben), das im ursprünglichen Kontext verwendet wurde.

Vorgehensweise

1. Wählen Sie **More** > **Start Recover**, um das Dialogfeld „Start Recover“ anzuzeigen.
2. Wählen Sie aus dem Menü **Replication Type** die Option **Directory** aus.
3. Wählen Sie im Menü **System to recover to** den Hostnamen des *Systems, für welches Daten wiederhergestellt werden sollen*.
4. Wählen Sie im Menü **System to recover from** den Hostnamen des *Systems, das als Datenquelle fungiert*.
5. Wählen Sie den wiederherzustellenden Kontext aus der Kontextliste aus.
6. Wenn Sie die Host-Verbindungseinstellungen ändern möchten, wählen Sie die Registerkarte **Advanced** aus.
7. Klicken Sie auf **OK**, um die Recovery zu starten.

Abbrechen der Recovery eines Replikationspaars

Wenn eine Recovery fehlschlägt oder beendet werden muss, können Sie die Replikations-Recovery wie folgt beenden.

Vorgehensweise

1. Wählen Sie das Menü „More“ und dann **Abort Recover** aus, um das Dialogfeld „Abort Recover“ anzuzeigen, in dem der Kontext einer kürzlich durchgeführten Recovery angezeigt wird.
2. Aktivieren Sie das Kontrollkästchen für mindestens einen abzubrechenden Kontext aus der Liste.
3. Wählen Sie **OK** aus.

Weitere Erfordernisse

Die Recovery muss auf der Quelle so schnell wie möglich neu gestartet werden.

Neusynchronisieren eines MTree-, Verzeichnis- oder Poolreplikationspaars

Die *Neusynchronisierung* ist der Prozess der Recovery oder Neusynchronisierung der Daten zwischen einem Quell- und Zielreplikationspaar nach einer manuellen Unterbrechung. Das Replikationspaar wird neu synchronisiert, sodass beide Endpunkte die gleichen Daten enthalten. Die Neusynchronisierung ist für die MTree-, Verzeichnis- oder Poolreplikation, aber nicht für die Sammelreplikation verfügbar.

Eine Neusynchronisierung einer Replikation kann auch in den folgenden Fällen verwendet werden:

- Zum Erstellen eines Kontexts, der gelöscht wurde
- Wenn kein Speicherplatz mehr auf einem Ziel vorhanden ist, die Quelle jedoch noch zu replizierende Daten enthält
- Zum Konvertieren eines Verzeichnisreplikationspaars in ein MTree-Replikationspaar

Vorgehensweise

1. Entfernen Sie den Kontext von den Replikationsquell- und den Replikationszielsystemen.
2. Wählen Sie auf dem Replikationsquell- oder dem Replikationszielsystem **More** > **Start Resync**, um das Dialogfeld „Start Resync“ anzuzeigen.
3. Wählen Sie den Replikationstyp aus, der neu synchronisiert werden soll: **Directory**, **MTree** oder **Pool**.
4. Wählen Sie im Menü **Source System** den Hostnamen des Replikationsquellsystems aus.
5. Wählen Sie im Menü **Destination System** den Hostnamen des Replikationszielsystems aus.
6. Geben Sie den Pfad für die Replikationsquelle in das Textfeld **Source Path** ein.
7. Geben Sie den Pfad für das Replikationsziel in das Textfeld **Destination Path** ein.
8. Wenn Sie die Host-Verbindungseinstellungen ändern möchten, wählen Sie die Registerkarte **Advanced** aus.
9. Wählen Sie **OK** aus.

CLI-Entsprechung

```
# replication resync destination
```

Abbrechen der Neusynchronisierung eines Replikationspaars

Wenn die Neusynchronisierung eines Replikationspaars fehlschlägt oder beendet werden muss, können Sie die Neusynchronisierung wie folgt beenden.

Vorgehensweise

1. Wählen Sie auf dem Quell- oder Zielsystem der Replikation **More** > **Abort Resync**, um das Dialogfeld „Abort Resync“ anzuzeigen, in dem alle Kontexte angezeigt werden, in denen derzeit eine Neusynchronisierung durchgeführt wird.
2. Aktivieren Sie das Kontrollkästchen für mindestens einen abzubrechenden Kontext, um die Neusynchronisierung abzubrechen.
3. Wählen Sie **OK** aus.

Ansicht „DD Boost“

Die Ansicht „DD Boost“ enthält Konfigurations- und Troubleshooting-Informationen für NetBackup-Administratoren, die ihre DD-Systeme für die Verwendung von DD Boost AIR (Automatic Image Replication) oder einer beliebigen DD Boost-Anwendung konfiguriert haben, die Managed File Replication verwendet.

Konfigurationsanweisungen für DD Boost AIR finden Sie im *Data Domain Boost for OpenStorage Administration Guide*.

Die Registerkarte **File Replication** wird angezeigt:

- Currently Active File Replication:
  - Die Richtung (ausgehend und ankommend) und die Anzahl der Dateien in jeder Replikation.
  - Die verbleibenden zu replizierenden Daten (vorkomprimierter Wert in GiB) und die bereits replizierte Datenmenge (vorkomprimierter Wert in GiB).

    - Total size: Die Menge der zu replizierenden Daten und die bereits replizierten Daten (vorkomprimierter Wert in GiB).
- Most Recent Status: Gesamtzahl der Dateireplikationen und deren Status (abgeschlossen oder fehlgeschlagen)
    - während der letzten Stunde
    - in den letzten 24 Stunden
- Remote Systems:
    - Wählen Sie eine Replikation in der Liste aus.
    - Wählen Sie den Zeitraum aus, der vom Menü abgedeckt werden soll.
    - Wählen Sie **Show Details** aus, um weitere Informationen zu diesen Remotesystemdateien anzuzeigen.

Die Registerkarte **Storage Unit Associations** zeigt die folgenden Informationen an, die Sie zu Auditzwecken verwenden können oder um den Status von DD Boost AIR-Ereignissen für die Imagereplikationen der Speichereinheit zu prüfen:

- Eine Liste aller **Speichereinheitzuordnungen**, die dem System bekannt sind. Die Quelle befindet sich links und das Ziel rechts. Diese Informationen zeigen die Konfiguration von AIR auf dem Data Domain-System an.
- Die **Event Queue** ist die Liste der ausstehenden Ereignisse. Es werden die lokale Speichereinheit, die Ereignis-ID und der Status des Ereignisses angezeigt.

Es wird versucht, beide Enden eines DD Boost-Pfads zuzuordnen, um ein Paar zu bilden. Das Ergebnis wird als ein Paar/Datensatz dargestellt. Wenn die Übereinstimmung aus verschiedenen Gründen nicht möglich ist, wird der Remotepfad als *Unresolved* aufgeführt.

Remotesystemdateien

Die Schaltfläche „Show Details“ stellt Informationen für das ausgewählte Remotedateireplikationssystem bereit. „File Replications“ zeigt die Start- und Enddaten sowie die Größe und die Datenmenge für das ausgewählte Remotedateireplikationssystem an. Der „Performance Graph“ zeigt die Leistung im Laufe der Zeit für das ausgewählte Remotedateireplikationssystem an.

Tabelle 188 Dateireplikationen

Element	Beschreibung
Start	Startpunkt des Zeitraums
End	Endpunkt des Zeitraums
File Name	Name der jeweiligen Replikationsdatei
Status	Aktueller Status (erfolgreich, fehlgeschlagen)
Pre-Comp Size (MiB)	Zahl der vorkomprimierten eingehenden und ausgehenden Daten im Vergleich zum Netzwerkdurchsatz oder den nachkomprimierten Daten (in MiB)
Network Bytes (MiB)	Menge der Netzwerkdurchsatzdaten (in MiB)

Tabelle 189 Performance Graph

Element	Beschreibung
Duration	Dauer der Replikation (entweder 1d, 7d oder 30d)
Interval	Intervall für die Replikation (täglich oder wöchentlich)
Pre-Comp Replicated	Menge der vorkomprimierten eingehenden und ausgehenden Daten (in GiB)
Post-Comp Replicated	Menge der nachkomprimierten Daten (in GiB)
Network Bytes	Menge der Netzwerkdurchsatzdaten (in GiB)
Files Succeeded	Anzahl der Dateien, die erfolgreich repliziert wurden
Files Failed	Anzahl der Dateien, deren Replikation fehlgeschlagen ist
Show in new window	Öffnet ein separates Fenster.
Print	Druckt die Grafik.

Topologieansicht

Die Ansicht „Topology“ zeigt, wie die ausgewählten Replikationspaare im Netzwerk konfiguriert sind.

- Der Pfeil zwischen DD-Systemen stellt ein oder mehrere Replikationspaare dar und wird grün (normal), gelb (Warnung) oder rot (Fehler) angezeigt.
- Wählen Sie zum Anzeigen von Details einen Kontext aus, um das Dialogfeld „Context Summary“ mit Links zu **Show Summary**, **Modify Options**, **Enable/ Disable Pair**, **Graph Performance** und **Delete Pair** zu öffnen.
- Wählen Sie **Collapse All**, um eine Übersicht der Kontextansicht „Expand All“ und damit nur den Namen des Systems und die Anzahl der Zielkontexte anzuzeigen.
- Wählen Sie **Expand All** aus, um alle Zielverzeichnis- und MTree-Kontexte anzuzeigen, die auf anderen Systemen konfiguriert sind.
- Wählen Sie **Reset Layout**, um zur Standardansicht zurückzukehren.
- Wählen Sie **Print** aus, um ein Standarddialogfeld zum Drucken zu öffnen.

Ansicht „Performance“

In der Ansicht „Performance“ wird ein Diagramm angezeigt, das die Schwankung von Daten bei der Replikation darstellt. Dies sind aggregierte Statistiken für jedes Replikationspaar für dieses DD-System.

- Die **Dauer** (X-Achse) ist standardmäßig auf 30 Tage eingestellt.
- Die **Replikationsperformance** (Y-Achse) ist in GibiByte oder MebiByte (binäre Entsprechungen von Gigabyte und Megabyte) angegeben.
- **Network In** gibt die Gesamtnetzwerkbyte der Replikation an, die im System eingehen (alle Kontexte).
- **Network Out** gibt die Gesamtnetzwerkbyte der Replikation an, die aus dem System ausgehen (alle Kontexte).
- Um den Messwert zu einem bestimmten Zeitpunkt anzuzeigen, bewegen Sie den Mauszeiger über eine Stelle im Diagramm.

- In Zeiten der Inaktivität (wenn keine Daten übertragen werden) zeigt die Form des Diagramms möglicherweise eine graduell absteigende Linie statt der erwarteten stark absteigenden Linie an.

Ansicht „Advanced Settings“

In der Ansicht „Advanced Settings“ können Sie Drosselungs- und Netzwerkeinstellungen verwalten.

Drosselungseinstellungen

- **Throttle Override** – Dieser Wert zeigt die Drosselungsrate oder 0 an, d. h. der gesamte Replikationsverkehr wird angehalten.
- **Permanent Schedule**: Dieser Wert zeigt die Zeit und die Wochentage an, an denen geplante Drosselungen stattfinden.

Netzwerkeinstellungen

- **Bandwidth**: Dieser Wert zeigt die konfigurierte Datenstreamrate an, sofern die Bandbreite konfiguriert wurde. Andernfalls wird „Unlimited“ (Standard) angezeigt. Der durchschnittliche Datenstream zum Replikationsziel ist mindestens 98.304 Bit pro Sekunde (12 KiB).
- **Delay**: Dieser Wert zeigt die konfigurierte Einstellung für die Netzwerkverzögerung in Millisekunden an, sofern eine Netzwerkverzögerung konfiguriert wurde. Andernfalls wird „None“ (Standard) angezeigt.
- **Listen Port**: Dieser Wert zeigt den konfigurierten Wert für den Listen-Port an, sofern dieser Wert konfiguriert wurde. Andernfalls wird „2051“ (Standard) angezeigt.

Hinzufügen von Drosselungseinstellungen

Um die Bandbreite zu ändern, die von einem Netzwerk für die Replikation verwendet wird, können Sie eine *Replikationsdrosselung* für Replikationsdatenverkehr festlegen.

Es gibt drei Arten von Replikationsdrosselungseinstellungen:

- **Scheduled throttle**: Die Drosselungsrate wird auf einen vorbestimmten Zeitpunkt oder Zeitraum festgelegt.
- **Current throttle**: Die Drosselungsrate wird bis zur nächsten geplanten Änderung oder bis zu einem Systemneustart festgelegt.
- **Override throttle**: Die beiden vorherigen Typen der Drosselung werden außer Kraft gesetzt. Dies bleibt auch bei einem Neustart bestehen, bis Sie **Clear Throttle Override** oder den Befehl `replication throttle reset override` ausführen.

Sie können auch eine Standarddrosselung oder eine Drosselung für bestimmte Ziele festlegen. Gehen Sie dafür wie folgt vor:

- **Default throttle**: Wenn sie konfiguriert ist, werden alle Replikationskontexte auf diese Drosselung begrenzt, außer für Ziele, die nach Zieldrosselungen angegeben sind (siehe nächster Punkt).
- **Destination throttle**: Diese Drosselung wird verwendet, wenn nur einige Ziele gedrosselt werden müssen oder wenn ein Ziel eine andere Drosselungseinstellung als die Standarddrosselung benötigt. Wenn eine Standarddrosselung bereits vorhanden ist, hat diese Drosselung Vorrang für das angegebene Ziel. Sie können beispielsweise die Standardreplikationsdrosselung auf *10 KB/s* festlegen, mit einer

Zieldrosselung jedoch einen einzelnen Sammelreplikationskontext auf *Unlimited* festlegen.

Hinweis

Derzeit können Sie Zieldrosselungen nur über die Befehlszeilenoberfläche (CLI) festlegen und ändern. Diese Funktion ist nicht im DD System Manager verfügbar. Dokumentation zu dieser Funktion finden Sie unter dem Befehl `replication throttle` im *Data Domain Operating System Command Reference Guide*. Wenn DD System Manager erkennt, dass Sie eine oder mehrere Zieldrosselungen festgelegt haben, wird Ihnen eine Warnung angezeigt und Sie sollten über die Befehlszeilenoberfläche fortfahren.

Weitere Hinweise zur Replikationsdrosselung:

- Drosselungen werden nur an der Quelle festgelegt. Die einzige Drosselung, die für ein Ziel gilt, ist die Option **0 Bps (Disabled)**, die jeglichen Replikationsdatenverkehr deaktiviert.
- Der Mindestwert für eine Replikationsdrosselung beträgt 98.304 Bit pro Sekunde.

Vorgehensweise

1. Wählen Sie **Replication** > **Advanced Settings** > **Add Throttle Setting**, um das Dialogfeld „Add Throttle Setting“ anzuzeigen.
2. Legen Sie die Wochentage fest, an denen die Drosselung aktiv sein soll, indem Sie **Every Day** auswählen oder durch Aktivierung der Kontrollkästchen neben den entsprechenden Tagen Ihre Auswahl treffen.
3. Legen Sie mit der Drop-down-Auswahl **Start Time** für die Stunde:Minute und „AM/PM“ die Zeit fest, zu der die Drosselung beginnen soll.
4. Für **Throttle Rate**:
   - Wählen Sie **Unlimited** aus, um keine Grenzen festzulegen.
   - Geben Sie eine Zahl in das Textfeld ein (z. B. 20.000) und wählen Sie die Rate aus dem Menü (bps, Kbps, Bps oder KBps).
   - Wählen Sie die Option **0 Bps (disabled)** aus, um jeglichen Replikationsdatenverkehr zu deaktivieren.
5. Klicken Sie auf **OK**, um diese Planung festzulegen. Die neue Planung wird unter **Permanent Schedule** angezeigt.

Ergebnisse

Die Replikation wird bis zur nächsten geplanten Änderungen oder bis zur Erzwingung einer Änderung durch eine neue Drosselungseinstellung mit der ausgewählten Rate ausgeführt.

Löschen der Drosselungseinstellungen

Sie können eine einzelne Drosselungseinstellung oder alle Drosselungseinstellungen auf einmal löschen.

Vorgehensweise

1. Wählen Sie **Replication** > **Advanced Settings** > **Delete Throttle Setting**, um das Dialogfeld „Delete Throttle Setting“ anzuzeigen.
2. Aktivieren Sie das Kontrollkästchen für die zu löschende Drosselungseinstellung oder das Kontrollkästchen darüber, um alle Einstellungen zu löschen. Diese Liste kann Einstellungen für den Status „disabled“ enthalten.

3. Wählen Sie **OK**, um die Einstellung zu entfernen.
4. Wählen Sie im Dialogfeld „Delete Throttle Setting Status“ die Option **Close**.

Vorübergehendes Außerkraftsetzen einer Drosselungseinstellung

Durch eine Außerkraftsetzung einer Drosselung wird eine Drosselungseinstellung vorübergehend geändert. Die aktuelle Einstellung ist oben im Fenster aufgeführt.

Vorgehensweise

1. Wählen Sie **Replication** > **Advanced Settings** > **Set Throttle Override**, um das Dialogfeld „Throttle Override“ anzuzeigen.
2. Legen Sie entweder eine neue Drosselungsaußerkraftsetzung fest oder löschen Sie eine vorherige Außerkraftsetzung.
   a. So legen Sie eine neue Drosselungsaußerkraftsetzung fest:
      - Wählen Sie **Unlimited** aus, um zu der vom System festgelegten Drosselungsrate zurückzukehren (Drosselung wird nicht durchgeführt) oder
      - Legen Sie Drosselungsbit und -rate im Textfeld fest (z. B. 20000) und bps, Kbps, Bps oder KBps) oder
      - Wählen Sie **0 Bps (Disabled)** aus, um die Drosselungsrate auf 0 festzulegen und damit im Wesentlichen den gesamten Replikationsnetzwerkdatenverkehr zu stoppen.
      - Wählen Sie **Clear at next scheduled throttle event** aus, um die Änderung vorübergehend zu erzwingen.

   b. Zum Löschen einer zuvor festgelegten Außerkraftsetzung wählen Sie **Clear Throttle Override**.
3. Wählen Sie **OK** aus.

Ändern der Netzwerkeinstellungen

Mithilfe der Bandbreiten- und Netzwerkverzögerungseinstellungen berechnet die Replikation die richtige TCP-Puffergröße (Transmission Control Protocol) für die Replikationsnutzung. Diese Netzwerkeinstellungen sind für das DD-System global und sollten nur einmal pro System festgelegt werden.

Beachten Sie Folgendes:

- Sie können die tatsächliche Bandbreite und die tatsächlichen Werte für die Netzwerkverzögerung für jeden Server über den Befehl `ping` ermitteln.
- Die Standardnetzwerkparameter in einem Restorer funktionieren gut für die Replikation in Konfigurationen mit niedriger Latenz, beispielsweise in einem lokalen Ethernetnetzwerk mit 100 Mbit/s oder 1.000 Mbit/s, in dem die Latenz-Round-Trip-Zeit (gemessen über den Befehl `ping`) für gewöhnlich unter 1 Millisekunde liegt. Die Standardeinstellungen funktionieren auch gut für die Replikation über WANs mit geringer bis mittlerer Bandbreite, in denen die Latenz bis zu 50 bis 100 Millisekunden hoch sein kann. Für Netzwerke mit hoher Bandbreite und hoher Latenz ist jedoch ein Tuning der Netzwerkparameter erforderlich.
  Eine wichtige Zahl für das Tuning ist der Wert für die Bandbreitenverzögerung, die durch Multiplizieren der Bandbreite mit der Round-Trip-Latenz des Netzwerks ermittelt werden kann. Diese Zahl ist ein Maß dafür, wie viele Daten über das Netzwerk übertragen werden können, bevor Bestätigungen vom anderen Ende zurückgegeben werden können. Wenn der Wert für die Bandbreitenverzögerung eines Replikationsnetzwerks über 100.000 liegt, profitiert die

Replikationsperformance von einer Festlegung der Netzwerkparameter in beiden Restorers.

Vorgehensweise

1. Wählen Sie **Replication** > **Advanced Settings** > **Change Network Settings** aus, um das Dialogfeld „Network Settings“ anzuzeigen.
2. Wählen Sie im Bereich „Network Settings“ **Custom Values** aus.
3. Geben Sie Werte für **Delay** und **Bandwidth** in die Textfelder ein. Die Einstellung für die Netzwerkverzögerung wird in Millisekunden, die für die Bandbreite in Byte pro Sekunde angegeben.
4. Geben Sie im Bereich „Listen Port“ einen neuen Wert in das Textfeld ein. Der Standard-IP-Überwachungsport für ein Replikationsziel zum Empfangen von Datenstreams aus der Replikationsquelle ist 2051. Das ist eine globale Einstellung für das DD-System.
5. Wählen Sie **OK** aus. Die neuen Einstellungen werden in der Tabelle mit den Netzwerkeinstellungen angezeigt.

Überwachen von Replikationen

DD System Manager bietet zahlreiche Möglichkeiten, den Replikationsstatus nachzuverfolgen: Prüfen des Replikationspaarstatus, Nachverfolgen von Backupjobs, Überprüfen der Performance, Nachverfolgen eines Replikationsprozesses.

Prüfen des Replikationspaarstatus

Statusupdates für Replikationspaare werden an verschiedenen Stellen im Replikationsbereich bereitgestellt.

Vorgehensweise

1. Wählen Sie **Replication** > **Topology**.
2. Prüfen Sie die Farben der Pfeile, die den Status des Kontexts zeigen.
3. Wählen Sie die Registerkarte **Summary** aus.
4. Wählen Sie im Drop-down-Menü **Filter By** (unter der Schaltfläche „Create Pair“) **State** aus und wählen Sie dann **Error**, **Warning** oder **Normal** aus dem Statusmenü aus.

   Die Replikationskontexte werden entsprechend der Auswahl sortiert.

Geschätzte Fertigstellungszeit für Backupjobs

Mithilfe von Completion Predictor können Sie die geschätzte Zeit für den Abschluss eines Backupreplikationsjobs anzeigen.

Vorgehensweise

1. Wählen Sie **Replication** > **Summary**.
2. Wählen Sie einen Replikationskontext aus, für den detaillierte Informationen angezeigt werden sollen.
3. Wählen Sie im Bereich „Completion Predictor“ Optionen aus der Drop-down-Liste **Source Time** für die Abschlusszeit einer Replikation und dann **Track** aus.

Die geschätzte Zeit für den Abschluss der Replikation an das Ziel eines bestimmten Backupjobs wird im Bereich „Completion Time“ angezeigt. Wenn die Replikation abgeschlossen ist, wird im Bereich `Completed` angezeigt.

Überprüfen der Performance eines Replikationskontexts

Wählen Sie zum Überprüfen der Performance eines Replikationskontexts über die Zeit einen Replikationskontext in der Ansicht „Summary“ und dann im Bereich „Detailed Information“ die Option **Performance Graph**.

Nachverfolgen des Status eines Replikationsprozesses

Zum Anzeigen des Fortschritts einer Replikationsinitialisierung, einer Neusynchronisierung oder einer Recovery verwenden Sie die Ansicht **Replication** > **Summary**, um den aktuellen Status zu überprüfen.

CLI-Entsprechung

```
# replication show config all
CTX  Source                                    Destination
Connection Host and Port     Enabled
---  ----------------------        ----------------------        ----------------------
-------
1       dir://host2/backup/dir2     dir://host3/backup/dir3
host3.company.com               Yes
2       dir://host3/backup/dir3     dir://host2/backup/dir2
host3.company.com               Yes
```

Verwenden Sie zum Angeben einer IP-Version den folgenden Befehl, um die Einstellung zu prüfen:

```
# replication show config rctx://2

CTX:                        2
Source:                     mtree://ddbeta1.dallasrdc.com/data/col1/EDM1
Destination:                mtree://ddbeta2.dallasrdc.com/data/col1/EDM_ipv6
Connection Host:            ddbeta2-ipv6.dallasrdc.com
Connection Port:            (default)
Ipversion:                  ipv6
Low-bw-optim:               disabled
Encryption:                 disabled
Enabled:                    yes
Propagate-retention-lock:   enabled
```

Replikation mit hoher Verfügbarkeit

Mit Floating-IP-Adressen können HA-Systeme eine einzelne IP-Adresse für die Replikationskonfiguration angeben, die unabhängig davon funktioniert, welcher Node des HA-Paars aktiv ist.

Über IP-Netzwerke verwenden HA-Systeme Floating IP-Adressen für den Datenzugriff auf das Data Domain-HA-Paar, unabhängig davon, welcher physische Node der aktive Node ist. Mit dem Befehl „net config“ wird die Option **`[type {fixed | floating}]`** bereitgestellt, mit der eine Floating-IP-Adresse konfiguriert werden kann. Weitere Informationen finden Sie im *Data Domain Operating System Command Reference Guide*.

Wenn ein Domainnamen zum Zugriff auf die Floating-IP-Adresse erforderlich ist, geben Sie den HA-Systemnamen als Domainname an. Führen Sie den Befehl `ha status` aus, um den HA-Systemnamen zu suchen.

Hinweis

Führen Sie den Befehl `net show hostname type ha-system` aus, um den HA-Systemnamen anzuzeigen, und führen Sie ggf. den Befehl `net set hostname ha-system command` aus, um den HA-Systemnamen zu ändern.

Der gesamte Dateisystemzugriff sollte über die Floating-IP-Adresse erfolgen. Geben Sie bei der Konfiguration von Backup- und Replikationsvorgängen auf einem HA-Paar immer die Floating-IP-Adresse als IP-Adresse für das Data Domain-System an. Data Domain-Funktionen wie DD Boost und Replikation akzeptieren die Floating-IP-Adresse für das HA-Paar auf die gleiche Weise, wie sie die System-IP-Adresse für ein Nicht-HA-System akzeptieren.

Replikation zwischen HA- und Nicht-HA-Systemen
Wenn Sie eine Replikation zwischen einem HA-System und einem System mit DD OS 5.7.0.3 oder früher einrichten möchten, müssen Sie diese Replikation auf dem HA-System erstellen und managen, wenn Sie die DD System Manager-GUI verwenden möchten.

Allerdings können Sie Replikationen von einem Nicht-HA-System zu einem HA-System über die Befehlszeilenoberfläche sowie vom HA-System zum Nicht-HA-System durchführen.

Sammlungsreplikation zwischen HA- und Nicht-HA-Systemen wird nicht unterstützt. Verzeichnis- oder MTree-Replikation ist erforderlich, um Daten zwischen HA- und Nicht-HA-Systemen zu replizieren.

Replizieren eines Systems mit Quotas auf ein System ohne Quotas

Replizieren Sie ein Data Domain-System mit einem DD OS, das Quotas unterstützt, auf ein System mit einem DD OS ohne Quotas.

- Eine umgekehrte Neusynchronisierung, die die Daten aus dem System ohne Quotas erstellt und diese wieder in einem MTree auf dem System bereitstellt, das Quotas aktiviert hat (und sie auch weiterhin aktiviert haben wird)
- Eine umgekehrte Initialisierung vom System ohne Quotas, bei der die Daten genommen werden und ein neuer MTree auf dem System erstellt wird, das Quotas unterstützt, aber keine Quotas aktiviert hat, da er aus Daten eines Systems ohne Quotas erstellt wurde

Hinweis

Quotas wurden ab DD OS 5.2 eingeführt.

Replikationskontextskalierung

Die Funktion der Replikationskontextskalierung bietet Ihnen mehr Flexibilität bei der Konfiguration von Replikationskontexten.

In Umgebungen mit mehr als 299 Replikationskontexten, die sowohl Verzeichnisreplikationskontexte als auch MTree-Replikationskontexte umfassen, können Sie mit dieser Funktion die Kontexte in beliebiger Reihenfolge konfigurieren. Zuvor mussten Sie zunächst die Verzeichnisreplikationskontexte gefolgt von den MTree-Replikationskontexten konfigurieren.

Die Gesamtzahl der Replikationskontexte darf 540 nicht überschreiten.

Hinweis

Diese Funktion wird nur auf Data Domain-Systemen mit DD OS Version 6.0 angezeigt.

Replikationsmigration (Verzeichnis zu MTree)

Mit der Replikationsoptimierungsfunktion Verzeichnis zu MTree (Directory-to-MTree, D2M) können Sie vorhandene Verzeichnisreplikationskontexte zu neuen Replikationskontexten migrieren, die auf MTrees basieren, die logische Partitionen des Dateisystems sind. Mit dieser Funktion können Sie außerdem den Prozess im Verlauf überwachen und überprüfen, ob er erfolgreich abgeschlossen wurde.

Die D2M-Funktion ist kompatibel mit Data Domain Operating System Version 6.0, 5.7 und 5.6.

Das Data Domain-Quellsystem muss zur Verwendung dieser Funktion mit DD OS 6.0 ausgeführt werden, aber das Zielsystem kann mit 6.0, 5.7 oder 5.6 ausgeführt werden. Allerdings sind die Vorteile der Performanceoptimierung nur dann verfügbar, wenn sowohl die Quell- als auch die Zielsysteme auf 6.0 ausgeführt werden.

Hinweis

Obwohl Sie die grafische Benutzeroberfläche (GUI) für diesen Vorgang verwenden können, wird für eine optimale Performance empfohlen, die Befehlszeilenoberfläche (CLI) zu verwenden.

Durchführen einer Migration von Verzeichnisreplikation zu MTree-Replikation

Fahren Sie das System während der Verzeichnis-zu-MTree-Migration (D2M) nicht herunter und starten Sie es nicht neu.

Vorgehensweise

1. Beenden Sie alle Aufnahmevorgänge in das Quellverzeichnis der Verzeichnisreplikation.
2. Erstellen Sie einen MTree auf dem DD-Quellsystem: `mtree create /data/col1/mtree-name`

   Hinweis

   Erstellen Sie den MTree nicht auf dem DD-Zielsystem.

3. (Optional) Aktivieren Sie DD Retention Lock auf dem MTree.

   Hinweis

   Wenn das Quellsystem zwecks Aufbewahrung gesperrte Dateien enthält, sollten Sie DD Retention Lock auf dem neuen MTree beibehalten.

   Siehe Aktivieren von DD Retention Lock Compliance auf einem MTree.
4. Erstellen Sie den MTree-Replikationskontext auf den DD-Quell- und Zielsystemen: `replication add source mtree://source-system-name/source mtree replication add destination mtree://destination-system-name/destination mtree`

5. Starten Sie die D2M-Migration: **replication dir-to-mtree start from *rctx://1* to *rctx://2***

   Im vorherigen Beispiel bezieht sich
   `rctx://1`
   auf den Verzeichnisreplikationskontext, mit dem das Verzeichnis `backup backup/dir1` auf dem Quellsystem repliziert wird;
   `rctx://2`
   bezieht sich auf den MTree-Replikationskontext, mit dem der MTree `/data/col1/mtree1` auf dem Quellsystem repliziert wird.

   Hinweis

   Die Ausführung dieses Befehls kann länger dauern als erwartet. Drücken Sie während dieses Prozesses nicht STRG + C. Wenn Sie dies tun, brechen Sie die D2M-Migration ab.

```
Phase 1 of 4 (precheck):
    Marking source directory /backup/dir1 as read-only...Done.

Phase 2 of 4 (sync):
    Syncing directory replication context...0 files flushed.
current=45 sync_target=47 head=47
current=45 sync_target=47 head=47
Done. (00:09)

Phase 3 of 4 (fastcopy):
    Starting fastcopy from /backup/dir1 to /data/col1/
mtree1...
    Waiting for fastcopy to complete...(00:00)
    Fastcopy status: fastcopy /backup/dir1 to /data/col1/
mtree1: copied 24
files, 1 directory in 0.13 seconds
    Creating snapshot 'REPL-D2M-
mtree1-2015-12-07-14-54-02'...Done

Phase 4 of 4 (initialize):
    Initializing MTree replication context...
(00:08) Waiting for initialize to start...
(00:11) Initialize started.

Use 'replication dir-to-mtree watch rctx://2' to monitor
progress.
```

Anzeigen des Fortschritts der Verzeichnis-zu-MTree-Datenmigration

Sie können sehen, welche Phase der Migration derzeit in der Verzeichnis-zu-MTree-Replikation (D2M) ausgeführt wird.

Vorgehensweise

1. Geben Sie den Befehl **replication dir-to-mtree watch*rctx://2*** ein, um den Fortschritt anzuzeigen.

   `rctx://2`
   gibt den Replikationskontext an.

   Sie sollten die folgende Ausgabe sehen können:

```
Use Control-C to stop monitoring.
Phase 4 of 4 (initialize).
```

```
(00:00) Replication initialize started...
(00:02) initializing:
(00:14)     100% complete, pre-comp: 0 KB/s, network: 0 KB/
s
(00:14) Replication initialize completed.
Migration for ctx 2 successfully completed.
```

Überprüfen des Status der Verzeichnis-zu-MTree-Replikationsmigration

Sie können mit dem Befehl `replication dir-to-mtree status` überprüfen, ob die Verzeichnis-zu-MTree-Migration (D2M) erfolgreich abgeschlossen wurde.

Vorgehensweise

1. Geben Sie den folgenden Befehl ein. Hierbei steht `rctx://2` für den Mtree-Replikationskontext auf dem Quellsystem: **`replication dir-to-mtree status rctx://2`**

   Die Ausgabe sollte der folgenden ähneln:

   ```
   Directory Replication CTX:          1
   MTree Replication CTX:              2
   Directory Replication Source:       dir://127.0.0.2/backup/dir1
   MTree Replication Source:           mtree://127.0.0.2/data/
   col1/mtree1
   MTree Replication Destination:      mtree://127.0.0.3/data/
   col1/mtree1
   Migration Status:                   completed
   ```

   Wenn keine Migration durchgeführt wird, sollten Sie die folgende Ausgabe erhalten:

   ```
   # replication dir-to-mtree status rctx://2
   No migration status for context 2.
   ```

2. Beginnen Sie mit der Aufnahme der Dateien in den MTree auf dem DD-Quellsystem, wenn der Migrationsprozess abgeschlossen ist.
3. (Optional) Unterbrechen Sie den Verzeichnisreplikationskontext auf den Quell- und Zielsystemen.

   Weitere Informationen zum Befehl `replication break` finden Sie im *Data Domain Operating System Version 6.0 Command Reference Guide*.

Abbrechen der D2M-Replikation

Falls erforderlich, können Sie das Verzeichnis-zu-MTree-Migrationsverfahren (D2M) abbrechen.

Mit dem Befehl `replication dir-to-mtree abort` wird das laufende Migrationsverfahren abgebrochen und das Verzeichnis von einem Nur-Lese- auf einen Lese-/Schreibstatus zurückgesetzt.

Vorgehensweise

1. Geben Sie in der Befehlszeilenoberfläche (CLI) den folgenden Befehl ein. Hierbei ist `rctx://2`

der MTree-Replikationskontext: **replication dir-to-mtree abort *rctx://2***

Sie sollten die folgende Ausgabe sehen können:

```
Canceling directory to MTree migration for context dir-name.
Marking source directory dir-name as read-write...Done.
The migration is now aborted.
Remove the MTree replication context and MTree on both source
and destination
host by running 'replication break' and 'mtree delete'
commands.
```

2. Unterbrechen Sie den MTree-Replikationskontext: **replication break *rctx://2***
3. Löschen Sie den MTree auf dem Quellsystem: **mtree delete *mtree-path***

D2M-Troubleshooting

Wenn Sie auf ein Problem bei der Verzeichnis-zu-MTree-Replikation (D2M) stoßen, können Sie einen Vorgang durchführen, mit dem Sie mehrere verschiedene Probleme angehen können.

Das Verfahren `dir-to-mtree abort` hilft dabei, den D2M-Prozess ordnungsgemäß abzubrechen. Sie sollten dieses Verfahren in den folgenden Fällen ausführen:

- Der Status der D2M-Migration wird als abgebrochen aufgeführt.
- Das Data Domain-System wird während der D2M-Migration neu gestartet.
- Ein Fehler ist während der Ausführung des Befehls `replication dir-to-mtree start` aufgetreten.
- Die Aufnahme wurde nicht beendet, bevor mit der Migration begonnen wurde.
- Der MTree-Replikationskontext wurde initialisiert, bevor der Befehl `replication dir-to-mtree start` eingegeben wurde.

Hinweis

Führen Sie den Befehl **replication break** nicht für den MTree-Replikationskontext aus, bevor der D2M-Prozess abgeschlossen ist.
Führen Sie immer den Befehl **replication dir-to-mtree abort** vor dem Befehl **replication break** für „mrepl ctx“ aus.

Das vorzeitige Ausführen des Befehls **replication break** gibt das Quellverzeichnis „drepl“ dauerhaft als schreibgeschützt zurück.

Wenn dies auftritt, wenden Sie sich an den Support.

Vorgehensweise

1. Geben Sie den Befehl **replication dir-to-mtree abort** ein, um den Prozess abzubrechen.
2. Unterbrechen Sie den neu erstellten MTree-Replikationskontext sowohl auf den Data Domain-Quell- als auch -Zielsystemen.

   Im folgenden Beispiel ist der MTree-Replikationskontext `rctx://2`

.

```
replication break rctx://2
```

3. Löschen Sie die entsprechenden MTrees auf den Quell- und Zielsystemen.

```
mtree delete mtree-path
```

Hinweis

Zur Löschung markierte MTrees verbleiben im Dateisystem, bis der Befehl `filesys clean` ausgeführt wird.

Weitere Informationen finden Sie im *Data Domain Operating System Version 6.0 Command Reference Guide*.

4. Führen Sie den Befehl `filesys clean start` sowohl auf den Quell- als auch auf den Zielsystemen aus.

   Weitere Informationen zu den `filesys clean`-Befehlen finden Sie im *Data Domain Operating System Version 6.0 Command Reference Guide*.

5. Starten Sie den Prozess neu.

   Siehe Durchführen einer Migration von Verzeichnisreplikation zu MTree-Replikation.

Zusätzliches D2M-Troubleshooting

Es sind Lösungen verfügbar, wenn Sie vergessen haben, DD Retention Lock für den neuen MTree zu aktivieren, oder wenn ein Fehler auftritt, nachdem die Verzeichnis-zu-MTree-Migration initialisiert wurde.

DD Retention Lock wurde nicht aktiviert.
Wenn Sie vergessen haben, DD Retention Lock für den neuen MTree zu aktivieren, und das Quellverzeichnis zur Aufbewahrung gesperrte Dateien oder Verzeichnisse enthält, haben Sie die folgenden Optionen:

- Setzen Sie die D2M-Migration fort. Allerdings liegen keine DD Retention Lock-Informationen im MTree nach der Migration vor.
- Brechen Sie den aktuellen D2M-Prozess wie in Abbrechen der D2M-Replikation auf Seite 477 beschrieben ab und starten Sie den Prozess mit aktiviertem DD Retention Lock auf dem Quell-MTree erneut.

Nach der Initialisierung tritt ein Fehler auf.
Wenn der Prozess `replication dir-to-mtree start` ohne Fehler abgeschlossen wird, Sie jedoch einen Fehler während der Initialisierung der MTree-Replikation (Phase 4 des D2M-Migrationsprozesses) erkennen, können Sie die folgenden Schritte ausführen:

1. Stellen Sie sicher, dass kein Netzwerkproblem vorliegt.
2. Initialisieren Sie den MTree-Replikationskontext.

Verwenden der Sammelreplikation zur Disaster Recovery mit SMT

Um das Zielsystem eines mit SMT konfigurierten Sammelreplikationspaars als Ersatzsystem für die Disaster Recovery zu verwenden, müssen weitere SMT-Konfigurationsschritte zusätzlich zu den anderen Konfigurationsschritten zur Onlinestellung eines Ersatzsystems durchgeführt werden.

Bevor Sie beginnen

Die Verwendung des Sammelreplikationszielsystems auf diese Weise erfordert das Konfigurieren und Speichern von Autosupport-Berichten. Weitere Informationen finden Sie im Wissensdatenbankartikel *Collection replica with smt enabled* unter https://support.emc.com.

Die Ersatzsystem verfügt nicht über die folgenden SMT-Details:

- Warnmeldungsbenachrichtigungslisten für jede Mandanteneinheit
- Alle Benutzer, die dem DD Boost-Protokoll von SMT-Mandanten zugewiesen sind, wenn DD Boost auf dem System konfiguriert ist
- Die Standardmandanteneinheit, die mit jedem DD Boost-Benutzer verbunden ist, falls vorhanden, wenn DD Boost auf dem System konfiguriert ist

Führen Sie die folgenden Schritte aus, um SMT auf dem Ersatzsystem zu konfigurieren.

Vorgehensweise

1. Suchen Sie im Autosupport-Bericht nach der Ausgabe für den Befehl `smt tenant-unit show detailed`.

```
Tenant-unit: "tu1"
Summary:
Name   Self-Service   Number of Mtrees   Types           Pre-Comp(GiB)
----   ------------   ----------------   --------        -------------
tu1    Enabled        2                  DD Boost        2.0
----   ------------   ----------------   --------        -------------

Management-User:
User     Role
------   ------------
tu1_ta   tenant-admin
tu1_tu   tenant-user
tum_ta   tenant-admin
------   ------------

Management-Group:
Group    Role
------   ------------
qatest   tenant-admin
------   ------------

DDBoost:
Name   Pre-Comp (GiB)   Status   User    Tenant-Unit
----   --------------   ------   -----   -----------
su1               2.0   RW/Q     ddbu1   tu1
----   --------------   ------   -----   -----------
Q    : Quota Defined
RO   : Read Only
RW   : Read Write

Getting users with default-tenant-unit tu1
DD Boost user   Default tenant-unit
-------------   -------------------
```

```
ddbu1           tu1
-------------   -------------------

Mtrees:
Name             Pre-Comp (GiB)   Status   Tenant-Unit
--------------   --------------   ------   -----------
/data/col1/m1               0.0   RW/Q     tu1
/data/col1/su1              2.0   RW/Q     tu1
--------------   --------------   ------   -----------
D    : Deleted
Q    : Quota Defined
RO   : Read Only
RW   : Read Write
RD   : Replication Destination
RLGE : Retention-Lock Governance Enabled
RLGD : Retention-Lock Governance Disabled
RLCE : Retention-Lock Compliance Enabled

Quota:
Tenant-unit: tu1
Mtree            Pre-Comp (MiB)   Soft-Limit (MiB)   Hard-Limit(MiB)
--------------   --------------   ----------------   ----------------
/data/col1/m1                 0              71680             81920
/data/col1/su1             2048              30720             51200
--------------   --------------   ----------------   ----------------

Alerts:
Tenant-unit: "tu1"
Notification list "tu1_grp"
Members
------------------
tom.tenant@abc.com
------------------

No such active alerts.
```

2. Aktivieren Sie SMT auf dem Ersatzsystem, wenn es noch nicht aktiviert ist.
3. Lizenzieren und aktivieren Sie DD Boost auf dem Ersatzsystem, wenn es erforderlich und noch nicht aktiviert ist.
4. Wenn DD Boost konfiguriert ist, weisen Sie jeden im Abschnitt `DD Boost` der Ausgabe „smt tenant-unit show detailed“ aufgeführten Benutzer als DD Boost-Benutzer zu.

   ```
   # ddboost user assign ddbu1
   ```

5. Wenn DD Boost konfiguriert ist, weisen Sie jeden im Abschnitt `DD Boost` der Ausgabe `smt tenant-unit show detailed` aufgeführten Benutzer der angezeigten Standardmandanteneinheit in der Ausgabe zu, falls vorhanden.

   ```
   # ddboost user option set ddbu1 default-tenant-unit tu1
   ```

6. Erstellen Sie eine neue Gruppe für Warnmeldungsbenachrichtigungen mit dem gleichen Namen wie die Gruppe für Warnmeldungsbenachrichtigungen im Abschnitt `Alerts` der Ausgabe `smt tenant-unit show detailed`.

   ```
   # alert notify-list create tu1_grp tenant-unit tu1
   ```

7. Weisen Sie jede E-Mail-Adresse in der Gruppe für Warnmeldungsbenachrichtigungen im Abschnitt `Alerts` der Ausgabe `smt tenant-unit show detailed` der neuen Gruppe für Warnmeldungsbenachrichtigungen zu..

   ```
   # alert notify-list add tu1_grp emails tom.tenant@abc.com
   ```

KAPITEL 17

DD Secure Multitenancy

Inhalt dieses Kapitels:

Überblick über Data Domain Secure Multi-tenancy

Data Domain *Secure Multi-tenancy (SMT)* bezieht sich auf das Hosting einer IT-Infrastruktur durch eine interne IT-Abteilung oder einen externen Anbieter für mehr als einen Verbraucher/eine Workload (Geschäftsbereich/Abteilung/Mandant) gleichzeitig.

SMT bietet die Möglichkeit, viele Benutzer und Workloads in einer gemeinsamen Infrastruktur sicher zu isolieren, sodass die Aktivitäten eines Mandanten nicht für die anderen Mandanten ersichtlich oder sichtbar sind.

Ein *Mandant* ist ein Verbraucher (Geschäftsbereich/Abteilung/Kunde), der dauerhaft in einer gehosteten Umgebung präsent ist.

Innerhalb eines Unternehmens besteht möglicherweise ein Mandant aus einem oder mehreren Geschäftseinheiten oder Abteilungen auf einem Data Domain-System, das von den IT-Mitarbeitern konfiguriert und gemanagt wird.

- In einem Anwendungsbeispiel für eine Geschäftseinheit könnten die Finanzabteilung und die Personalabteilung eines Unternehmens das gleiche DD-System nutzen, aber jede Abteilung bemerkt das Vorhandensein der anderen nicht.
- In einem Anwendungsbeispiel für einen Serviceanbieter (SP) könnte der SP eine oder mehrere Data Domain-Systeme nutzen, um verschiedene Datenschutzspeicherservices für mehrere Endkunden anzubieten.

Beide Anwendungsbeispiele heben die Trennung von verschiedenen Kundendaten auf demselben physischen Data Domain-System hervor.

SMT-Architektur – Grundlagen

Secure Multitenancy (SMT) bietet einen einfachen Ansatz für das Konfigurieren von Mandanten und Mandanteneinheiten mit MTrees. Die SMT-Konfiguration wird mithilfe von DD Management Center und/oder der DD OS-Befehlszeilenoberfläche durchgeführt. Dieses Administratorhandbuch beschreibt die Funktionsweise von SMT und einige allgemeine Befehlszeilenanweisungen.

Die grundlegende Architektur von SMT ist wie folgt.

- Ein Mandant wird in DD Management Center und/oder im DD-System erstellt.
- Eine Mandanteneinheit wird auf einem DD-System für den Mandanten erstellt.
- Ein oder mehrere MTrees werden erstellt, um die Speicheranforderungen der verschiedenen Backuptypen des Mandanten zu erfüllen.
- Die neu erstellten MTrees werden der Mandanteneinheit hinzugefügt.
- Backupanwendungen sind so konfiguriert, dass jedes Backup an seinen konfigurierten Mandanteneinheit-MTree gesendet wird.

Hinweis

Weitere Informationen zu DD Managment Center finden Sie im *DD Management Center User Guide*. Weitere Informationen zur DD OS-Befehlszeilenoberfläche finden Sie in der *DD OS Command Reference*.

Für Secure Muti-Tenancy (SMT) verwendete Terminologie

Die Kenntnis der für SMT verwendeten Terminologie ermöglicht ein besseres Verständnis dieser besonderen Umgebung.

MTrees
MTrees sind logische Partitionen des Dateisystems. Sie bieten ein Höchstmaß an Managementgranularität. Das bedeutet, dass die Benutzer die Vorgänge auf einem bestimmten MTree ausführen können, ohne das gesamte Dateisystem zu beeinträchtigen. MTrees werden Mandanteneinheiten zugewiesen und enthalten die individuellen Einstellungen der Mandanteneinheiten für das Management und Monitoring der SMT-Umgebung.

Mehrmandantenfähigkeit
Mehrmandantenfähigkeit bezieht sich auf das Hosting einer IT-Infrastruktur durch eine interne IT-Abteilung oder einen externen Serviceanbieter für mehr als einen Verbraucher/eine Workload (Geschäftsbereich/Abteilung/Mandant) gleichzeitig. Data Domain SMT ermöglicht *Data Protection as a Service*.

RBAC (Role-Based Access Control, rollenbasierte Zugriffskontrolle)
RBAC bietet mehrere Rollen mit unterschiedlichen Berechtigungsleveln, die zusammen die Verwaltungsisolierung auf einem Data Domain-System mit mehreren Mandanten bieten. (Diese Rollen werden im nächsten Abschnitt definiert.)

Speichereinheit
Eine *Speichereinheit* ist ein MTree, der für das DD Boost-Protokoll konfiguriert ist. Datenisolierung wird erreicht, indem eine Speichereinheit erstellt und einem DD Boost-Benutzer zugewiesen wird. Das DD Boost-Protokoll ermöglicht nur Zugriff auf Speichereinheiten, die DD Boost-Benutzern zugewiesen sind, die mit dem Data Domain-System verbunden sind.

Tenant
Ein *Mandant* ist ein Verbraucher (Geschäftsbereich/Abteilung/Kunde), der eine dauerhafte Präsenz in einer gehosteten Umgebung beibehält.

Mandanten-Selfservice
Der *Mandanten-Selfservice* ist eine Methode, mit der ein Mandant sich bei einem Data Domain-System anmelden kann, um einige grundlegende Services durchzuführen (Hinzufügen, Bearbeiten oder Löschen lokaler Benutzer, NIS-Gruppen und/oder AD-Gruppen). Dies macht es überflüssig, stets einen Administrator für diese grundlegenden Aufgaben einzubeziehen. Der Mandant kann nur auf seine zugewiesenen Mandanteneinheiten zugreifen. Mandantenbenutzer und Mandantenadministratoren haben natürlich unterschiedliche Rechte.

Mandanteneinheit
Eine *Mandanteneinheit* ist die Partition eines Data Domain-Systems, die als Einheit der administrativen Isolierung zwischen Mandanten fungiert. Mandanteneinheiten, die einem Mandanten zugewiesen sind, können sich auf demselben oder unterschiedlichen Data Domain-Systemen befinden und werden gesichert und logisch voneinander isoliert. Dadurch wird für die Sicherheit und Isolierung des Kontrollpfads gesorgt, wenn mehrere Mandanten gleichzeitig in der freigegebenen Infrastruktur ausgeführt werden. Mandanteneinheiten können einen oder mehrere *MTrees* enthalten, die alle Konfigurationselemente umfassen, die in einem mehrmandantenfähigen Setup benötigt werden. Benutzer, Managementgruppen, Benachrichtigungsgruppen und andere Konfigurationselemente sind Teil einer Mandanteneinheit.

Kontrollpfad- und Netzwerkisolierung

Die *Kontrollpfadisolierung* wird erreicht, indem die Benutzerrollen *tenant-admin* und *tenant-user* für eine Mandanteneinheit bereitgestellt werden. Die *Netzwerkisolierung* für den Daten- und Administratorzugriff wird erreicht, indem Sie einen festen Satz an *Datenzugriffs-IP-Adressen* und *Management-IP-Adressen* einer Mandanteneinheit zuordnen.

Diese Rollen *tenant-admin* und *tenant-user* werden in Umfang und Funktion auf bestimmte Mandanteneinheiten und auf einen eingeschränkten Satz von Vorgängen eingeschränkt, die sie in diesen Mandanteneinheiten durchführen können. Um einen logisch sicheren und isolierten Datenpfad zu ermöglichen, muss ein Systemadministrator mindestens einen Mandanteneinheiten-MTree für jedes Protokoll in einer SMT-Umgebung konfigurieren. Zu den unterstützten Protokollen zählen DD Boost, NFS, CIFS und DD VTL. Der Zugriff wird über die nativen Zugriffskontrollmechanismen jedes Protokolls streng reguliert.

Mandanten-Selfservice-Sitzungen (über ssh) können auf einen festen Satz an *Management-IP-Adressen* auf einem DD-System beschränkt werden. Administrative Zugriffssitzungen (über ssh/http/https) können auch auf einen festen Satz von Management-IP-Adressen auf DD-Systemen beschränkt werden. Standardmäßig sind jedoch keine Management-IP-Adressen vorhanden, die einer Mandanteneinheit zugeordnet sind. Das heißt, die Standardeinschränkung erfolgt über die Verwendung der Rollen *tenant-admin* und *tenant-user*. Sie müssen `smt tenant-unit management-ip` verwenden, um Management-IP-Adressen für Mandanteneinheiten hinzuzufügen und zu verwalten.

Auf ähnliche Weise kann der Datenzugriff und der Datenfluss (in den und aus den Mandanteneinheiten) auf einen festen Satz an *Datenzugriffs-IP-Adressen* (lokal oder remote) beschränkt sein. Die Verwendung der zugewiesenen Datenzugriffs-IP-Adressen erhöht die Sicherheit der DD Boost- und NFS-Protokolle durch Hinzufügen von SMT-bezogenen Sicherheitsprüfungen. Beispielsweise kann die Liste der über DD Boost-RPC zurückgegebenen Speichereinheiten auf diejenigen beschränkt werden, die zur Mandanteneinheit mit der zugewiesenen lokalen Datenzugriffs-IP-Adresse gehören. Für NFS können der Zugriff und die Transparenz von Exporten basierend auf den konfigurierten lokalen Datenzugriffs-IP-Adressen gefiltert werden. Durch die Verwendung von `showmount -e` aus der lokalen Datenzugriffs-IP-Adresse einer Mandanteneinheit werden nur NFS-Exporte angezeigt, die zu dieser Mandanteneinheit gehören.

Der Benutzer *sysadmin* muss den Befehl `smt tenant-unit data-ip` zum Hinzufügen und Verwalten von Datenzugriffs-IP-Adressen für Mandanteneinheiten verwenden.

Hinweis

Wenn Sie versuchen, einen MTree in einer SMT-IP-Adresse über eine Nicht-SMT-IP-Adresse zu mounten, schlägt der Vorgang fehl.

Mehrere Mandanteneinheiten, die zum selben Mandanten gehören, können ein Standardgateway gemeinsam verwenden. Mehrere Mandanteneinheiten, die zu unterschiedlichen Mandanten gehören, können dasselbe Standardgateway jedoch nicht gemeinsam verwenden.

Mehrere zum selben Mandanten gehörende Mandanteneinheiten können ein Standardgateway gemeinsam verwenden. Mehrere zu unterschiedlichen Mandanten gehörende Mandanteneinheiten können nicht dasselbe Standardgateway verwenden.

RBAC in SMT

Bei SMT (Secure Multi-Tenancy) ist die Berechtigung zur Ausführung einer Aufgabe von der einem Benutzer zugewiesenen Rolle abhängig. DD Management Center steuert diese Berechtigungen mithilfe von RBAC (Role-Based Access Control, rollenbasierte Zugriffskontrolle).

Alle DD Management Center-Benutzer können:

- alle Mandanten anzeigen
- Mandanteneinheiten eines beliebigen Mandanten erstellen, lesen, aktualisieren oder löschen, sofern der Benutzer auf dem Data Domain-Hostsystem der Mandanteneinheit über Administratorrechte verfügt
- Zuweisungen zwischen Mandanteneinheiten und Mandanten herstellen und aufheben, sofern der Benutzer auf dem Data Domain-Hostsystem der Mandanteneinheit über Administratorrechte verfügt
- Mandanteneinheiten eines beliebigen Mandanten anzeigen, sofern dem Benutzer auf dem Data Domain-Hostsystem der Mandanteneinheit eine beliebige Rolle zugewiesen ist

Die Durchführung erweiterter Aufgaben ist von der jeweiligen Benutzerrolle abhängig:

Rolle „admin“
Ein Benutzer mit der Rolle *admin* kann alle Administrationsvorgänge auf einem Data Domain-System durchführen. Die Rolle *admin* kann auch alle SMT-Administrationsvorgänge auf einem Data Domain-System durchführen und z. B. SMT einrichten, SMT-Benutzerrollen zuweisen, den Mandanten-Selfservice-Modus aktivieren, Mandanten erstellen usw. Im Kontext von SMT wird der *admin* in der Regel als *landlord* bezeichnet. In DD OS ist dies die Rolle *sysadmin*.

Für die Berechtigung zum Bearbeiten oder Löschen von Mandanten sind sowohl die DD Management Center-Rolle *admin* als auch die DD OS-Rolle *sysadmin* auf allen Data Domain-Systemen erforderlich, die den Mandanteneinheiten des entsprechenden Mandanten zugeordnet sind. Wenn der Mandant nicht über Mandanteneinheiten verfügt, ist zum Bearbeiten oder Löschen des Mandanten lediglich die DD Management Center-Rolle *admin* erforderlich.

Rolle „limited-admin“
Ein Benutzer mit der Rolle *limited-admin* kann alle Administrationsvorgänge auf einem Data Domain-System als *admin* durchführen. Benutzer mit der Rolle *limited-admin* können jedoch keine MTrees löschen oder entfernen. In DD OS gibt es die entsprechende Rolle *limited-admin*.

Rolle „tenant-admin“
Ein Benutzer mit der Mandantenadministratorrolle (*tenant-admin*) kann bestimmte Aufgaben nur durchführen, wenn der *Mandanten-Selfservice-Modus* für eine bestimmte Mandanteneinheit aktiviert ist. Zum Verantwortungsbereich dieser Rolle gehören die Planung und Ausführung einer Backupanwendung für den Mandanten sowie das Monitoring von Ressourcen und Statistiken innerhalb der zugewiesenen Mandanteneinheit. Die Rolle *tenant-admin* kann Auditprotokolle anzeigen. RBAC sorgt jedoch dafür, dass nur auf die Auditprotokolle der Mandanteneinheiten zugegriffen werden kann, die zu der Rolle *tenant-admin* gehören. Darüber hinaus stellen *tenant-admins* eine administrative Trennung dar, wenn der Mandanten-Selfservice-Modus aktiviert ist. Im Kontext von SMT wird die Rolle *tenant-admin* in der Regel als *backup admin* bezeichnet.

Rolle „tenant-user“
Die Rolle *tenant-user* ermöglicht Benutzern das Monitoring der Performance und der Nutzung der SMT-Komponenten nur für ihre zugewiesenen Mandanteneinheiten bei aktiviertem Mandanten-Selfservice-Modus. Ein Nutzer mit dieser Rolle kann jedoch keine Auditprotokolle für die ihm zugewiesenen Mandanteneinheiten anzeigen. Darüber hinaus können *tenant-users* die Befehle `show` und `list` ausführen.

Rolle „none“
Ein Benutzer mit der Rolle *none* ist nicht berechtigt, weitere Vorgänge an einem Data Domain-System auszuführen, die über das Ändern des Passworts und den Zugriff auf Daten mithilfe von DD Boost hinausgehen. Nachdem SMT aktiviert wurde, kann der

Benutzer mit der Rolle *admin* jedoch einen Benutzer mit der Rolle *none* aus dem Data Domain-System auswählen und ihm die SMT-spezifische Rolle *tenant-admin* oder *tenant-user* zuweisen. Anschließend kann der Benutzer Vorgänge an SMT-Managementobjekten durchführen.

Managementgruppen

BSPs (Backupserviceprovider) können mithilfe von *Managementgruppen*, die in einem einzigen externen AD (Active Directory) oder NIS (Network Information Service) definiert werden, das Management von Benutzerrollen für Mandanteneinheiten vereinfachen. Jeder BSP-Mandant kann ein separates, externes Unternehmen sein und einen Namensservice wie Active Directory oder NIS verwenden.

Mit SMT-Managementgruppen werden die AD- und NIS-Server durch den *admin* auf die gleiche Weise wie lokale SMT-Benutzer eingerichtet und konfiguriert. Der *admin* kann den AD- oder NIS-Administrator bitten, die Gruppe zu erstellen und zu füllen. Der *admin* weist dann der gesamten Gruppe eine SMT-Rolle zu. Jeder Benutzer innerhalb der Gruppe, der sich beim Data Domain-System anmeldet, wird mit der Rolle angemeldet, die der Gruppe zugewiesen ist.

Wenn Benutzer einem Mandantenunternehmen beitreten oder es verlassen, können sie der Gruppe durch den AD- oder NIS-Administrator hinzugefügt bzw. aus der Gruppe entfernt werden. Die RBAC-Konfiguration auf einem Data Domain-System muss nicht geändert werden, wenn Benutzer hinzugefügt oder entfernt werden, die Teil der Gruppe sind.

Provisioning einer Mandanteneinheit

Beim Starten des Konfigurationsassistenten beginnt das erste Provisioning-Verfahren für SMT (Secure Multitenancy). Während des Verfahrens erstellt der Assistent eine neue Mandanteneinheit basierend auf Mandantenkonfigurationsanforderungen und stellt sie bereit. Informationen werden vom Administrator nach Aufforderung eingegeben. Nach Abschluss des Verfahrens fährt der Administrator mit den nächsten Aufgaben fort, beginnend mit der Aktivierung des Mandantenselfservice-Modus. Nach der erstmaligen Einrichtung können manuelle Verfahren und Konfigurationsänderungen nach Bedarf ausgeführt werden.

Vorgehensweise

1. Starten Sie SMT.

   ```
   # smt enable SMT enabled.
   ```

2. Überprüfen Sie, ob SMT aktiviert ist.

   ```
   # smt status SMT is enabled.
   ```

3. Starten Sie den SMT-Konfigurationsassistenten.

   ```
   # smt tenant-unit setup No tenant-units.
   ```

4. Befolgen Sie die Konfigurationsanweisungen.

```
SMT TENANT-UNIT Configuration

  Configure SMT TENANT-UNIT at this time (yes|no) [no]: yes

  Do you want to create new tenant-unit (yes/no)? : yes

Tenant-unit Name
  Enter tenant-unit name to be created
  : SMT_5.7_tenant_unit
Invalid tenant-unit name.
  Enter tenant-unit name to be created
  : SMT_57_tenant_unit
```

```
Pending Tenant-unit Settings
Create Tenant-unit   SMT_57_tenant_unit

Do you want to save these settings (Save|Cancel|Retry): save
SMT Tenant-unit Name Configurations saved.

SMT TENANT-UNIT MANAGEMENT-IP Configuration

  Configure SMT TENANT-UNIT MANAGEMENT-IP at this time (yes|no) [no]: yes

  Do you want to add a local management ip to this tenant-unit? (yes|no) [no]: yes

port  enabled  state  DHCP        IP address              netmask     type additional
                                                       /prefix length        setting
----- ------- ------- ---- ------------------------- -------------- ---- ----------
ethMa   yes   running  no  192.168.10.57             255.255.255.0   n/a
                           fe80::260:16ff:fe49:f4b0** /64
eth3a   yes   running ipv4 192.168.10.236*           255.255.255.0*  n/a
                           fe80::260:48ff:fe1c:60fc** /64
eth3b   yes   running  no  192.168.50.57             255.255.255.0   n/a
                           fe80::260:48ff:fe1c:60fd** /64
eth4b   yes   running  no  192.168.60.57             255.255.255.0   n/a
                           fe80::260:48ff:fe1f:5183** /64
----- ------- ------- ---- ------------------------- -------------- ---- ----------
* Value from DHCP
** auto_generated IPv6 address

Choose an ip from above table or enter a new ip address. New ip addresses will need
to be created manually.

Ip Address
  Enter the local management ip address to be added to this tenant-unit
  : 192.168.10.57

  Do you want to add a remote management ip to this tenant-unit? (yes|no) [no]:

Pending Management-ip Settings

Add Local Management-ip    192.168.10.57
  Do you want to save these settings (Save|Cancel|Retry): yes
  unrecognized input, expecting one of Save|Cancel|Retry

  Do you want to save these settings (Save|Cancel|Retry): save
  Local management access ip "192.168.10.57" added to tenant-unit "SMT_57_tenant_unit".

SMT Tenant-unit Management-IP Configurations saved.

SMT TENANT-UNIT MANAGEMENT-IP Configuration

  Do you want to add another local management ip to this tenant-unit? (yes|no) [no]:

  Do you want to add another remote management ip to this tenant-unit? (yes|no) [no]:

SMT TENANT-UNIT DDBOOST Configuration
  Configure SMT TENANT-UNIT DDBOOST at this time (yes|no) [no]:

SMT TENANT-UNIT MTREE Configuration
  Configure SMT TENANT-UNIT MTREE at this time (yes|no) [no]: yes

Name                       Pre-Comp (GiB)   Status   Tenant-Unit
-------------------------  --------------   ------   -----------
/data/col1/laptop_backup          4846.2   RO/RD     -
/data/col1/random                23469.9   RO/RD     -
/data/col1/software2              2003.7   RO/RD     -
/data/col1/tsm6                 763704.9   RO/RD     -
-------------------------  --------------   ------   -----------
D    : Deleted
Q    : Quota Defined
RO   : Read Only
RW   : Read Write
```

```
RD   : Replication Destination
RLGE : Retention-Lock Governance Enabled
RLGD : Retention-Lock Governance Disabled
RLCE : Retention-Lock Compliance Enabled

  Do you want to assign an existing MTree to this tenant-unit? (yes|no) [no]:

  Do you want to create a mtree for this tenant-unit now? (yes|no) [no]: yes

MTree Name
  Enter MTree name
  :  SMT_57_tenant_unit
Invalid mtree path name.
  Enter MTree name
  :
SMT_57_tenant_unit


Invalid mtree path name.
  Enter MTree name
  : /data/col1/SMT_57_tenant_unit

MTree Soft-Quota
  Enter the quota soft-limit to be set on this MTree (<n> {MiB|GiB|TiB|PiB}|none)
  :

MTree Hard-Quota
  Enter the quota hard-limit to be set on this MTree (<n> {MiB|GiB|TiB|PiB}|none)
  :

Pending MTree Settings
Create MTree        /data/col1/SMT_57_tenant_unit
MTree Soft Limit    none
MTree Hard Limit    none

  Do you want to save these settings (Save|Cancel|Retry): save
  MTree "/data/col1/SMT_57_tenant_unit" created successfully.
  MTree "/data/col1/SMT_57_tenant_unit" assigned to tenant-unit  "SMT_57_tenant_unit".

SMT Tenant-unit MTree Configurations saved.

SMT TENANT-UNIT MTREE Configuration

Name                        Pre-Comp (GiB)   Status   Tenant-Unit
-------------------------   --------------   ------   -----------
/data/col1/laptop_backup           4846.2   RO/RD     -
/data/col1/random                 23469.9   RO/RD     -
/data/col1/software2               2003.7   RO/RD     -
/data/col1/tsm6                  763704.9   RO/RD     -
-------------------------   --------------   ------   -----------
D    : Deleted
Q    : Quota Defined
RO   : Read Only
RW   : Read Write
RD   : Replication Destination
RLGE : Retention-Lock Governance Enabled
RLGD : Retention-Lock Governance Disabled
RLCE : Retention-Lock Compliance Enabled

  Do you want to assign another MTree to this tenant-unit? (yes|no) [no]: yes

  Do you want to assign an existing MTree to this tenant-unit? (yes|no) [no]:

  Do you want to create another mtree for this tenant-unit? (yes|no) [no]:

SMT TENANT-UNIT SELF-SERVICE Configuration

  Configure SMT TENANT-UNIT SELF-SERVICE at this time (yes|no) [no]: yes
  Self-service of this tenant-unit is disabled
```

```
  Do you want to enable self-service of this tenant-unit? (yes|no) [no]: yes

  Do you want to configure a management user for this tenant-unit? (yes|no) [no]:

  Do you want to configure a management group for this tenant-unit (yes|no) [no]: yes

Management-Group Name
  Enter the group name to be assigned to this tenant-unit
  : SMT_57_tenant_unit_group

What role do you want to assign to this group  (tenant-user|tenant-admin) [tenant-user]:
tenant-admin

Management-Group Type
  What type do you want to assign to this group (nis|active-directory)?
  : nis

Pending Self-Service Settings
Enable Self-Service       SMT_57_tenant_unit
Assign Management-group   SMT_57_tenant_unit_group
Management-group role     tenant-admin
Management-group type     nis

  Do you want to save these settings (Save|Cancel|Retry): save
  Tenant self-service enabled for tenant-unit "SMT_57_tenant_unit"
  Management group "SMT_57_tenant_unit_group" with type "nis" is assigned to tenant-unit
  "SMT_57_tenant_unit" as "tenant-admin".

SMT Tenant-unit Self-Service Configurations saved.

SMT TENANT-UNIT SELF-SERVICE Configuration

  Do you want to configure another management user for this tenant-unit? (yes|no) [no]:

  Do you want to configure another management group for this tenant-unit? (yes|no)
[no]:

SMT TENANT-UNIT ALERT Configuration

  Configure SMT TENANT-UNIT ALERT at this time (yes|no) [no]: yes
  No notification lists.

Alert Configuration

Alert Group Name
  Specify alert notify-list group name to be created
  : SMT_57_tenant_unit_notify

Alert email addresses
  Enter email address to receive alert for this tenant-unit
  : dd_proserv@emc.com

  Do you want to add more emails (yes/no)?
  : no

Pending Alert Settings
Create Notify-list group   SMT_57_tenant_unit_notify
Add emails                 dd_proserv@emc.com

  Do you want to save these settings (Save|Cancel|Retry): save
  Created notification list "SMT_57_tenant_unit_notify" for tenant "SMT_57_tenant_unit".
  Added emails to notification list "SMT_57_tenant_unit_notify".

SMT Tenant-unit Alert Configurations saved.

Configuration complete.
```

Aktivieren des Mandantenselfservice-Modus

Um Aufgaben administrativ voneinander zu trennen und zur Implementierung des Mandantenselfservice Administrations- und Managementaufgaben zu delegieren, kann der Systemadministrator diesen Modus für eine Mandanteneinheit aktivieren und der Einheit anschließend Benutzer mit den Rollen „tenant-admin“ oder „tenant-user“ zuweisen, die diese Einheit managen. Der Mandantenselfservice ist zur Steuerung der Pfadisolierung erforderlich. Diese Rollen ermöglichen es Benutzern, die kein Administrator sind, bestimmte Aufgaben für die Mandanteneinheit durchzuführen, der sie zugewiesen sind. Neben der administrativen Trennung trägt der Mandantenselfservice-Modus zur Reduzierung des Managementaufwands für interne IT-Mitarbeiter und Serviceprovider bei.

Vorgehensweise

1. Zeigen Sie den Status des Mandantenselfservice für eine oder alle Mandanteneinheiten an.
   ```
   # smt tenant-unit option show { tenant-unit | all }
   ```
2. Aktivieren Sie den Mandantenselfservice-Modus für die ausgewählte Mandanteneinheit.
   ```
   # smt tenant-unit option set tenant-unit self-service { enabled
   | disabled }
   ```

Datenzugriff nach Protokoll

Sichere Datenpfade mit protokollspezifischer Zugriffskontrolle ermöglichen Sicherheit und Isolierung für Mandanteneinheiten. In einer SMT-Umgebung (Secure Multitenancy) werden Befehle für das Datenzugriffsmanagement auch mit einem Mandanteneinheitsparameter erweitert, um konsolidiertes Reporting nutzen zu können.

DD-Systeme unterstützen mehrere Datenzugriffsprotokolle gleichzeitig, einschließlich DD Boost, NFS, CIFS und DD VTL. Ein DD-System kann sich einer Anwendung gegenüber als bestimmte Schnittstelle darstellen, z. B. als Dateiserver, der NFS- oder CIFS-Zugriff über Ethernet bietet, als DD-VTL-Gerät oder als DD Boost-Gerät.

Die nativen Zugriffskontrollmechanismen jedes unterstützten Protokolls ermöglichen, dass die Datenpfade für jeden Mandanten getrennt und isoliert bleiben. Derartige Mechanismen umfassen ACLs (Zugriffskontrolllisten) für CIFS, Exporte für NFS- und DD Boost-Anmeldedaten sowie eine Zugriffskontrolle, die die Boost-Anmeldedaten mehrerer Benutzer berücksichtigt.

Mehrbenutzer-DD Boost und Speichereinheiten in SMT

Bei Verwendung von Mehrbenutzer-DD Boost mit SMT (Secure Multi-Tenancy) werden Benutzerberechtigungen durch die Eigentumsrechte der Speichereinheiten bestimmt.

Der Begriff *Mehrbenutzer-DD Boost* bezieht sich auf die Verwendung von mehreren DD Boost-Benutzeranmeldedaten für die DD Boost-Zugriffskontrolle, bei der jeder Benutzer über einen eigenen Benutzernamen und ein eigenes Passwort verfügt.

Eine *Speichereinheit* ist ein MTree, der für das DD Boost-Protokoll konfiguriert ist. Ein Benutzer kann einer oder mehreren Speichereinheiten zugeordnet sein oder diese „besitzen“. Speichereinheiten, die einem Benutzer gehören, können nicht zugleich einem anderen Benutzer gehören. Daher kann nur der Benutzer, der die Speichereinheit besitzt, auf die Speichereinheit für jeden Datentypzugriff wie

beispielsweise Backup/Wiederherstellung zugreifen. Die Anzahl der DD Boost-Benutzernamen kann die maximale Anzahl von MTrees nicht überschreiten. (Im Kapitel „MTrees“ in diesem Dokument finden Sie die aktuelle maximale Anzahl an MTrees für jedes DD-Modell.) Speichereinheiten, die mit SMT verknüpft sind, muss die Rolle *none* zugewiesen sein.

Jede Backupanwendung muss mithilfe des DD Boost-Benutzernamens und -Passworts authentifiziert werden. Nach der Authentifizierung prüft DD Boost die authentifizierten Anmeldedaten, um den Besitz der Speichereinheit zu bestätigen. Der Backupanwendung wird der Zugriff auf die Speichereinheit nur dann erteilt, wenn die von der Backupanwendung vorgelegten Anmeldedaten mit den Benutzernamen übereinstimmen, die der Speichereinheit zugeordnet sind. Wenn die Benutzeranmeldedaten und die Benutzernamen nicht übereinstimmen, schlägt der Job mit einem Berechtigungsfehler fehl.

Konfigurieren des Datenzugriffs für CIFS

Das CIFS (Common Internet File System) ist ein Dateifreigabeprotokoll für den Remotedateizugriff. In einer SMT-Konfiguration (Secure Multitenancy) benötigen Backups und Wiederherstellungen Clientzugriff auf CIFS-Shares, die sich in einem MTree der zugehörigen Mandanteneinheit befinden. Die Datenisolierung wird unter Verwendung von CIFS-Shares und CIFS-ACLs erreicht.

Vorgehensweise

1. Erstellen Sie einen MTree für CIFS und weisen Sie den MTree der Mandanteneinheit zu.

   ```
   # mtree create mtree-path tenant-unit tenant-unit
   ```

2. Legen Sie die festen und variablen Kapazitäts-Quotas für den MTree fest.

   ```
   # mtree create mtree-path tenant-unit tenant-unit] [quota-soft-
   limit n{MiB|GiB|TiB|PiB} ] [quota-hard-limit n {MiB|GiB|TiB|PiB}
   ```

3. Erstellen Sie eine CIFS-Share für *pathname* über den MTree.

   ```
   # cifs share create share path pathname clients clients
   ```

Konfigurieren des NFS-Zugriffs

NFS ist ein UNIX-basiertes Dateifreigabeprotokoll für den Remotedateizugriff. In einer SMT-Umgebung (Secure Multitenancy) benötigen Backups und Wiederherstellungen Clientzugriff auf NFS-Exporte, die sich in einem MTree der zugehörigen Mandanteneinheit befinden. Die Datenisolierung wird über NFS-Exporte und eine Netzwerkisolierung erreicht. NFS bestimmt, ob ein MTree einer vom Netzwerk isolierten Mandanteneinheit zugeordnet ist. Wenn ja, überprüft NFS die Verbindungseigenschaften, die der Mandanteneinheit zugeordnet sind. Zu den Verbindungseigenschaften gehören die Ziel-IP-Adresse und die Schnittstelle oder der Clienthostname.

Vorgehensweise

1. Erstellen Sie einen MTree für NFS und weisen Sie den MTree der Mandanteneinheit zu.

   ```
   # mtree create mtree-path tenant-unit tenant-unit
   ```

2. Legen Sie die festen und variablen Kapazitäts-Quotas für den MTree fest.

   ```
   # mtree create mtree-path tenant-unit tenant-unit] [quota-soft-
   limit n{MiB|GiB|TiB|PiB} ] [quota-hard-limit n {MiB|GiB|TiB|PiB}
   ```

3. Erstellen Sie einen NFS-Export, indem Sie dem MTree mindestens einen Client hinzufügen.

```
# nfs add path client-list
```

Konfigurieren des Datenzugriffs für DD VTL

Die DD VTL-Mandantendatenisolierung wird mithilfe von DD VTL-Zugriffsgruppen erzielt, die einen virtuellen Zugriffspfad zwischen einem Hostsystem und DD VTL erstellen. (Die physische Fibre-Channel-Verbindung zwischen dem Hostsystem und DD VTL muss bereits vorhanden sein.)

Durch die Platzierung von Bändern in der DD VTL können diese in die Backupanwendung auf dem Hostsystem geschrieben und von dieser gelesen werden. DD VTL-Bänder werden in einem DD VTL-Pool erstellt, der ein MTree ist. Da DD VTL-Pools MTrees sind, können sie Mandanteneinheiten zugewiesen werden. Diese Zuweisung ermöglicht das SMT-Monitoring und -Reporting.

Wenn beispielsweise einem Mandantenadministrator eine Mandanteneinheit zugewiesen wird, die einen DD VTL-Pool enthält, kann er MTree-Befehle ausführen, um schreibgeschützte Informationen anzuzeigen. Befehle können nur in dem DD VTL-Pool ausgeführt werden, der der Mandanteneinheit zugewiesen ist.

Zu diesen Befehlen gehören:

- `mtree list` zum Anzeigen einer Liste der MTrees in der Mandanteneinheit
- `mtree show compression` zum Anzeigen von Statistiken zur MTree-Komprimierung
- `mtree show performance` zum Anzeigen von Statistiken zur Performance

Die Ausgabe der meisten `list`- und `show`-Befehle beinhaltet Statistiken, mit denen Serviceprovider die Speicherplatznutzung messen und Chargeback-Gebühren berechnen können.

DD VTL-Vorgänge sind davon nicht betroffen und funktionieren weiterhin normal.

Verwenden von DD VTL-NDMP-TapeServer

Die Isolierung von DD VTL-Mandantendaten wird auch mithilfe von NDMP erzielt. DD OS implementiert einen NDMP-Bandserver (Network Data Management Protocol), mit dem NDMP-fähige Systeme über ein Dreiwege-NDMP-Backup Backupdaten an das DD-System senden können.

Die Backupdaten werden von einer DD VTL, die der speziellen DD VTL-Gruppe *TapeServer* zugewiesen ist, auf virtuelle Bänder geschrieben, die sich in einem Pool befinden.

Da die Backupdaten auf Bänder in einem Pool geschrieben werden, gelten die Informationen im DD VTL-Thema bezüglich MTrees auch für den NDMP-TapeServer von Data Domain.

Datenmanagementvorgänge

Zu den SMT-Managementvorgängen (Secure Multitenancy) zählen das Monitoring von Mandanteneinheiten und anderen Objekten wie Speichereinheiten und MTrees. Bei einigen SMT-Objekten ist möglicherweise auch eine zusätzliche Konfiguration oder Änderung erforderlich.

Erfassen von Statistiken zur Performance

Jeder MTree kann auf Statistiken und andere Echtzeitinformationen zur Performance oder „Nutzung“ gemessen werden. Historische Auslastungsraten sind für DD Boost-

Speichereinheiten verfügbar. Die Befehlsausgabe ermöglicht dem Mandantenadministrator die Erfassung von Nutzungsstatistiken und Komprimierungsverhältnissen für einer Mandanteneinheit zugewiesene MTrees oder für alle MTrees und zugehörigen Mandanteneinheiten. Die Ausgabe kann gefiltert werden, um die Nutzung in Intervallen von wenigen Minuten bis zu Monaten anzuzeigen. Die Ergebnisse werden an den Administrator weitergeleitet, der die Statistiken als Chargeback-Metriken verwendet. Eine ähnliche Methode wird verwendet, um die Nutzungsstatistiken und Komprimierungsverhältnisse für Speichereinheiten zu erfassen.

Vorgehensweise

1. Erfassen Sie die MTree-Performancestatistiken in Echtzeit.
   ```
   # mtree show stats
   ```
2. Erfassen Sie die Performancestatistiken für MTrees, die einer Mandanteneinheit zugewiesen sind.
   ```
   # mtree show performance
   ```
3. Erfassen Sie die Komprimierungsstatistiken für MTrees, die einer Mandanteneinheit zugewiesen sind.
   ```
   # mtree show compression
   ```

Ändern von Quotas

Um QoS-Kriterien zu erfüllen, kann ein Systemadministrator mithilfe von DD OS-„Knobs“ die von der Mandantenkonfiguration erforderlichen Einstellungen anpassen. Beispiel: Der Administrator kann „feste“ und „variable“ Quota-Limits für DD Boost-Speichereinheiten festlegen. Der Stream von „variablen“ und „festen“ Quota-Limits kann nur DD Boost-Speichereinheiten zugewiesen werden, die Mandanteneinheiten zugewiesen wurden. Nachdem der Administrator die Quotas festgelegt hat, kann der Mandantenadministrator eine oder alle Mandanteneinheiten überwachen, damit kein Objekt die zugewiesenen Quotas überschreitet und fremde Systemressourcen nutzt.

Quotas werden anfänglich nach Aufforderung durch den Konfigurationsassistenten festgelegt, können aber später angepasst werden. Im folgenden Beispiel wird das Ändern der Quotas für DD Boost beschrieben. (Sie können sowohl `quota capacity` als auch `quota streams` verwenden, um Probleme bei der Kapazität, Stream-Quotas und Limits zu handhaben).

Vorgehensweise

1. So ändern Sie die festen und variablen Quota-Limits für DD Boost-Speichereinheit „su33“:
   ```
   ddboost storage-unit modify su33 quota-soft-limit 10 Gib quota-hard-limit 20 Gib
   ```
2. So ändern Sie die festen und variablen Stream-Quota-Limits für DD Boost-Speichereinheit „su33“:
   ```
   ddboost storage-unit modify su33 write-stream-soft-limit 20 read-stream-soft-limit 6 repl -stream-soft-limit 20 combined-stream-soft-limit 20
   ```
3. So melden Sie die physische Größe für DD Boost-Speichereinheit „su33“:
   ```
   ddboost storage-unit modify su33 report-physical-size 8 GiB
   ```

SMT und Replikation

Bei einem Notfall geben Benutzerrollen vor, wie ein Benutzer Daten-Recovery-Vorgänge unterstützen kann. In einer SMT-Konfiguration sind verschiedene

Replikationstypen verfügbar. (Ausführliche Informationen zum Durchführen der Replikation finden Sie im Kapitel *DD Replicator*.)

Hier sind einige Punkte, die Sie in Bezug auf Benutzerrollen berücksichtigen sollten:

- Der Administrator kann MTrees aus einer replizierten Kopie wiederherstellen.
- Der Mandantenadministrator kann MTrees mithilfe von DD Boost MFR (Managed File Replication) von einem System zu einem anderen replizieren.
- Der Mandantenadministrator kann MTrees ebenfalls mithilfe von DD Boost MFR aus einer replizierten Kopie wiederherstellen.

Sammelreplikation
Bei der Sammelreplikation werden Konfigurationsinformationen für die Kernmandanteneinheit repliziert.

Sichere Replikation über das öffentliche Internet
Um Schutz vor Man-in-the-Middle-Angriffen (MITM) bei der Replikation über eine öffentliche Internetverbindung zu bieten, umfasst die Authentifizierung die Validierung von SSL-Zertifikat-bezogenen Informationen für Replikationsquelle und -ziel.

MTree-Replikation (NFS/CIFS) mit DD Boost MFR
Die MTree-Replikation wird mithilfe von DD Boost MFR auf MTrees unterstützt, die Mandanteneinheiten zugewiesen sind. Während der MTree-Replikation kann ein MTree, der einer Mandanteneinheit auf einem System zugewiesen ist, an einen MTree repliziert werden, der einer Mandanteneinheit auf einem anderen System zugewiesen ist. Die MTree-Replikation zwischen zwei verschiedenen Mandanten auf den beiden DD-Systemen ist nicht zulässig. Wenn der Sicherheitsmodus auf *strict* festgelegt ist, ist die MTree-Replikation nur zulässig, wenn die MTrees zu denselben Mandanten gehören.

Aus Gründen der Abwärtskompatibilität wird die MTree-Replikation von einem MTree, der einer Mandanteneinheit auf einem nicht zugewiesenen MTree zugewiesen ist, unterstützt, muss aber manuell konfiguriert werden. Eine manuelle Konfiguration stellt sicher, dass der Ziel-MTree über die richtigen Einstellungen für die Mandanteneinheit verfügt. Umgekehrt wird auch die MTree-Replikation von einem nicht zugewiesenen MTree zu einem MTree unterstützt, der einer Mandanteneinheit zugewiesen ist.

Beim Einrichten der SMT-fähigen MTree-Replikation definiert *security mode*, in welchem Umfang auf dem Mandanten geprüft wird. Der Modus *default* prüft, ob Quelle und Ziel nicht zu anderen Mandanten gehören. Der Modus *strict* sorgt dafür, dass Quelle und Ziel zu demselben Mandanten gehören. Wenn Sie den Modus „strict“ verwenden, müssen Sie daher einen Mandanten auf dem Zielrechner mit der UUID erstellen, die für den Mandanten auf der Quellmaschine verwendet wird, die mit dem replizierten MTree verknüpft ist.

DD Boost MFR (auch mit DD Boost AIR)
DD Boost MFR wird zwischen Speichereinheiten unterstützt, unabhängig davon, ob eine Speichereinheit oder beide Mandanteneinheiten zugewiesen sind.

Bei DD Boost MFR werden Speichereinheiten nicht in ihrer Gesamtheit repliziert. Stattdessen werden bestimmte Dateien innerhalb einer Speichereinheit von der Backupanwendung für die Replikation ausgewählt. Die Dateien, die in einer Speichereinheit ausgewählt wurden und einer Mandanteneinheit auf einem System zugewiesen sind, können an eine Speichereinheit repliziert werden, die einer Mandanteneinheit auf einem anderen System zugewiesen ist.

Aus Gründen der Abwärtskompatibilität können ausgewählte Dateien in einer Speichereinheit, die einer Mandanteneinheit zugewiesen ist, an eine nicht zugewiesene Speichereinheit repliziert werden. Umgekehrt können ausgewählte

Dateien in einer nicht zugewiesenen Speichereinheit an eine Speichereinheit repliziert werden, die einer Mandanteneinheit zugewiesen ist.

DD Boost MFR kann auch in DD Boost AIR-Bereitstellungen verwendet werden.

Replikationskontrolle für QoS
Eine Obergrenze für den Replikationsdurchsatz (`repl-in`) kann für einen MTree angegeben werden. Da MTrees für jeden Mandanten einer Mandanteneinheit zugewiesen werden, kann die Replikationsressourcennutzung jedes Mandanten durch die Anwendung dieser Grenzwerte begrenzt werden. Die Beziehung dieser Funktion zu SMT ist, dass diese MTree-Replikation dem Durchsatzgrenzwert unterliegt.

SMT-Mandantenwarnmeldungen

Ein DD-System erzeugt *Events*, wenn es auf potenzielle Probleme mit der Software oder Hardware trifft. Wenn ein Event erzeugt wird, wird sofort eine *Warnmeldung* per E-Mail an die Mitglieder der Benachrichtigungsliste sowie an den Data Domain-Administrator gesendet.

SMT-Warnmeldungen sind für jede Mandanteneinheit spezifisch und unterscheiden sich von DD-Systemwarnmeldungen. Wenn der Mandantenselfservice-Modus aktiviert ist, kann der Mandantenadministrator Warnmeldungen wahlweise über die unterschiedlichen Systemobjekte erhalten oder allen wichtigen Events wie einem unerwarteten Herunterfahren des Systems zugeordnet sein. Ein Mandantenadministrator kann nur Benachrichtigungslisten anzeigen oder ändern, denen er zugeordnet ist.

Im Folgenden sehen Sie ein Beispiel für eine Warnmeldung. Beachten Sie, dass die beiden Eventmeldungen unten in der Benachrichtigung für eine Umgebung mit mehreren Mandanten spezifisch sind (wird durch das Wort „Tenant“ angegeben). Die gesamte Liste der DD OS- und SMT-Warnmeldungen finden Sie im *Data Domain MIB Quick Reference Guide* oder in der SNMP-MIB.

```
EVT-ENVIRONMENT-00021 – Description: The system has been shutdown by
abnormal method; for example, not by one of the following: 1) Via
IPMI chassis control command 2) Via power button 3) Via OS shutdown.

Action: This alert is expected after loss of AC (main power) event.
If this shutdown is not expected and persists, contact your
contracted support provider or visit us online at https://
my.datadomain.com.

Tenant description: The system has experienced an unexpected power
loss and has restarted.

Tenant action: This alert is generated when the system restarts after
a power loss. If this alert repeats, contact your System
Administrator.
```

Managen von Snapshots

Ein *Snapshot* ist eine schreibgeschützte Kopie eines an einem bestimmten Point-in-Time erfassten MTree. Ein Snapshot kann für viele Zwecke verwendet werden, beispielsweise als Wiederherstellungspunkt im Fall einer Fehlfunktion des Systems. Die erforderliche Rolle für die Verwendung von `snapshot` ist admin oder tenantadmin.

So zeigen Sie Snapshot-Informationen für einen MTree oder eine Mandanteneinheit an:

```
# snapshot list mtree mtree-path | tenant-unit tenant-unit
```

So zeigen Sie eine Snapshot-Planung für einen MTree oder eine Mandanteneinheit an:

```
# snapshot schedule show [name | mtrees mtree-listmtree-list | tenant-unit tenant-unit]
```

Durchführen einer FastCopy für ein Dateisystem

Mit einem FastCopy-Vorgang werden Dateien und Verzeichnisstrukturen eines Quellverzeichnisses in ein Zielverzeichnis auf einem DD-System kopiert. Ein FastCopy-Vorgang mit SMT (Secure Multitenancy) unterliegt besonderen Bedingungen.

Beachten Sie beim Durchführen eines FastCopy-Vorgangs für ein Dateisystem mit aktiviertem Mandantenselfservice-Modus die folgenden Überlegungen:

- Ein Mandantenadministrator kann Dateien per FastCopy aus einer Mandanteneinheit in eine andere kopieren, wenn der Mandantenadministrator für beide betroffenen Mandanteneinheiten Mandantenadministrator ist und die beiden Mandanteneinheiten demselben Mandanten angehören.
- Ein Mandantenadministrator kann Dateien per FastCopy innerhalb derselben Mandanteneinheit kopieren.
- Ein Mandantenadministrator kann Dateien per FastCopy innerhalb der Mandanteneinheiten an Quelle und Ziel kopieren.

So führen Sie eine Dateisystem-FastCopy aus:

```
# filesys fastcopy source <src> destination <dest>
```

KAPITEL 18

DD Cloud Tier

Inhalt dieses Kapitels:

DD Cloud Tier – Übersicht

DD Cloud Tier ist eine native Funktion von DD OS 6.0 (oder höher) zum Verschieben von Daten vom aktiven Tier in kostengünstigen Objektspeicher mit hoher Kapazität in der Public, Private oder Hybrid Cloud zur langfristigen Aufbewahrung. DD Cloud Tier ist am besten geeignet für die langfristige Speicherung von selten abgerufenen Daten, die aus Gründen von Compliance, behördlichen Auflagen und Governance gespeichert werden. Ideale Daten für DD Cloud Tier sind Daten, die außerhalb des normalen Recovery-Fensters liegen.

DD Cloud Tier wird mit einem einzigen Data Domain-Namespace verwaltet. Es ist kein separates Cloudgateway bzw. keine virtuelle Appliance erforderlich. Die Datenverschiebung wird durch das native Data Domain-Policy-Managementframework unterstützt. Der Cloudspeicher wird als zusätzlicher mit dem Data Domain-System verbundenener Storage Tier (DD Cloud Tier) behandelt und Daten werden nach Bedarf zwischen Tiers verschoben. Dateisystem-Metadaten, die in der Cloud gespeicherten Daten zugeordnet sind, werden im lokalen Speicher verwaltet und ebenfalls auf die Cloud gespiegelt. Die Metadaten im lokalen Speicher erleichtern die Vorgänge wie Deduplizierung, Bereinigung, Fast Copy und Replikation. Dieser lokale Speicher ist für vereinfachte Verwaltbarkeit in unabhängige Buckets, sogenannte Cloudeinheiten, unterteilt.

Unterstützte Plattformen

Cloud-Tier wird auf physischen Plattformen unterstützt, die über den erforderlichen Arbeitsspeicher, die erforderliche CPU und die erforderliche Speicherkonnektivität verfügen, um einen anderen Speicher-Tier zu berücksichtigen.

DD Cloud-Tier wird auf diesen Systemen unterstützt:

Tabelle 190 Von DD Cloud-Tier unterstützte Konfigurationen

Modell	Arbeitsspeicher	Cloudkapazität	Erforderliche Anzahl von SAS-I/O-Modulen	Unterstützte Datenträgereinschub-Typen für Metadatenspeicher	Anzahl der erforderlichen ES30-Einschübe oder DS60-Spindeln	Erforderliche Kapazität für Metadatenspeicher
DD990	256 GB	1140 TB	4	ES30	4	60 x 3 TB HDDs = 180 TB
DD3300 4 TB	16 GB	8 TB	–	–	–	1 x 1 Tb großes virtuelles Laufwerk = 1 TB
DDD3300 16 TB	48 GB	32 TB	–	–	–	2 x 1 TB große virtuelle Laufwerke = 2 TB
DD3300 32 TB	64 GB	64 TB	–	–	–	4 x 1 TB große virtuelle Laufwerke = 4 TB

Tabelle 190 Von DD Cloud-Tier unterstützte Konfigurationen (Fortsetzung)

Modell	Arbeitsspeicher	Cloudkapazität	Erforderliche Anzahl von SAS-I/O-Modulen	Unterstützte Datenträgereinschub-Typen für Metadatenspeicher	Anzahl der erforderlichen ES30-Einschübe oder DS60-Spindeln	Erforderliche Kapazität für Metadatenspeicher
DD4200	128 GB	378 TB	3	DS60 oder ES30	2	30 x 3 TB HDDs = 90 TB
DD4500	192 GB	570 TB	3	DS60 oder ES30	2	30 x 4 TB HDDs = 120 TB
DD6800	192 GB	576 TB	2	DS60 oder ES30	2	30 x 4 TB HDDs = 120 TB
DD7200	256 GB	856 TB	4	DS60 oder ES30	4	60 x 4 TB HDDs = 240 TB
DD9300	384 GB	1400 TB	2	DS60 oder ES30	4	60 x 4 TB HDDs = 240 TB
DD9500	512 GB	1728 TB	4	DS60 oder ES30	5	75 x 4 TB HDDs = 300 TB
DD9800	768 GB	2016 TB	4	DS60 oder ES30	5	75 x 4 TB HDDs = 300 TB
DD VE 16 TB	32 GB	32 TB	–	–	–	1 x 500 GB großes virtuelles Laufwerk = 500 GB[a]
DD VE 64 TB	60 GB	128 TB	–	–	–	1 x 500 GB großes virtuelles Laufwerk = 500 GB[a]
DD VE 96 TB	80 GB	192 TB	–	–	–	1 x 500 GB großes virtuelles Laufwerk = 500 GB[a]

a. Die minimale Metadatengröße ist ein fester Grenzwert. Data Domain empfiehlt Benutzern, mit 1 TB für Metadatenspeicher zu beginnen und in Schritten von 1 TB zu erweitern. Im *Data Domain Virtual Edition Installation and Administration Guide* finden Sie weitere Informationen zur Verwendung von DD Cloud-Tier mit DD VE.

Hinweis

DD Cloud-Tier wird in einer Umgebung mit hoher Data Domain-Verfügbarkeit (HA, High Availability) unterstützt. Beide Nodes müssen auf DD OS 6.0 (oder höher) ausgeführt werden und sie müssen für HA aktiviert sein.

Hinweis

DD Cloud-Tier wird auf keinem der nicht aufgeführten Systeme und auf keinem System mit aktivierter Extended Retention-Funktion unterstützt.

Hinweis

Die Cloud-Tier-Funktion kann die gesamte verfügbare Bandbreite in einem gemeinsam genutzten WAN-Link verbrauchen, insbesondere in einer Konfiguration mit niedriger Bandbreite (1 Gbit/s), und dies kann sich auf andere Anwendungen auswirken, die die WAN-Verbindung gemeinsam nutzen. Wenn gemeinsam genutzte Anwendungen auf dem WAN vorhanden sind, wird die Verwendung von QoS oder anderer Netzwerkeinschränkungen empfohlen, um Überlastungen zu vermeiden und eine konsistente Performance über eine längere Zeit zu gewährleisten.
Wenn die Bandbreite beschränkt ist, werden die Daten langsamer verschoben und Sie können nicht so viele Daten in die Cloud verschieben. Es wird empfohlen, eine dedizierte Verbindung für Daten zum Cloud-Tier zu verwenden.

Hinweis

Senden Sie keinen Datenverkehr über integrierte Managementnetzwerkschnittstellen-Controller (ethMx-Schnittstellen).

DD Cloud Tier-Performance

Das Data Domain-System verwendet interne Optimierungen zur Maximierung der DD Cloud Tier-Performance.

Große Objektgröße
DD Cloud Tier verwendet Objektgrößen von 1 MB oder 4 MB (je nach Cloudspeicheranbieter), um den Metadaten-Overhead zu reduzieren und die Anzahl der Objekte für die Migration zum Cloudspeicher zu senken.

Konfigurieren von Cloud-Tier

Um Cloud-Tier zu konfigurieren, fügen Sie die Lizenz und die Gehäuse hinzu, legen Sie eine Systempassphrase fest und erstellen Sie ein Dateisystem mit Unterstützung für die Datenverschiebung in die Cloud.

- Für Cloud-Tier ist die Cloudkapazitätslizenz erforderlich.
- Aktuelle Informationen zu Produktfunktionen, Softwareupdates, Kompatibilitätsleitfäden für Software und Informationen zu Produkten, Lizenzierung und Service von Data Domain finden Sie in den entsprechenden *Data Domain Operating System Release Notes*, um Cloud-Tier zu lizenzieren.
- Um eine Systempassphrase festzulegen, verwenden Sie die Registerkarte **Administration** > **Access** > **Administrator Access**.
  Wenn keine System-Passphrase festgelegt wurde, wird im Bereich Passphrase die Schaltfläche **Set Passphrase** angezeigt. Wenn eine System-Passphrase konfiguriert wurde, wird die Schaltfläche **Change Passphrase** angezeigt, und Sie haben nur die Möglichkeit, die Passphrase zu ändern.
- Verwenden Sie zum Konfigurieren von Speicher die Registerkarte **Hardware** > **Storage**.

- Um ein Dateisystem zu erstellen, verwenden Sie den File System Create Wizard.

Konfigurieren von Speicher für DD Cloud-Tier

Auf dem DD-System ist Cloud-Tier-Speicher für die Cloudeinheiten erforderlich – er enthält die Metadaten für die Dateien, während sich die Daten in der Cloud befinden.

Vorgehensweise

1. Wählen Sie **Hardware** > **Storage** aus.
2. Erweitern Sie in der Registerkarte „Overview“ die Option **Cloud Tier**.
3. Klicken Sie auf **Configure**.

   Das Dialogfeld „Configure Cloud Tier“ wird angezeigt.
4. Aktivieren Sie das Kontrollkästchen für den Einschub, der über den Abschnitt „Addable Storage“ hinzugefügt werden soll.

   ⚠ ACHTUNG

   DD3300-Systeme erfordern die Verwendung von 1-TB-Speichergeräten für DD Cloud-Tier-Metadatenspeicher.
5. Klicken Sie auf die Schaltfläche **Add to Tier**.
6. Klicken Sie auf **Save**, um den Speicher hinzuzufügen.
7. Wählen Sie **Data Management** > **File System** und aktivieren Sie die Cloud-Tier-Funktion.
8. Klicken Sie auf **Disable** (am unteren Bildschirmrand), um das Dateisystem zu deaktivieren.
9. Klicken Sie auf **OK**.
10. Nachdem das Dateisystem deaktiviert wurde, wählen Sie **Enable Cloud Tier** aus.

    Um den Cloud-Tier zu aktivieren, müssen Sie die Speicheranforderungen für die lizenzierte Kapazität erfüllen. Konfigurieren Sie den Cloud-Tier des Dateisystems. Klicken Sie auf **Next**.
    Ein Clouddateisystem erfordert einen lokalen Speicher für eine lokale Kopie der Cloudmetadaten.
11. Wählen Sie **Enable file system** aus.

    Der Cloud-Tier wird mit dem festgelegten Speicher aktiviert.
12. Klicken Sie auf **OK**.

    Sie müssen Cloudeinheiten separat erstellen, nachdem das Dateisystem erstellt wurde.

Konfigurieren von Cloudeinheiten

Der Cloud-Tier besteht aus bis zu zwei Cloudeinheiten und jede Cloudeinheit ist einem Cloudanbieter zugeordnet, sodass mehrere Cloudanbieter pro Data Domain-System zugeordnet werden können. Das Data Domain-System muss mit der Cloud verbunden sein und über ein Konto bei einem unterstützten Cloudanbieter verfügen.

Das Konfigurieren von Cloudeinheiten beinhaltet die folgenden Schritte:

- Konfigurieren des Netzwerks, einschließlich Firewall- und Proxyeinstellungen
- Importieren von CA-Zertifikaten
- Hinzufügen von Cloudeinheiten

Einstellungen der Firewall und des Proxy

- Netzwerkfirewallports
  - Port 443 (HTTPS) und/oder Port 80 (HTTP) müssen auf die Cloudanbieternetzwerke für die Endpunkt-IP-Adresse und die Anbieterauthentifizierungs-IP-Adresse für einen bidirektionalen Datenverkehr offen sein.
    Für Amazon S3 müssen beispielsweise sowohl für s3-ap-southeast-1.amazonaws.com als auch für s3.amazonaws.com Port 80 und/oder Port 443 offen und so eingestellt sein, dass sie bidirektionalen IP-Datenverkehr zulassen.

    Hinweis

    Verschiedene Public-Cloud-Anbieter verwenden IP-Bereiche für ihre Endpunkt- und Authentifizierungsadressen. In diesem Fall müssen die vom Anbieter verwendeten IP-Bereiche entsperrt werden, um potenzielle IP-Änderungen zu berücksichtigen.
  - Remotecloudanbieter-Ziel-IP- und Zugriffsauthentifizierungs-IP-Adressbereiche müssen durch die Firewall zugelassen werden.
  - Für ECS Private Cloud müssen lokale ECS-Authentifizierungs- und Webspeicherzugriffs-IP-Adressbereiche (S3) und die Ports 9020 (HTTP) und 9021 (HTTPS) durch lokale Firewalls zugelassen werden.

    Hinweis

    ECS Private Cloud-Load Balancer-IP-Zugriff und -Portregeln müssen ebenfalls konfiguriert werden.
- Proxyeinstellungen
  - Ändern Sie alle möglicherweise vorhandenen Proxyeinstellungen, die dazu führen, dass Daten über einer bestimmten Größe zurückgewiesen werden, um Objektgrößen bis zu 4,5 MB zu ermöglichen.
  - Wenn Kundendatenverkehr über einen Proxy weitergeleitet wird, muss das selbstsignierte/CA-signierte Proxyzertifikat importiert werden. Weitere Informationen finden Sie unter „Importieren von CA-Zertifikaten“.
- OpenSSL-Cipher-Suites
  - Verschlüsselungsverfahren – ECDHE-RSA-AES256-SHA384 AES256-GCM-SHA384

    Hinweis

    Standardkommunikation mit allen Cloudanbietern wird mit einem starken Verschlüsselungsverfahren initiiert.
  - TLS-Version: 1.2
- Unterstützte Protokolle
  - HTTP und HTTPS

Hinweis

Standardkommunikation mit allen Public-Cloud-Anbietern erfolgt auf sicherem HTTP (HTTPS), Sie können die Standardeinstellung jedoch überschreiben, um HTTP zu verwenden.

Importieren von CA-Zertifikaten

Bevor Sie Cloudeinheiten für Elastic Cloud Storage (ECS), Virtustream Storage Cloud, Amazon Web Services S3 (AWS) und Azure Cloud hinzufügen können, müssen Sie CA-Zertifikate importieren.

Bevor Sie beginnen

Für die Public-Cloud-Anbieter AWS, Virtustream und Azure können Root-CA-Zertifikate von https://www.digicert.com/digicert-root-certificates.htm heruntergeladen werden.

- Laden Sie für den Cloudanbieter AWS das Zertifikat Baltimore CyberTrust Root herunter.
- Laden Sie für den Cloudanbieter Virtustream das CA-Zertifikat DigiCert High Assurance EV Root herunter.
- Für ECS variiert die Stammzertifizierungsstelle je nach Kunde.
  Die Implementierung von Cloudspeicher auf ECS erfordert einen Load Balancer. Wenn ein HTTPS-Endpunkt als Endpunkt in der Konfiguration verwendet wird, achten Sie darauf, dass Sie das Stammzertifikat der CA importieren. Weitere Informationen erhalten Sie von Ihrem Load Balancer-Anbieter.
- Laden Sie für den Cloudanbieter Azure das Zertifikat Baltimore CyberTrust Root herunter.
- Importieren Sie das Stammzertifikat der CA für einen S3 Flexible-Anbieter.
  Wenden Sie sich an Ihren S3 Flexible-Anbieter, um Details zu erhalten.

Wenn Ihr heruntergeladenes Zertifikat die Erweiterung .crt hat, muss es wahrscheinlich in ein PEM-kodiertes Zertifikat konvertiert werden. Wenn dies der Fall ist, verwenden Sie OpenSSL, um die Datei aus dem .crt-Format in das .pem.-Format zu konvertieren (z. B. `openssl x509 -inform der -in BaltimoreCyberTrustRoot.crt -out BaltimoreCyberTrustRoot.pem`).

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Cloud Units**.
2. Klicken Sie in der Symbolleiste auf **Manage Certificates**.

   Das Dialogfeld „Manage Certificates for Cloud“ wird angezeigt.
3. Klicken Sie auf **Add**.
4. Wählen Sie eine der folgenden Optionen:
   - **I want to upload the certificate as a .pem file.**
     Navigieren Sie zur Zertifikatsdatei und wählen Sie sie aus.
   - **I want to copy and paste the certificate text.**
     - Kopieren Sie den Inhalt der .pem-Datei in Ihre Zwischenablage.
     - Fügen Sie den Inhalt der Zwischenablage in das Dialogfeld ein.
5. Klicken Sie auf **Add**.

Hinzufügen einer Cloudeinheit für Elastic Cloud Storage (ECS)

Ein Data Domain-System oder eine DD VE-Instanz erfordert eine enge zeitliche Synchronisation mit dem ECS-System, um eine Data Domain-Cloudeinheit zu konfigurieren. Durch das Konfigurieren von NTP auf dem Data Domain-System oder der DD VE-Instanz löst das ECS-System dieses Problem.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Cloud Units**.
2. Klicken Sie auf **Add**.

   Das Dialogfeld „Add Cloud Unit“ wird angezeigt.
3. Geben Sie einen Namen für diese Cloudeinheit ein. Es sind nur alphanumerische Zeichen zulässig.

   Die übrigen Felder im Dialogfeld „Add Cloud Unit“ beziehen sich auf das Cloudanbieterkonto.
4. Wählen Sie für **Cloud provider** die Option **EMC Elastic Cloud Storage (ECS)** aus der Drop-down-Liste aus.
5. Geben Sie den **Access key** des Anbieters als Passworttext ein.
6. Geben Sie den **Secret key** des Anbieters als Passworttext ein.
7. Geben Sie den **Endpoint** des Anbieters im folgenden Format ein: `http://<ip/hostname>:<port>`. Wenn Sie einen sicheren Endpunkt verwenden, verwenden Sie stattdessen `https`.

   Hinweis

   Die Implementierung von Cloudspeicher auf ECS erfordert einen Load Balancer.

   Standardmäßig führt ECS das S3-Protokoll auf Port 9020 für HTTP und auf Port 9021 für HTTPS aus. Wenn ein Load Balancer verwendet wird, werden diese Ports manchmal auf 80 für HTTP bzw. auf 443 für HTTPS neu zugeordnet. Wenden Sie sich an Ihren Netzwerkadministrator, um die richtigen Ports zu finden.
8. Wenn ein HTTP-Proxyserver erforderlich ist, um eine Firewall für diesen Anbieter zu umgehen, klicken Sie auf **Configure** für **HTTP Proxy Server**.

   Geben Sie den Hostnamen, den Port, den Benutzer und das Passwort für den Proxyserver ein.
9. Klicken Sie auf **Add**.

   Das Hauptfenster des Dateisystems zeigt nun zusammenfassende Informationen für die neue Cloudeinheit sowie ein Steuerelement zum Aktivieren und Deaktivieren der Cloudeinheit an.

Hinzufügen einer Cloudeinheit für Virtustream

Virtustream bietet eine Reihe von Speicherklassen. Die *Cloud Providers Compatibility Matrix*, die auf der Seite der Data Protection Community unter https://inside.dell.com/community/active/data-protection verfügbar ist, bietet die meisten aktuellen Informationen zu den unterstützten Speicherklassen.

Die folgenden Endpunkte werden vom Virtustream-Cloudanbieter je nach Speicherklasse und -region verwendet. Achten Sie darauf, dass DNS diesen Hostnamen vor der Konfiguration von Cloudeinheiten auflösen kann.

- s-us.objectstorage.io
- s-eu.objectstorage.io
- s-eu-west-1.objectstorage.io
- s-eu-west-2.objectstorage.io
- s-us-central-1.objectstorage.io

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Cloud Units**.
2. Klicken Sie auf **Add**.

   Das Dialogfeld „Add Cloud Unit“ wird angezeigt.
3. Geben Sie einen Namen für diese Cloudeinheit ein. Es sind nur alphanumerische Zeichen zulässig.

   Die übrigen Felder im Dialogfeld „Add Cloud Unit“ beziehen sich auf das Cloudanbieterkonto.
4. Wählen Sie für **Cloud provider** die Option **Virtustream Storage Cloud** aus der Drop-down-Liste aus.
5. Wählen Sie in der Drop-down-Liste die Speicherklasse aus.
6. Wählen Sie den entsprechenden Bereich, der dem Typ Ihres Kontos entspricht, aus der Drop-down-Liste aus.
7. Geben Sie den **Access key** des Anbieters als Passworttext ein.
8. Geben Sie den **Secret key** des Anbieters als Passworttext ein.
9. Wenn ein HTTP-Proxyserver erforderlich ist, um eine Firewall für diesen Anbieter zu umgehen, klicken Sie auf **Configure** für **HTTP Proxy Server**.

   Geben Sie den Hostnamen, den Port, den Benutzer und das Passwort für den Proxyserver ein.
10. Klicken Sie auf **Save**.

    Das Hauptfenster des Dateisystems zeigt nun zusammenfassende Informationen für die neue Cloudeinheit sowie ein Steuerelement zum Aktivieren und Deaktivieren der Cloudeinheit an.

Hinzufügen einer Cloudeinheit für Amazon Web Services S3

AWS bietet eine Reihe von Speicherklassen. Die *Cloud Providers Compatibility Matrix*, die auf der Seite der Data Protection Community unter https://inside.dell.com/community/active/data-protection verfügbar ist, bietet die meisten aktuellen Informationen zu den unterstützten Speicherklassen.

Für noch mehr Sicherheit verwendet die Cloud-Tier-Funktion Signature Version 4 für alle AWS-Anfragen. Signature Version 4-Signierung ist standardmäßig aktiviert.

Die folgenden Endpunkte werden vom AWS-Cloudanbieter je nach Speicherklasse und -region verwendet. Achten Sie darauf, dass DNS diesen Hostnamen vor der Konfiguration von Cloudeinheiten auflösen kann.

- s3.amazonaws.com

- s3-us-west-1.amazonaws.com
- s3-us-west-2.amazonaws.com
- s3-eu-west-1.amazonaws.com
- s3-ap-northeast-1.amazonaws.com
- s3-ap-southeast-1.amazonaws.com
- s3-ap-southeast-2.amazonaws.com
- s3-sa-east-1.amazonaws.com
- ap-south-1
- ap-northeast-2
- eu-central-1

Hinweis

China wird nicht unterstützt.

Hinweis

Die AWS-Benutzeranmeldedaten müssen über Berechtigungen zum Erstellen und Löschen von Buckets und zum Hinzufügen, Ändern und Löschen von Dateien in den Buckets verfügen, die sie erstellen. S3FullAccess wird bevorzugt, aber dies sind die Mindestanforderungen:

- CreateBucket
- ListBucket
- DeleteBucket
- ListAllMyBuckets
- GetObject
- PutObject
- DeleteObject

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Cloud Units**.
2. Klicken Sie auf **Add**.

   Das Dialogfeld „Add Cloud Unit“ wird angezeigt.
3. Geben Sie einen Namen für diese Cloudeinheit ein. Es sind nur alphanumerische Zeichen zulässig.

   Die übrigen Felder im Dialogfeld „Add Cloud Unit“ beziehen sich auf das Cloudanbieterkonto.
4. Wählen Sie für **Cloud provider** in der Drop-down-Liste die Option **Amazon Web Services S3** aus.
5. Wählen Sie in der Drop-down-Liste die Speicherklasse aus.
6. Wählen Sie die jeweilige **Storage region** aus der Drop-down-Liste aus.
7. Geben Sie den **Access key** des Anbieters als Passworttext ein.
8. Geben Sie den **Secret key** des Anbieters als Passworttext ein.

9. Stellen Sie sicher, dass Port 443 (HTTPS) nicht in Firewalls blockiert wird. Die Kommunikation mit dem AWS-Cloudanbieter erfolgt auf Port 443.
10. Wenn ein HTTP-Proxyserver erforderlich ist, um eine Firewall für diesen Anbieter zu umgehen, klicken Sie auf **Configure** für **HTTP Proxy Server**.

    Geben Sie den Hostnamen, den Port, den Benutzer und das Passwort für den Proxyserver ein.
11. Klicken Sie auf **Add**.

    Das Hauptfenster des Dateisystems zeigt nun zusammenfassende Informationen für die neue Cloudeinheit sowie ein Steuerelement zum Aktivieren und Deaktivieren der Cloudeinheit an.

Hinzufügen einer Cloudeinheit für Azure

Microsoft Azure bietet eine Reihe von Speicherkontotypen. Die *Cloud Providers Compatibility Matrix*, die auf der Seite der Data Protection Community unter https://inside.dell.com/community/active/data-protection verfügbar ist, bietet die meisten aktuellen Informationen zu den unterstützten Speicherklassen.

Die folgenden Endpunkte werden vom Azure-Cloudanbieter je nach Speicherklasse und -region verwendet. Achten Sie darauf, dass DNS diesen Hostnamen vor der Konfiguration von Cloudeinheiten auflösen kann.

- *Kontoname*.blob.core.windows.net

Der Kontoname wird in der Azure-Cloudanbieterkonsole abgerufen.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Cloud Units**.
2. Klicken Sie auf **Add**.

   Das Dialogfeld „Add Cloud Unit“ wird angezeigt.
3. Geben Sie einen Namen für diese Cloudeinheit ein. Es sind nur alphanumerische Zeichen zulässig.

   Die übrigen Felder im Dialogfeld „Add Cloud Unit“ beziehen sich auf das Cloudanbieterkonto.
4. Wählen Sie für **Cloud provider** in der Drop-down-Liste die Option **Microsoft Azure Storage** aus.
5. Wählen Sie für **Account type** die Option **Government** oder **Public** aus.
6. Wählen Sie in der Drop-down-Liste die Speicherklasse aus.
7. Geben Sie den **Account name** für den Anbieter ein.
8. Geben Sie den **Primary key** des Anbieters als Passworttext ein.
9. Geben Sie den **Secondary key** des Anbieters als Passworttext ein.
10. Stellen Sie sicher, dass Port 443 (HTTPS) nicht in Firewalls blockiert wird. Die Kommunikation mit dem Azure-Cloudanbieter erfolgt auf Port 443.
11. Wenn ein HTTP-Proxyserver erforderlich ist, um eine Firewall für diesen Anbieter zu umgehen, klicken Sie auf **Configure** für **HTTP Proxy Server**.

    Geben Sie den Hostnamen, den Port, den Benutzer und das Passwort für den Proxyserver ein.
12. Klicken Sie auf **Add**.

Das Hauptfenster des Dateisystems zeigt nun zusammenfassende Informationen für die neue Cloudeinheit sowie ein Steuerelement zum Aktivieren und Deaktivieren der Cloudeinheit an.

Hinzufügen einer S3 Flexible-Anbietercloudeinheit

Die Cloud-Tier-Funktion unterstützt zusätzliche qualifizierte S3-Cloudanbieter unter einer Konfigurationsoption für S3 Flexible-Anbieter.

Die S3 Flexible-Anbieteroption unterstützt die Speicherklassen „Standard“ und „Standard Infrequent“. Die Endpunkte variieren abhängig vom Cloudanbieter und der Speicherklasse und -region. Achten Sie darauf, dass DNS diesen Hostnamen vor der Konfiguration von Cloudeinheiten auflösen kann.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Cloud Units**.
2. Klicken Sie auf **Add**.

   Das Dialogfeld „Add Cloud Unit“ wird angezeigt.
3. Geben Sie einen Namen für diese Cloudeinheit ein. Es sind nur alphanumerische Zeichen zulässig.

   Die übrigen Felder im Dialogfeld „Add Cloud Unit“ beziehen sich auf das Cloudanbieterkonto.
4. Wählen Sie für **Cloud provider** die Option **Flexible Cloud Tier Provider Framework for S3** aus der Drop-down-Liste aus.
5. Geben Sie den **Access key** des Anbieters als Passworttext ein.
6. Geben Sie den **Secret key** des Anbieters als Passworttext ein.
7. Geben Sie die jeweilige **Storage region** ein.
8. Geben Sie den **Endpoint** des Anbieters im folgenden Format ein: `http://<ip/hostname>:<port>`. Wenn Sie einen sicheren Endpunkt verwenden, verwenden Sie stattdessen `https`.
9. Wählen Sie für **Storage class** die jeweilige Speicherklasse aus der Drop-down-Liste aus.
10. Stellen Sie sicher, dass Port 443 (HTTPS) nicht in Firewalls blockiert wird. Die Kommunikation mit dem S3-Cloudanbieter erfolgt auf Port 443.
11. Wenn ein HTTP-Proxyserver erforderlich ist, um eine Firewall für diesen Anbieter zu umgehen, klicken Sie auf **Configure** für **HTTP Proxy Server**.

    Geben Sie den Hostnamen, den Port, den Benutzer und das Passwort für den Proxyserver ein.
12. Klicken Sie auf **Add**.

    Das Hauptfenster des Dateisystems zeigt nun zusammenfassende Informationen für die neue Cloudeinheit sowie ein Steuerelement zum Aktivieren und Deaktivieren der Cloudeinheit an.

Ändern einer Cloudeinheit oder eines Cloudprofils

Ändern Sie die Anmeldedaten der Cloudeinheit, einen S3 Flexible-Anbieternamen oder Details eines Cloudprofils.

Ändern von Cloudeinheit-Anmeldeinformationen

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Cloud Units**.
2. Klicken Sie auf das Bleistiftsymbol für die Cloudeinheit, deren Anmeldedaten Sie ändern möchten.

   Das Dialogfeld „Modify Cloud Unit“ wird angezeigt.
3. Geben Sie für **Account name** den neuen Kontonamen ein.
4. Geben Sie für **Access key** den neuen Zugriffsschlüssel des Anbieters als Passworttext ein.

   Hinweis

   Das Ändern des Zugriffsschlüssels wird für ECS-Umgebungen nicht unterstützt.
5. Geben Sie für **Secret key** den neuen geheimen Schlüssel des Anbieters als Passworttext ein.
6. Geben Sie für **Primary key** den neuen primären Schlüssel des Anbieters als Passworttext ein.

   Hinweis

   Das Ändern des primären Schlüssels wird nur für Azure-Umgebungen unterstützt.
7. Wenn ein HTTP-Proxyserver erforderlich ist, um eine Firewall für diesen Anbieter zu umgehen, klicken Sie auf **Configure** für **HTTP Proxy Server**.
8. Klicken Sie auf **OK**.

Ändern eines Flexible S3-Anbieternamens

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Cloud Units**.
2. Klicken Sie auf das Bleistiftsymbol für die S3 Flexible-Cloudeinheit, deren Namen Sie ändern möchten.

   Das Dialogfeld „Modify Cloud Unit“ wird angezeigt.
3. Geben Sie für **S3 Provider Name** den neuen Anbieternamen ein.
4. Klicken Sie auf **OK**.

Verwenden der CLI zum Ändern eines Cloudprofils

Vorgehensweise

1. Führen Sie den Befehl `cloud profile modify` aus, um die Details eines Cloudprofils zu ändern. Das System fordert Sie auf, einzelne Details des Cloudprofils zu ändern.

   Führen Sie für Virtustream-, AWS S3- oder Azure-Profile diesen Befehl aus, um eine Speicherklasse zu einem vorhandenen Cloudprofil hinzuzufügen.

   Die Profildetails, die geändert werden können, hängen vom Cloudanbieter ab:

- ECS unterstützt die Änderung des geheimen Schlüssels.
- Virtustream unterstützt die Änderung des Zugriffsschlüssels und geheimen Schlüssels.
- AWS S3 unterstützt die Änderung des Zugriffsschlüssels und geheimen Schlüssels.
- Azure unterstützt die Änderung des Zugriffsschlüssels, des geheimen Schlüssels und primären Schlüssels.
- S3 Flexible unterstützt die Änderung des Zugriffsschlüssels, geheimen Schlüssels und Anbieternamens.

Löschen einer Cloudeinheit

Dieser Vorgang führt zum Verlust aller Daten in der Cloudeinheit, die zum Löschen ausgewählt wurde. Achten Sie darauf, dass Sie alle Dateien löschen, bevor Sie die Cloudeinheiten löschen.

Bevor Sie beginnen

- Prüfen Sie, ob die Datenverschiebung in die Cloud ausgeführt wird (CLI-Befehl: data-movement status). Ist dies der Fall, beenden Sie die Datenverschiebung mithilfe des CLI-Befehls „data-movement stop“.
- Prüfen Sie, ob für diese Cloudeinheit eine Cloudbereinigung ausgeführt wird (CLI-Befehl: cloud clean status). Wenn dies der Fall ist, beenden Sie die Cloudbereinigung mithilfe des CLI-Befehls „cloud clean“.
- Prüfen Sie, ob eine Datenverschiebungs-Policy für diese Cloudeinheit konfiguriert ist (CLI-Befehl: data-movement policy show). Wenn dies der Fall ist, entfernen Sie diese Richtlinie mit dem CLI-Befehl „data-movement policy reset“.

Vorgehensweise

1. Verwenden Sie den folgenden CLI-Befehl, um Dateien in der Cloudeinheit zu identifizieren.

   ```
   # filesys report generate file-location
   ```

2. Löschen Sie die Dateien, die sich in der Cloudeinheit befinden, die gelöscht werden soll.
3. Verwenden Sie den folgenden CLI-Befehl, um die Cloudbereinigung auszuführen.

   ```
   # cloud clean start unit-name
   ```

   Warten Sie bis zum Abschluss der Bereinigung. Die Bereinigung kann einige Zeit dauern, je nachdem, wie viele Daten in der Cloudeinheit vorhanden sind.
4. Deaktivieren Sie das Dateisystem.
5. Verwenden Sie den folgenden CLI-Befehl, um die Cloudeinheit zu löschen.

   ```
   # cloud unit del unit-name
   ```

   Intern, kennzeichnet die Cloudeinheit als DELETE_PENDING.
6. Verwenden Sie den folgenden CLI-Befehl, um zu überprüfen, ob die Cloudeinheit den Status „DELETE_PENDING“ hat.

   ```
   # cloud unit list
   ```

7. Aktivieren Sie das Dateisystem.

   Das Dateisystem initiiert das Verfahren im Hintergrund, um alle verbleibenden Objekte aus den Buckets in der Cloud für diese Cloudeinheit zu löschen und anschließend die Buckets zu löschen. Dieser Vorgang kann lange dauern, je nachdem, wie viele Objekte in diesen Buckets vorhanden sind. Bis die Bucket-Bereinigung abgeschlossen ist, verwendet diese Cloudeinheit weiterhin einen Steckplatz auf dem Data Domain-System. Dies kann die Erstellung einer neuen Cloudeinheit verhindern, wenn beide Steckplätze belegt sind.
8. Prüfen Sie regelmäßig den Status mit diesem CLI-Befehl:

   ```
   # cloud unit list
   ```

   Der Status bleibt DELETE_PENDING, während die Hintergrundbereinigung ausgeführt wird.
9. Prüfen Sie im Cloud Provider S3 Portal, ob alle entsprechenden Buckets gelöscht wurden und der verknüpfte Speicherplatz freigegeben wurde.
10. Konfigurieren Sie bei Bedarf die Datenverschiebungs-Policies für betroffene MTrees neu und starten Sie die Datenverschiebung erneut.

Ergebnisse

Wenn Sie Schwierigkeiten haben, kontaktieren Sie den Support.

Datenverschiebung

Daten werden vom aktiven Tier auf den Cloud-Tier verschoben, wie durch Ihre individuelle Datenverschiebungs-Policy angegeben. Die Policy wird auf einer Basis pro MTree festgelegt. Die Datenverschiebung kann manuell oder automatisch mit einem Zeitplan initiiert werden.

Hinzufügen von Datenverschiebungs-Policies auf MTrees

Eine Datei wird basierend auf dem Datum, an dem sie das letzte Mal geändert wurde, aus dem aktiven in den Cloud-Tier verschoben. Für die Integrität der Daten wird zu diesem Zeitpunkt die gesamte Datei verschoben. Die *Datenverschiebungs-Policy* legt den Schwellenwert für das Alter von Dateien, den Altersbereich und das Ziel fest.

Hinweis

Eine Datenverschiebungs-Policy kann nicht für den /backup-Mtree konfiguriert werden.

Vorgehensweise

1. Wählen Sie**Data Management** > **MTree** aus.
2. Wählen Sie im oberen Bereich den MTree aus, dem Sie eine Datenverschiebungs-Policy hinzufügen möchten.
3. Klicken Sie auf die Registerkarte **Summary**.
4. Klicken Sie unter **Data Movement Policy** auf die Option **Add**.
5. Legen Sie für **File Age in Days** den Schwellenwert für das Alter von Dateien (**Older than**) und optional den Altersbereich (**Younger than**) fest.

Hinweis

Die Mindestanzahl der Tage für **Older than** ist 14. Auf in den Cloud-Tier verschobene Dateien kann für nicht integrierte Backupanwendungen nicht direkt zugegriffen werden. Sie müssen in den aktiven Tier abgerufen werden, bevor Sie darauf zugreifen können. Wählen Sie also den Schwellenwert für das Alter entsprechend aus, um die Notwendigkeit des Zugriffs auf eine in den Cloud-Tier verschobene Datei zu minimieren oder zu vermeiden.

6. Geben Sie die Zielcloudeinheit für **Destination** an.
7. Klicken Sie auf **Add**.

Manuelles Verschieben von Daten

Sie können die Datenverschiebung manuell starten und beenden. Bei jedem MTree mit einer gültigen Datenverschiebungs-Policy werden Dateien verschoben.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System**
2. Klicken Sie am unteren Rand der Seite auf **Show Status of File System Services**.

   Die folgenden Statuselemente werden angezeigt:

   - Dateisystem
   - Messungen der physischen Kapazität
   - Datenverschiebung
   - Bereinigung des aktiven Tier

3. Klicken Sie für **Data Movement** auf die Option **Start**.

Automatisches Verschieben von Daten

Sie können Daten mit einem Zeitplan und einer Drosselung automatisch verschieben. Zeitpläne können täglich, wöchentlich oder monatlich sein.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Settings** aus.
2. Klicken Sie auf die Registerkarte **Data Movement**.
3. Legen Sie die Drosselung und den Zeitplan fest.

Hinweis

Die Drosselung dient der Anpassung von Ressourcen für interne Data Domain-Prozesse. Sie wirkt sich nicht auf die Netzwerkbandbreite aus.

Hinweis

Wenn auf eine Cloudeinheit bei der Cloud-Tier-Datenverschiebung nicht zugegriffen werden kann, wird die Cloudeinheit in dieser Ausführung übersprungen. Die Datenverschiebung auf dieser Cloudeinheit erfolgt in der nächsten Ausführung, wenn die Cloudeinheit verfügbar wird. Der Zeitplan für die Datenverschiebung bestimmt die Dauer zwischen zwei Ausführungen. Wenn die Cloudeinheit verfügbar wird und es Ihnen nicht möglich ist, auf die nächste geplante Ausführung zu warten, können Sie die Datenverschiebung manuell starten.

Abrufen einer Datei aus dem Cloud-Tier

Für nicht integrierte Backupanwendungen müssen Sie die Daten in den aktiven Tier abrufen, bevor Sie die Daten wiederherstellen können. Backupadministratoren müssen einen Abruf auslösen oder Backupanwendungen einen Abruf durchführen, bevor cloudbasierte Backups wiederhergestellt werden können. Sobald eine Datei abgerufen wird, wird ihr Alter zurückgesetzt, die Zählung beginnt erneut bei 0 und die Datei ist basierend auf dem Alters-Policy-Satz qualifiziert. Eine Datei kann nur auf dem Quell-MTree abgerufen werden. Integrierte Anwendungen können eine Datei direkt abrufen.

Hinweis

Wenn eine Datei nur in einem Snapshot vorhanden ist, kann sie nicht direkt abgerufen werden. Um eine Datei in einem Snapshot abzurufen, verwenden Sie fastcopy, um die Datei aus dem Snapshot zurück in den aktiven MTree zu kopieren. Rufen Sie die Datei anschließend aus der Cloud ab. Eine Datei kann nur in einen aktiven Mtree aus der Cloud abgerufen werden.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Summary** aus.
2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie im Bereich „Cloud Tier“ des Fensterbereichs „Space Usage“ auf **Recall**.
   - Blenden Sie den Statusfensterbereich „File System“ unten ein und klicken Sie auf **Recall**.

     Hinweis

     Der Link **Recall** ist nur verfügbar, wenn eine Cloudeinheit erstellt wird und Daten aufweist.
3. Geben Sie im Dialogfeld „Recall File from Cloud“ den exakten Dateinamen (keine Platzhalter) und den vollständigen Pfad zur aufzurufenden Datei an, beispielsweise: `/data/col1/mt11/file1.txt`. Klicken Sie auf **Recall**.
4. Um den Status des Abrufs zu prüfen, gehen Sie wie folgt vor:
   - Klicken Sie im Bereich „Cloud Tier“ des Fensterbereichs „Space Usage“ auf **Details**.
   - Blenden Sie den Statusfensterbereich „File System“ unten ein und klicken Sie auf **Details**.

   Das Dialogfeld „Cloud File Recall Details“ mit Dateipfad, Cloudanbieter, Abruf-Fortschritt und Menge der übertragenen Daten wird angezeigt. Wenn während

des Abrufs nicht behebbare Fehler auftreten, wird eine Fehlermeldung angezeigt. Bewegen Sie den Mauszeiger über die Fehlermeldung, um eine Kurzinformation mit weiteren Details und mögliche Korrekturmaßnahmen anzuzeigen.

Ergebnisse

Sobald die Datei zum aktiven Tier abgerufen wurde, können Sie die Daten wiederherstellen.

Hinweis

Sobald eine Datei aus dem Cloud-Tier in den aktiven Tier abgerufen wurde, müssen für nicht integrierte Anwendungen mindestens 14 Tage verstreichen, bis die Datei für die Datenverschiebung berechtigt ist. Die Datei ist nach 14 Tagen für die normale Datenverschiebungsverarbeitung berechtigt. Diese Einschränkung gilt nicht für integrierte Anwendungen.

Hinweis

Für die Datenverschiebung konfigurieren nicht integrierte Anwendungen eine altersbasierte Datenverschiebungs-Policy auf dem Data Domain-System, um anzugeben, welche Dateien zum Cloud-Tier migriert werden. Diese Policy gilt gleichermaßen für alle Dateien in einem MTree. Integrierte Anwendungen verwenden eine anwendungsverwaltete Datenverschiebungs-Policy, sodass Sie bestimmte Dateien identifizieren können, die zum Cloud-Tier migriert werden sollen.

Verwenden der CLI zum Abrufen einer Datei aus dem Cloud-Tier

Für nicht integrierte Backupanwendungen müssen Sie die Daten in den aktiven Tier abrufen, bevor Sie die Daten wiederherstellen können. Backupadministratoren müssen einen Abruf auslösen oder Backupanwendungen einen Abruf durchführen, bevor cloudbasierte Backups wiederhergestellt werden können. Sobald eine Datei abgerufen wird, wird ihr Alter zurückgesetzt, die Zählung beginnt erneut bei 0 und die Datei ist basierend auf dem Alters-Policy-Satz qualifiziert. Eine Datei kann nur auf dem Quell-MTree abgerufen werden. Integrierte Anwendungen können eine Datei direkt abrufen.

Hinweis

Wenn eine Datei nur in einem Snapshot vorhanden ist, kann sie nicht direkt abgerufen werden. Um eine Datei in einem Snapshot abzurufen, verwenden Sie fastcopy, um die Datei aus dem Snapshot zurück in den aktiven MTree zu kopieren. Rufen Sie die Datei anschließend aus der Cloud ab. Eine Datei kann nur in einen aktiven Mtree aus der Cloud abgerufen werden.

Vorgehensweise

1. Überprüfen Sie den Speicherort der verwendeten Datei:
   `filesys report generate file-location [path {<path-name> | all}] [output-file <filename>]`

   Bei dem Pfadnamen kann es sich um eine Datei oder ein Verzeichnis handeln. Wenn es sich um ein Verzeichnis handelt, werden alle Dateien im Verzeichnis aufgeführt.

```
Filename                    Location
--------                    --------
/data/col1/mt11/file1.txt   Cloud Unit 1
```

2. Rufen Sie die Datei mit folgendem Befehl ab:
   `data-movement recall path <path-name>`

   Dieser Befehl ist asynchron und startet den Abruf.

   ```
   data-movement recall path /data/col1/mt11/file1.txt
   Recall started for "/data/col1/mt11/file1.txt".
   ```

3. Überwachen Sie den Status des Abrufs unter Verwendung des folgenden Befehls:
   `data-movement status [path {pathname | all | [queued] [running] [completed] [failed]} | to-tier cloud | all]`

   ```
   data-movement status path /data/col1/mt11/file1.txt
   Data-movement recall:
   ---------------------
   Data-movement for "/data/col1/mt11/file1.txt": phase 2 of 3
   (Verifying)
   80% complete; time: phase  XX:XX:XX total  XX:XX:XX
   Copied (post-comp): XX XX, (pre-comp) XX XX
   ```

   Wenn der Status anzeigt, dass der Abruf für einen bestimmten Pfad ausgeführt wird, ist der Abruf möglicherweise abgeschlossen oder fehlgeschlagen.

4. Überprüfen Sie den Speicherort der Datei unter Verwendung des folgenden Befehls:
   `filesys report generate file-location [path { | all}] [output-file ]`

   ```
   Filename                    Location
   --------                    --------
   /data/col1/mt11/file1.txt   Active
   ```

Ergebnisse

Sobald die Datei zum aktiven Tier abgerufen wurde, können Sie die Daten wiederherstellen.

Hinweis

Sobald eine Datei aus dem Cloud-Tier in den aktiven Tier abgerufen wurde, müssen für nicht integrierte Anwendungen mindestens 14 Tage verstreichen, bis die Datei für die Datenverschiebung berechtigt ist. Die Datei ist nach 14 Tagen für die normale Datenverschiebungsverarbeitung berechtigt. Diese Einschränkung gilt nicht für integrierte Anwendungen.

Hinweis

Für die Datenverschiebung konfigurieren nicht integrierte Anwendungen eine altersbasierte Datenverschiebungs-Policy auf dem Data Domain-System, um anzugeben, welche Dateien zum Cloud-Tier migriert werden. Diese Policy gilt gleichermaßen für alle Dateien in einem MTree. Integrierte Anwendungen verwenden eine anwendungsverwaltete Datenverschiebungs-Policy, sodass Sie bestimmte Dateien identifizieren können, die zum Cloud-Tier migriert werden sollen.

Direkte Wiederherstellung aus dem Cloud-Tier

Dank der direkten Wiederherstellung können nicht integrierte Anwendungen Dateien direkt aus dem Cloud-Tier lesen, ohne Durchlaufen des aktiven Tier.

Wichtige Überlegungen im Hinblick auf die direkte Wiederherstellung umfassen:

- Die direkte Wiederherstellung erfordert keine integrierte Anwendung und ist für nicht integrierte Anwendungen transparent.
- Das Lesen aus dem Cloud-Tier erfordert kein vorheriges Kopieren in den aktiven Tier.
- Histogramme und Statistiken sind für die Nachverfolgung von direkten Lesevorgängen vom Cloud-Tier verfügbar.
- Die direkte Wiederherstellung wird nur für ECS-Cloudanbieter unterstützt.
- Bei Anwendungen tritt Cloud-Tier-Latenz auf.
- Das Lesen direkt aus dem Cloud-Tier ist nicht bandbreitenoptimiert.
- Die direkte Wiederherstellung unterstützt eine kleine Zahl von Jobs.

Die direkte Wiederherstellung ist für nicht integrierte Anwendungen nützlich, die nicht über den Cloud-Tier informiert sein und nicht häufig Clouddateien wiederherstellen müssen.

Verwenden der Befehlszeilenoberfläche (CLI) zur Konfiguration von DD Cloud-Tier

Sie können die Data Domain-Befehlszeilenoberfläche zur Konfiguration von DD Cloud-Tier verwenden.

Vorgehensweise

1. Konfigurieren Sie Speicher für den aktiven und für den Cloud-Tier. Als Voraussetzung müssen für die aktiven und für die Cloud-Tiers die entsprechenden Kapazitätslizenzen installiert sein.

   a. Vergewissern Sie sich, dass Lizenzen für die Funktionen CLOUDTIER-CAPACITY und CAPACITY-ACTIVE installiert sind. So prüfen Sie die ELMS-Lizenz:

   ```
   # elicense show
   ```

   Wenn die Lizenz nicht installiert ist, verwenden Sie den Befehl `elicense update`, um die Lizenz zu installieren. Geben Sie den Befehl ein und fügen Sie den Inhalt der Lizenzdatei nach der Aufforderung ein. Stellen Sie nach dem Einfügen sicher, dass ein Zeilenumbruch vorhanden ist, und klicken Sie auf **Control-D**, um zu speichern. Sie werden dazu aufgefordert, Lizenzen zu ersetzen, und nach der Beantwortung mit „yes“ werden die Lizenzen angewendet und angezeigt.

   ```
   # elicense update
   Enter the content of license file and then press Control-D,
   or press Control-C to cancel.
   ```

   b. Zeigen Sie den verfügbaren Speicher an:

   ```
   # storage show all# disk show state
   ```

   c. Fügen Sie Speicher zum aktiven Tier hinzu:

   ```
   # storage add enclosures <enclosure no> tier active
   ```

   d. Fügen Sie Speicher zum Cloud-Tier hinzu:

   ```
   # storage add enclosures <enclosure no> tier cloud
   ```

2. Installieren Sie Zertifikate.

   Bevor Sie ein Cloudprofil erstellen können, müssen Sie die zugehörigen Zertifikate installieren.

   Für die Public-Cloud-Anbieter AWS, Virtustream und Azure können Root-CA-Zertifikate hier https://www.digicert.com/digicert-root-certificates.htm heruntergeladen werden.

   - Laden Sie für den Cloudanbieter AWS das Zertifikat Baltimore CyberTrust Root herunter.
   - Laden Sie für den Cloudanbieter Virtustream das CA-Zertifikat DigiCert High Assurance EV Root herunter.
   - Laden Sie für den Cloudanbieter Azure das Zertifikat Baltimore CyberTrust Root herunter.
   - Für ECS variiert die Stammzertifizierungsstelle je nach Kunde. Weitere Informationen erhalten Sie von Ihrem Load Balancer-Anbieter.

   Heruntergeladene Zertifikatdateien haben die Erweiterung .crt. Verwenden Sie OpenSSL auf jedem Linux- oder Unix-System, auf dem es ist installiert ist, um die Datei aus dem .crt-Format in das .pem-Format zu konvertieren.

   ```
   $openssl x509 -inform der -in DigiCertHighAssuranceEVRootCA.crt
   -out DigiCertHighAssuranceEVRootCA.pem
   ```

   ```
   $openssl x509 -inform der -in BaltimoreCyberTrustRoot.crt -out
   BaltimoreCyberTrustRoot.pem
   ```

   ```
   # adminaccess certificate import ca application cloud
   Enter the certificate and then press Control-D, or press
   Control-C to cancel.
   ```

3. Um das Data Domain-System für die Datenverschiebung in die Cloud zu konfigurieren, müssen Sie zunächst die Funktion „Cloud“ aktivieren und die Systempassphrase festlegen, wenn sie nicht bereits festgelegt wurde.

   ```
   # cloud enable
   Cloud feature requires that passphrase be set on the system.
   Enter new passphrase:
   Re-enter new passphrase:
   Passphrases matched.
   The passphrase is set.
   Encryption is recommended on the cloud tier.
       Do you want to enable encryption? (yes|no) [yes]:
   Encryption feature is enabled on the cloud tier.
   Cloud feature is enabled.
   ```

4. Konfigurieren Sie das Cloudprofil mit den Anmeldedaten des Cloudanbieters. Die Aufforderungen und Variablen variieren je nach Anbieter.

   ```
   # cloud profile add <profilename>
   ```

   Hinweis

   Aus Sicherheitsgründen zeigt dieser Befehl die von Ihnen eingegebenen Zugriffsschlüssel und geheimen Schlüssel nicht an.

   Wählen Sie den Anbieter aus:

   ```
   Enter provider name (aws|azure|ecs|s3_flexible|virtustream)
   ```

   - AWS S3 erfordert den Zugriffsschlüssel, den geheimen Schlüssel, die Speicherklasse und die Region.

- Azure erfordert einen Kontonamen, unabhängig davon, ob das Konto ein Azure Government-Konto ist, einen primären, einen sekundären Schlüssel und eine Speicherklasse.
- ECS erfordert die Eingabe des Zugriffsschlüssels, des geheimen Schlüssels und des Endpunkts.
- S3 Flexible-Anbieter erfordern den muss der Anbieternamen, den Zugriffsschlüssel, den geheimen Schlüssel, die Region, den Endpunkt und die Speicherklasse.
- Virtustream erfordert den Zugriffsschlüssel, den geheimen Schlüssel, die Speicherklasse und die Region.

Sie werden jeweils am Ende des Vorgangs zum Hinzufügen eines Profils gefragt, ob Sie einen Proxy einrichten möchten. Wenn Sie dies tun, sind die folgenden Werte erforderlich: *proxy hostname*, *proxy port*, *proxy username* und *proxy password*.

5. Überprüfen Sie die Konfiguration des Cloudprofils:

   ```
   # cloud profile show
   ```

6. Erstellen Sie das Dateisystem des aktiven Tier, wenn es nicht bereits erstellt wurde:

   ```
   # filesys create
   ```

7. Aktivieren Sie das Dateisystem:

   ```
   # filesys enable
   ```

8. Konfigurieren Sie die Cloudeinheit:

   ```
   # cloud unit add unitname profile profilename
   ```

   Verwenden Sie den Befehl `cloud unit list` zum Auflisten der Cloudeinheiten.

9. Konfigurieren Sie optional die Verschlüsselung für die Cloudeinheit.
   a. Überprüfen Sie, ob die Lizenz ENCRYPTION installiert ist:

      ```
      # elicense show
      ```

   b. Aktivieren Sie die Verschlüsselung für die Cloudeinheit:

      ```
      # filesys encryption enable cloud-unit unitname
      ```

   c. Überprüfen Sie den Verschlüsselungsstatus:

      ```
      # filesys encryption status
      ```

10. Erstellen Sie einen oder mehrere MTrees:

    ```
    # mtree create /data/col1/mt11
    ```

11. Überprüfen Sie die Konfiguration von DD Cloud Tier:

```
# cloud provider verify
This operation will perform test data movement after creating a temporary profile and
bucket.
Do you want to continue? (yes|no) [yes]:
Enter provider name (aws|azure|virtustream|ecs|s3_generic): aws
Enter the access key:
Enter the secret key:
```

```
Enter the region (us-east-1|us-west-1|us-west-2|eu-west-1|apnortheast-1|ap-southeast-1|
ap-southeast-2|
sa-east-1|ap-south-1|ap-northeast-2|eu-central-1):

Verifying cloud provider …
This process may take a few minutes.
Cloud Enablement Check:
 Checking Cloud feature enabled: PASSED
 Checking Cloud volume: PASSED

Connectivity Check:
 Checking firewall access: PASSED
 Validating certificate PASSED

Account Validation:
 Creating temporary profile: PASSED
 Creating temporary bucket: PASSED

S3 API Validation:
 Validating Put Bucket: PASSED
 Validating List Bucket: PASSED
 Validating Put Object: PASSED
 Validating Get Object: PASSED
 Validating List Object: PASSED
 Validating Delete Object: PASSED
 Validating Bulk Delete: PASSED

Cleaning Up:
 Deleting temporary bucket: PASSED
 Deleting temporary profile: PASSED

Provider verification passed.
```

12. Konfigurieren Sie die Dateimigrations-Policy für diesen MTree. Sie können mehrere MTrees in diesem Befehl angeben. Die Policy kann auf dem Altersschwellenwert oder dem Bereich basieren.

    a. So konfigurieren Sie den Altersschwellenwert (Migration von Dateien in die Cloud, die älter als das angegebene Alter sind):

    ```
    # data-movement policy set age-threshold age_in_days to-tier
    cloud cloud-unit unitname mtrees mtreename
    ```

    b. So konfigurieren Sie den Altersbereich (Migration ausschließlich von Dateien, die sich im festgelegten Altersbereich befinden):

    ```
    # data-movement policy set age-range min-age age_in_days max-
    age age_in_days to-tier cloud cloud-unit unitname mtrees
    mtreename
    ```

13. Exportieren Sie das Dateisystem. Mounten Sie das Dateisystem über den Client und nehmen Sie Daten in den aktiven Tier auf. Ändern Sie das Änderungsdatum der aufgenommenen Dateien, sodass sie jetzt für die Datenmigration qualifiziert sind. (Setzen Sie das Datum auf einen Wert, der älter ist als der bei der Konfiguration der Datenverschiebungs-Policy festgelegte Altersschwellenwert.)
14. Initiieren Sie die Dateimigration der veralteten Dateien. Auch in diesem Befehl können Sie mehrere MTrees angeben.

    ```
    # data-movement start mtrees mtreename
    ```

    So prüfen Sie den Status der Datenverschiebung:

    ```
    # data-movement status
    ```

    Sie können ebenso den Fortschritt der Datenverschiebung überwachen:

    ```
    # data-movement watch
    ```

15. Überprüfen Sie, dass die Dateimigration erfolgreich war und die Dateien sich nun im Cloud-Tier befinden:

```
# filesys report generate file-location path all
```

16. Sobald Sie eine Datei in den Cloud-Tier migriert haben, können Sie nicht direkt in der Datei lesen. (Der Versuch führt zu einem Fehler.) Die Datei kann nur zurück zum aktiven Tier abgerufen werden. So rufen Sie eine Datei zum aktiven Tier ab:

```
# data-movement recall path pathname
```

Konfigurieren der Verschlüsselung für DD-Cloudeinheiten

Verschlüsselung kann auf drei Ebenen aktiviert werden: Data Domain-System, aktiver Tier und Cloudeinheit. Verschlüsselung des aktiven Tier ist nur anwendbar, wenn die Verschlüsselung für das Data Domain-System aktiviert ist. Cloudeinheiten verfügen über separate Steuerelemente zum Aktivieren der Verschlüsselung.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **DD Encryption** aus.

   Hinweis

   Wenn keine Verschlüsselungslizenz auf dem System vorhanden ist, wird die Seite „Add Licenses“ angezeigt.

2. Führen Sie im Bereich „DD Encryption“ einen der folgenden Schritte aus:
   - Zum Aktivieren der Verschlüsselung für **Cloud Unit *x***, klicken Sie auf **Enable**.
   - Zum Deaktivieren der Verschlüsselung für **Cloud Unit *x***, klicken Sie auf **Disable**.

   Hinweis

   Sie werden zum Aktivieren der Verschlüsselung aufgefordert, die Anmeldedaten für den Security Officer einzugeben.

3. Geben Sie den **Username** und das **Password** für den Security Officer ein. Wählen Sie optional **Restart file system now** aus.
4. Klicken Sie nach Bedarf auf **Enable** oder **Disable**.
5. Sperren oder entsperren Sie im Bereich „File System Lock“ das Dateisystem.
6. Klicken Sie im Bereich „Key Management“ auf **Configure**.
7. Konfigurieren Sie im Dialogfeld „Change Key Manager“ die Anmeldedaten für den Security Manager und den Key Manager.

   Hinweis

   Cloudverschlüsselung darf nur über den Data Domain Embedded Key Manager erfolgen. Externe Key Manager werden nicht unterstützt.

8. Klicken Sie auf **OK**.

9. Verwenden Sie den Bereich „DD Encryption Keys“, um Chiffrierschlüssel zu konfigurieren.

Bei Systemverlust erforderliche Informationen

Notieren Sie sich nach der Cloud Tier-Konfiguration auf dem Data Domain-System die folgenden Informationen zum System und bewahren Sie sie an einem sicheren Ort auf (nicht direkt beim Data Domain-System). Diese Informationen werden benötigt, um die Cloud Tier-Daten wiederherzustellen, wenn das Data Domain-System verloren geht.

Hinweis

Dieser Prozess ist nur für Notfallsituationen entwickelt und beinhaltet einen signifikanten Zeit- und Arbeitsaufwand für die Data Domain Engineering-Mitarbeiter.

- Seriennummer des ursprünglichen Data Domain-Systems
- Systempassphrase des ursprünglichen Data Domain-Systems
- DD OS-Versionsnummer des ursprünglichen Data Domain-Systems
- Cloud Tier-Profil und Konfigurationsinformationen

Verwenden von DD Replicator mit Cloud Tier

Die Sammelreplikation wird in für Cloud Tier aktivierten Data Domain-Systemen nicht unterstützt.

Die Verzeichnisreplikation funktioniert nur auf dem /backup-Mtree und dieser MTree kann dem Cloud-Tier nicht zugewiesen werden. Die Verzeichnisreplikation ist also von Cloud Tier nicht betroffen.

Gemanagte Dateireplikation und die MTree-Replikation werden auf Cloud Tier-fähigen Data Domain-Systemen unterstützt. Ein oder beide Systeme können Cloud Tier aktiviert haben. Wenn das Quellsystem für Cloud Tier aktiviert ist, müssen möglicherweise Daten aus der Cloud gelesen werden, wenn die Datei bereits auf den Cloud-Tier migriert wurde. Eine replizierte Datei wird immer zuerst im aktiven Tier auf dem Zielsystem abgelegt, selbst wenn Cloud Tier aktiviert ist. Eine Datei kann nur auf dem Quell-MTree vom Cloud-Tier zurück zum aktiven Tier abgerufen werden. Abrufen einer Datei auf dem Ziel-MTree ist nicht zulässig.

Hinweis

Wenn das Quellsystem DD OS 5.6 oder 5.7 ist und in ein für Cloud Tier aktiviertes System mithilfe der MTree-Replikation repliziert wird, muss das Quellsystem auf eine Version aktualisiert werden, die auf ein für Cloud Tier aktiviertes System repliziert werden kann. Weitere Informationen finden Sie in den Systemanforderungen in den *Versionshinweisen zu DD OS*.

Hinweis

Dateien im Cloud-Tier können als Basisdateien für virtuelle synthetische Vorgänge verwendet werden. Die kontinuierlichen inkrementellen oder synthetischen kompletten Backups müssen sicherstellen, dass die Dateien im aktiven Tier bleiben, wenn sie in virtuellen Synthesen neuer Backups verwendet werden.

Verwenden von DD Virtual Tape Library (VTL) mit Cloud-Tier

Auf Systemen mit Cloud Tier und DD VTL wird der Cloudspeicher als VTL-Vault unterstützt. Um DD VTL-Band-zu-Cloud zu verwenden, lizenzieren und konfigurieren Sie zuerst den Cloudspeicher und wählen Sie ihn dann als Vault-Speicherort für die VTL aus.

DD VTL-Band-zu-Cloud auf Seite 384 enthält zusätzliche Informationen über die Verwendung von VTL mit Cloud Tier.

Anzeigen von Kapazitätsverbrauchsdiagrammen für DD Cloud-Tier

Für die Anzeige von Statistiken zum Cloud-Tier-Verbrauch stehen drei Diagramme zur Verfügung – „Space Usage“, „Consumption“ und „Daily Written“.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Charts** aus.
2. Wählen Sie für **Chart** eine der folgenden Optionen aus:
   - Space Usage
   - Consumption
   - Daily Written
3. Wählen Sie für **Scope** die Option **Cloud Tier** aus.
   - Die Registerkarte „Space Usage“ zeigt die Speicherplatznutzung im Laufe der Zeit in MiB an. Sie können eine Dauer (eine Woche, einen Monat, drei Monate, ein Jahr oder alle) auswählen. Die Daten werden wie folgt dargestellt (mit Farbcodierung): vor der Komprimierung verwendet (blau), nach der Komprimierung verwendet (rot) und Komprimierungsfaktor (grün).
   - Die Registerkarte „Consumption“ zeigt die Menge des verwendeten Speichers nach der Komprimierung und die Komprimierungsrate im Laufe der Zeit an, wodurch Sie Verbrauchstrends analysieren können. Sie können eine Dauer (eine Woche, einen Monat, drei Monate, ein Jahr oder alle) auswählen. Die Daten werden wie folgt dargestellt (mit Farbcodierung): als Kapazität (blau), nach der Komprimierung verwendet (rot), Komprimierungsfaktor (grün), Bereinigung (orange) und Datenverschiebung (violett).
   - Die Registerkarte „Daily Written“ zeigt die Menge der pro Tag geschriebenen Daten an. Sie können eine Dauer (eine Woche, einen Monat, drei Monate, ein Jahr oder alle) auswählen. Die Daten werden (mit Farbcodierung) als vor der Komprimierung geschrieben (blau), nach der Komprimierung verwendet (rot) und mit dem Gesamtkomprimierungsfaktor (grün) dargestellt.

DD Cloud-Tier-Protokolle

Wenn DD Cloud-Tier bei der Konfiguration oder beim Betrieb auf eine beliebige Art ausfällt, erstellt das System automatisch einen Ordner mit einem Zeitstempel, der dem Zeitpunkt des Ausfalls zugeordnet werden kann.

Die detaillierten Protokolle für den DD Cloud-Tier-Ausfall werden unter `/ddvar/log/debug/verify_logs` erstellt. Mounten Sie das Verzeichnis `/ddvar/log/debug`, um auf die Protokolle zuzugreifen.

Hinweis

Die Ausgabe des Befehls `log list view` führt nicht alle ausführlichen Protokolldateien auf, die für den DD Cloud-Tier-Ausfall erstellt wurden.

Verwenden der Befehlszeilenoberfläche (CLI) zur Entfernung von DD Cloud-Tier

Sie können die Data Domain-Befehlszeilenoberfläche zur Entfernung von DD Cloud-Tier verwenden.

Bevor Sie beginnen

Löschen Sie alle Dateien in den Cloudeinheiten, bevor Sie die DD Cloud-Tier-Konfiguration aus dem System entfernen. Führen Sie den Befehl `filesys report generate file-location path all output-file file_loc` aus, um die Dateien in den Cloudeinheiten zu ermitteln, und löschen Sie sie aus den NFS-Mount-Punkten der MTrees.

Hinweis

Der obige Befehl erstellt den Bericht `file_loc` im Verzeichnis `/ddr/var/`.

Vorgehensweise

1. Deaktivieren Sie das Dateisystem.

```
# filesys disable

This action will disable the file system.
Applications may experience interruptions
while the file system is disabled.
    Are you sure? (yes|no) [no]: yes

ok, proceeding.

Please wait.............
The filesystem is now disabled.
```

2. Listen Sie die Cloudeinheiten auf dem System auf.

```
# cloud unit list
Name           Profile        Status
------------   ------------   ------
cloud_unit-1   cloudProfile   Active
cloud_unit-2   cloudProfile2  Active
------------   ------------   ------
```

3. Löschen Sie die Cloudeinheiten einzeln.

```
# cloud unit del cloud_unit-1

This command irrevocably destroys all data
 in the cloud unit "cloud_unit-1".
    Are you sure? (yes|no) [no]: yes

ok, proceeding.

Enter sysadmin password to confirm:

Destroying cloud unit "cloud_unit-1"
Cloud unit 'cloud_unit-1' deleted. The data in the cloud will be deleted asynchronously
on the filesystem startup.

# cloud unit del cloud_unit-2

This command irrevocably destroys all data
 in the cloud unit "cloud_unit-2".
    Are you sure? (yes|no) [no]: yes

ok, proceeding.

Enter sysadmin password to confirm:

Destroying cloud unit "cloud_unit-2"
Cloud unit 'cloud_unit-2' deleted. The data in the cloud will be deleted asynchronously
on the filesystem startup.
```

4. Stellen Sie sicher, dass die Löschvorgänge durchgeführt werden.

```
# cloud unit list
Name           Profile        Status
------------   ------------   ------
cloud_unit-1   cloudProfile   Delete-Pending
cloud_unit-2   cloudProfile2  Delete-Pending
------------   ------------   ------
```

5. Starten Sie das Dateisystem neu.

```
# filesys enable
Please wait.....................................
The filesystem is now enabled.
```

6. Führen Sie den Befehl `cloud unit list` aus, um sicherzustellen, dass keine Cloudeinheit angezeigt wird.

   Kontaktieren Sie den Support, wenn eine oder beide Cloudeinheiten weiterhin mit dem Status `Delete-Pending` angezeigt werden.

7. Identifizieren Sie die Festplattengehäuse, die dem DD Cloud-Tier zugewiesen sind.

```
# storage show tier cloud

Cloud tier details:
Disk   Disks               Count   Disk     Additional
Group                              Size     Information
------ ------------------- ------  -------- ------------
dgX    2.1-2.15, 3.1-3.15  30      3.6 TiB
------ ------------------- ------  -------- ------------
Current cloud tier size: 0.0 TiB
Cloud tier maximum capacity: 108.0 TiB
```

8. Entfernen Sie die Festplattengehäuse vom DD Cloud-Tier.

```
# storage remove enclosures 2, 3

Removing enclosure 2...Enclosure 2 successfully removed.
```

```
Updating system information...done
Successfuly removed: 2 done
Removing enclosure 3...Enclosure 3 successfully removed.
Updating system information...done
Successfuly removed: 3 done
```

KAPITEL 19

DD Extended Retention

Dieses Kapitel enthält die folgenden Themen:

Überblick über DD Extended Retention

DD Extended Retention (Data Domain Extended Retention) bietet einen internen Tiering-Ansatz, der die kosteneffektive, langfristige Aufbewahrung von Backupdaten in einem DD-System ermöglicht. Mit DD Extended Retention können Sie DD-Systeme zur langfristigen Aufbewahrung von Backupdaten und zur Minimierung der Abhängigkeit von Bändern nutzen.

Hinweis

DD Extended Retention war früher bekannt als *Data Domain Archiver.*

Two-Tiered-Dateisystem

Das interne Two-Tiered-Dateisystem eines DD-Systems mit DD Extended Retention besteht aus einem *aktiven Tier* und einem *Aufbewahrungs-Tier*. Das Dateisystem wird jedoch als eine einzige Einheit angezeigt. Eingehende Daten werden zunächst im aktiven Tier des Dateisystems abgelegt. Die Daten (in Form von vollständigen Dateien) werden später in den Aufbewahrungs-Tier des Dateisystems verschoben, wie durch Ihre individuelle *Datenverschiebungs-Policy* angegeben. Beispielsweise kann der aktive Tier wöchentliche komplette und tägliche inkrementelle Backups 90 Tage lang aufbewahren, während der Aufbewahrungs-Tier monatliche komplette Backups sieben Jahre lang aufbewahren kann.

Der Aufbewahrungs-Tier besteht aus einer oder mehreren Aufbewahrungseinheiten, von denen jede Speicher von einem oder mehreren Einschüben nutzen kann.

Hinweis

Ab DD OS 5.5.1 ist nur eine Aufbewahrungseinheit pro Aufbewahrungs-Tier zulässig. Vor DD OS 5.5.1 eingerichtete Systeme können zwar mehr als eine Aufbewahrungseinheit enthalten, Sie können ihnen jedoch keine weiteren Aufbewahrungseinheiten hinzufügen.

Transparenz des Vorgangs

DD-Systeme mit aktivierter DD Extended Retention unterstützen vorhandene Backupanwendungen unter Verwendung gleichzeitiger Datenzugriffsmethoden mit den Dateiserviceprotokollen NFS und CIFS über Ethernet, DD VTL für offene Systeme und IBMi oder als festplattenbasiertes Ziel mit anwendungsspezifischen Schnittstellen wie DD Boost (zur Verwendung mit Avamar®, NetWorker®, Greenplum, Symantec OpenStorage und Oracle RMAN).

DD Extended Retention erweitert die DD-Architektur mit einer automatisierten transparenten Datenverschiebung vom aktiven Tier in den Aufbewahrungs-Tier. Alle Daten in den beiden Tiers sind zugänglich, auch wenn es ggf. eine geringe Verzögerung beim Erstzugriff auf Daten im Aufbewahrungs-Tier gibt. Der Namespace des Systems ist global und wird nicht durch die Datenverschiebung beeinflusst. Es ist keine Partitionierung des Dateisystems erforderlich, um das Two-Tier-Dateisystem zu nutzen.

Datenverschiebungs-Policy

Die *Datenverschiebungs-Policy*, die Sie anpassen können, ist die Policy, nach der Dateien vom aktiven in den Retention-Tier verschoben werden. Sie basiert auf dem Zeitpunkt, zu dem die Datei zuletzt geändert wurde. Sie können eine andere Policy für die jeweilige Untergruppe von Daten festlegen, da die Policy pro MTree festgelegt werden kann. Dateien, die aktualisiert werden können, benötigen eine Policy, die sich von denen für Dateien unterscheidet, die sich nie ändern.

Deduplizierung in der Aufbewahrungseinheit
Zu Fehleridentifikationszwecken erfolgt die Deduplizierung für DD-Systeme mit aktivierter DD Extended Retention vollständig in der Aufbewahrungseinheit. Es gibt keine übergreifende Deduplizierung zwischen aktiven und Aufbewahrungs-Tiers oder zwischen verschiedenen Aufbewahrungseinheiten (falls zutreffend).

Storage aus jedem Tier
Das Konzept des Tiering weitet sich auf die Speicherebene für ein DD-System mit aktivierter DD Extended Retention aus. Der aktive Tier des Dateisystems nutzt Speicher vom aktiven Tier des Speichers. Der Aufbewahrungs-Tier des Dateisystems nutzt Speicher vom Aufbewahrungs-Tier des Speichers.

Hinweis

Sowohl beim aktiven als auch beim Aufbewahrungs-Tier unterstützt DD OS 5.2 und höher ES20- und ES30-Einschübe. DD OS 5.7 und höher unterstützt DS60-Einschübe auf bestimmten Modellen. Verschiedene Data Domain-Einschubtypen können nicht in derselben Einschubgruppe gemischt werden und die Einschubgruppen müssen entsprechend den Konfigurationsregeln geschützt werden, die im *ES30 Expansion Shelf Hardware Guide* oder *DS60 Expansion Shelf Hardware Guide* angegeben werden. Mit DD Extended Retention können Sie deutlich mehr Speicher auf demselben Controller anhängen. Beispielsweise können Sie bis zu 56 ES30-Einschübe auf einem DD990 mit DD Extension Retention anhängen. Der aktive Tier muss den Speicher enthalten, der aus mindestens einem Einschub besteht. Die minimale und maximale Einschubkonfiguration für die Data Domain-Controllermodelle finden Sie in den Hardwareleitfäden für Erweiterungseinschübe für ES30 und DS60.

Datensicherheit
Auf einem DD-System mit aktivierter DD Extended Retention werden Daten mit integrierten Fehleridentifizierungsfunktionen, Disaster Recovery-Funktionen und DIA (Data Invulnerability Architecture) geschützt. DIA überprüft Daten, wenn sie vom aktiven in den Aufbewahrungs-Tier verschoben werden. Nachdem die Daten in den Aufbewahrungs-Tier kopiert wurden, werden die Container- und Dateisystemstrukturen ausgelesen und verifiziert. Der Speicherort der Datei wird aktualisiert und der Speicherplatz im aktiven Tier wird zurückgewonnen, nachdem überprüft wurde, um zu verifizieren, dass die Datei korrekt in den Aufbewahrungs-Tier geschrieben wurden.

Wenn eine Aufbewahrungseinheit voll ist, werden Namespace-Informationen und Systemdateien in die Einheit kopiert, sodass die Daten in der Aufbewahrungseinheit auch dann wiederhergestellt werden, wenn andere Teile des Systems ausgefallen sind.

Hinweis

Die Bereinigung und einige Replikationsformen werden auf DD-Systemen mit aktivierter DD Extended Retention nicht unterstützt.

Speicherplatzrückgewinnung
Um Speicherplatz zurückzugewinnen, der durch die Verschiebung der Daten in den Aufbewahrungs-Tier freigegeben wurde, können Sie die *Speicherplatzgewinnung* (ab DD OS 5.3) verwenden, die im Hintergrund als Aktivität mit niedriger Priorität ausgeführt wird. Die Funktion unterbricht sich selbst, wenn Aktivitäten mit höherer Priorität vorhanden sind, wie der Datenverschiebung und Bereinigung.

Data-at-Rest-Verschlüsselung
Ab DD OS 5.5.1 können Sie die *Data-at-Rest-Verschlüsselung* für DD-Systeme mit aktivierter DD Extended Retention verwenden, wenn Sie über eine Verschlüsselungslizenz verfügen. Verschlüsselung ist nicht standardmäßig aktiviert.

Hierbei handelt es sich um eine Erweiterung der bereits vor DD OS 5.5.1 verfügbaren Verschlüsselungsfunktion für Systeme, die DD Extended Retention nicht verwenden.

Umfassende Anweisungen zur Einrichtung und Nutzung der Verschlüsselungsfunktion finden Sie im Kapitel zum *Verwalten der Data-at-Rest-Verschlüsselung* in diesem Handbuch.

Unterstützte Protokolle bei DD Extended Retention

DD-Systeme mit aktivierter DD Extended Retention unterstützen die Protokolle NFS, CIFS und DD Boost. Unterstützung für DD VTL wurde in DD OS 5.2 hinzugefügt und Unterstützung für NDMP wurde in DD OS 5.3 hinzugefügt.

Hinweis

Eine Liste der Anwendungen, die mit DD Boost unterstützt werden, finden Sie in der *DD Boost-Kompatibilitätsliste* auf der Onlinesupport-Website.

Wenn Sie DD Extended Retention verwenden, werden Daten zunächst im aktiven Tier platziert. Dateien werden in ihrer Gesamtheit in die Aufbewahrungseinheit im Aufbewahrungs-Tier verschoben, wie von Ihrer Datenverschiebungs-Policy angegeben. Alle Dateien werden im selben Namespace angezeigt. Daten müssen nicht partitioniert werden und Sie können das Dateisystem wie gewünscht erweitern.

Alle Daten sind für alle Benutzer sichtbar und alle Dateisystem-Metadaten befinden sich im aktiven Tier.

Der Kompromiss beim Verschieben von Daten vom aktiven in den Aufbewahrungs-Tier ist mehr Kapazität im Vergleich zu einer langsameren Zugriffszeit, wenn die aufzurufende Einheit derzeit nicht für den Zugriff vorbereitet ist.

HA und Extended Retention

Data Domain-Systeme mit HA unterstützen nicht DD Extended Retention.
DD OS unterstützt Extended Retention mit HA aktuell nicht.

Verwenden von DD Replicator mit DD Extended Retention

Einige Replikationsformen werden auf DD-Systemen mit aktivierter DD Extended Retention unterstützt.

Die unterstützten Replikationstypen hängen von den zu schützenden Daten ab:

- Um Daten auf einem System als *Quelle* zu schützen, unterstützt ein DD-System mit aktivierter DD Extended Retention Sammelreplikation, MTree-Replikation und DD Boost Managed File Replication.
- Um Daten von anderen Systemen als *Ziel* zu schützen, unterstützt ein DD-System mit aktivierter DD Extended Retention außer der Sammelreplikation, der MTree-Replikation und der DD Boost Managed File Replication auch die Verzeichnisreplikation.

Hinweis

Die Deltareplikation (Optimierung der niedrigen Bandbreite) wird von DD Extended Retention nicht unterstützt. Sie müssen die Deltareplikation in allen Kontexten deaktivieren, bevor Sie DD Extended Retention auf einem DD-System aktivieren.

Sammelreplikation mit DD Extended Retention

Die Sammelreplikation findet zwischen dem entsprechenden aktiven Tier und der Aufbewahrungseinheit der beiden DD-Systeme statt, bei denen DD Extended Retention aktiviert ist. Wenn der aktive Tier oder die Aufbewahrungseinheit an der Quelle ausfällt, können die Daten von der entsprechenden Einheit am Remotestandort in eine neue Einheit kopiert werden, die als Ersatzeinheit an Ihren Standort geliefert wird.

Die Voraussetzungen für die Einrichtung der Sammelreplikation umfassen Folgendes:

- Quell- und Zielsysteme müssen als DD-Systeme konfiguriert werden, auf denen DD Extended Retention aktiviert ist.
- Das Dateisystem des Ziels darf erst aktiviert werden, wenn ihm die Aufbewahrungseinheit hinzugefügt und die Replikation konfiguriert wurde.

Verzeichnisreplikation mit DD Extended Retention

Bei der Verzeichnisreplikation dient ein DD Extended Retention-fähiges DD-System als Replikationsziel und unterstützt 1:1- und n:1-Topologien von allen unterstützten DD-Systemen. DD Extended Retention-fähige DD-Systeme unterstützen jedoch keine bidirektionale Verzeichnisreplikation und können keine *Quelle* der Verzeichnisreplikation sein.

Hinweis

Um Daten mithilfe der Verzeichnisreplikation in ein DD Extended Retention-fähiges DD-System zu kopieren, muss die Quelle DD OS 5.0 oder höher ausführen. Aus diesem Grund müssen Sie auf Systemen mit DD OS 5.0 oder früher zunächst die Daten in ein Transitsystem mit DD OS 5.0 oder höher importieren. Beispielsweise kann die Replikation von einem Extended Retention-fähigen System mit DD OS 4.9 in ein nicht Extended Retention-fähiges System mit DD OS 5.2 durchgeführt werden. Anschließend kann die Replikation vom DD OS 5.2-System in das DD OS 4.9-System vorgenommen werden.

MTree-Replikation mit DD Extended Retention

Sie können zwischen zwei DD-Systemen mit aktivierter DD Extended Retention eine MTree-Replikation einrichten. Replizierte Daten werden zuerst im aktiven Tier auf dem Zielsystem gespeichert. Die Datenverschiebungs-Policy auf dem Zielsystem legt dann fest, wann die replizierten Daten auf den Aufbewahrungs-Tier verschoben werden.

Beachten Sie, dass Einschränkungen und Policies der MTree-Replikation der verschiedenen DD OS-Versionen wie folgt variieren:

- Ab Version DD OS 5.1 können Daten mithilfe der MTree-Replikation von einem System ohne aktivierte DD Extended Retention auf ein System mit aktivierter DD Extended Retention repliziert werden.

- Ab Version DD OS 5.2 können Daten in einem aktiven Tier geschützt werden, indem sie auf den aktiven Tier eines Systems mit aktivierter DD Extended Retention repliziert werden.
- Ab Version DD OS 5.5 wird die MTree-Replikation von Systemen mit aktivierter DD Extended Retention auf Systeme ohne aktivierte DD Extended Retention unterstützt, wenn auf beiden Systemen DD OS 5.5 oder höher ausgeführt wird.
- Version DD OS 5.3 und 5.4: Wenn Sie die Aktivierung von DD Extended Retention planen, richten Sie auf der Quellmaschine keine Replikation für den MTree „/backup“ ein. (Versionen DD OS 5.5 und höher haben diese Beschränkung nicht.)

Managed File Replication mit DD Extended Retention

DD Extended Retention-fähige DD-Systeme unterstützen für DD Boost Managed File Replication folgende Topologien: 1:1, n:1, bidirektional und kaskadiert.

Hinweis

Für DD Boost 2.3 oder höher können Sie angeben, wie mehrere Kopien innerhalb der Backupanwendung erstellt und gemanagt werden sollen.

Hardware und Lizenzierung für DD Extended Retention

Für DD-Systeme mit aktivierter DD Extended Retention sind bestimmte Hardwarekonfigurationen erforderlich. Die Lizenzierung, insbesondere Kapazitätslizenzen für separate Einschübe, erfolgt ebenfalls spezifisch für diese Funktion.

Unterstützte Hardware für DD Extended Retention

Die Hardwareanforderungen für DD Extended Retention-fähige DD-Systeme umfassen Speicheranforderungen, Einschübe, NIC- und FC-Karten usw. Details zu den erforderlichen Hardwarekonfigurationen für DD Extended Retention finden Sie im Installations- und Konfigurationshandbuch für Ihr DD-System und den Hardwareleitfäden für die entsprechenden Erweiterungseinschübe.

Die folgenden DD-Systeme unterstützen DD Extended Retention:

DD860

- 72 GB RAM
- 1 NVRAM-IO-Modul (1 GB)
- 3 Quad-Port-SAS-IO-Module
- 2 1-GbE-Ports auf der Hauptplatine
- 0 bis 2 1/10-GbE-NIC-I/O-Karten für externe Verbindungen
- 0 bis 2 FC-HBA-IO-Karten mit zwei Ports für externe Verbindungen
- 0 bis 2 kombinierte NIC- und FC-Karten
- 1 bis 24 ES20- oder ES30-Einschübe (1-TB- oder 2-TB-Festplatten), die die maximal nutzbare Kapazität des Systems von 142 TB nicht überschreiten

Wenn DD Extended Retention auf einem DD860 aktiviert ist, ist die maximal nutzbare Speicherkapazität eines aktiven Tier 142 TB. Der Aufbewahrungs-Tier kann über eine maximal nutzbare Kapazität von 142 TB verfügen. Der aktive und der Aufbewahrungs-Tier haben eine nutzbare Gesamtspeicherkapazität von 284 TB.

DD990

- 256 GB RAM
- 1 NVRAM-IO-Modul (2 GB)
- 4 Quad-Port-SAS-IO-Module
- 2 1-GbE-Ports auf der Hauptplatine
- 0 bis 4 1-GbE-NIC-I/O-Karten für externe Verbindungen
- 0 bis 3 10-GbE-NIC-Karten für externe Verbindungen
- 0 bis 3 FC-HBA-IO-Karten mit zwei Ports für externe Verbindungen
- 0 bis 3 kombinierte NIC- und FC-Karten, nicht mehr als drei pro einem bestimmten I/O-Modul
- 1 bis 56 ES20- oder ES30-Einschübe (1-TB-, 2-TB- oder 3-TB-Festplatten), die die maximal nutzbare Kapazität des Systems von 570 TB nicht überschreiten

Wenn DD Extended Retention auf einem DD990 aktiviert ist, ist die maximal nutzbare Speicherkapazität eines aktiven Tier 570 TB. Der Aufbewahrungs-Tier kann über eine maximal nutzbare Kapazität von 570 TB verfügen. Der aktive und der Aufbewahrungs-Tier haben eine nutzbare Gesamtspeicherkapazität von 1140 TB.

DD4200

- 128 GB RAM
- 1 NVRAM-IO-Modul (4 GB)
- 4 Quad-Port-SAS-IO-Module
- 1 1-GbE-Port auf der Hauptplatine
- 0 bis 6 1/10-GbE-NIC-Karten für externe Verbindungen
- 0 bis 6 FC-HBA-IO-Karten mit zwei Ports für externe Verbindungen
- 0 bis 6 kombinierte NIC- und FC-Karten, nicht mehr als vier pro einem bestimmten I/O-Modul
- 1 bis 16 ES30-SAS-Einschübe (2-TB- oder 3-TB-Festplatten), die die maximal nutzbare Kapazität des Systems von 192 TB nicht überschreiten ES30-SATA-Einschübe (1-, 2- oder 3 TB-Festplatten) werden für Systemcontrollerupgrades unterstützt.

Wenn DD Extended Retention auf einem DD4200 aktiviert ist, ist die maximal nutzbare Speicherkapazität eines aktiven Tier 192 TB. Der Aufbewahrungs-Tier kann über eine maximal nutzbare Kapazität von 192 TB verfügen. Der aktive und der Aufbewahrungs-Tier haben eine nutzbare Gesamtspeicherkapazität von 384 TB. Externe Verbindungen werden für DD Extended Retention-Konfigurationen bis zu 16 Einschüben unterstützt.

DD4500

- 192 GB RAM
- 1 NVRAM-IO-Modul (4 GB)
- 4 Quad-Port-SAS-IO-Module
- 1 1-GbE-Port auf der Hauptplatine
- 0 bis 6 1/10-GbE-NIC-I/O-Karten für externe Verbindungen
- 0 bis 6 FC-HBA-IO-Karten mit zwei Ports für externe Verbindungen
- 0 bis 5 kombinierte NIC- und FC-Karten, nicht mehr als vier pro einem bestimmten I/O-Modul

- 1 bis 20 ES30-SAS-Einschübe (2-TB- oder 3-TB-Festplatten), die die maximal nutzbare Kapazität des Systems von 285 TB nicht überschreiten ES30-SATA-Einschübe (1-TB-, 2-TB- oder 3 TB-Festplatten) werden für Systemcontrollerupgrades unterstützt.

Wenn DD Extended Retention auf einem DD4500 aktiviert ist, ist die maximal nutzbare Speicherkapazität eines aktiven Tier 285 TB. Der Aufbewahrungs-Tier kann über eine maximal nutzbare Kapazität von 285 TB verfügen. Der aktive und der Aufbewahrungs-Tier haben eine nutzbare Gesamtspeicherkapazität von 570 TB. Externe Verbindungen werden für DD Extended Retention-Konfigurationen mit bis zu 24 Einschüben unterstützt.

DD6800

- 192 GB RAM
- 1 NVRAM-IO-Modul (8 GB)
- 3 Quad-Port-SAS-IO-Module
- 1 1-GbE-Port auf der Hauptplatine
- 0 bis 4 1/10-GbE-NIC-Karten für externe Verbindungen
- 0 bis 4 FC-HBA-IO-Karten mit zwei Ports für externe Verbindungen
- 0 bis 4 kombinierte NIC- und FC-Karten
- Einschubkombinationen sind im Installations- und Konfigurationshandbuch für Ihr DD-System und den Hardwareleitfäden für die entsprechenden Erweiterungseinschübe dokumentiert.

Wenn DD Extended Retention auf einem DD6800 aktiviert ist, ist die maximal nutzbare Speicherkapazität eines aktiven Tier 288 TB. Der Aufbewahrungs-Tier kann über eine maximal nutzbare Kapazität von 288 TB verfügen. Der aktive und der Aufbewahrungs-Tier haben eine nutzbare Gesamtspeicherkapazität von 0,6 PB. Externe Verbindungen werden für DD Extended Retention-Konfigurationen bis zu 28 Einschüben unterstützt.

DD7200

- 256 GB RAM
- 1 NVRAM-IO-Modul (4 GB)
- 4 Quad-Port-SAS-IO-Module
- 1 1-GbE-Port auf der Hauptplatine
- 0 bis 6 1/10-GbE-NIC-Karten für externe Verbindungen
- 0 bis 6 FC-HBA-IO-Karten mit zwei Ports für externe Verbindungen
- 0 bis 5 kombinierte NIC- und FC-Karten, nicht mehr als vier pro einem bestimmten I/O-Modul
- 1 bis 20 ES30-SAS-Einschübe (2-TB- oder 3-TB-Festplatten), die die maximal nutzbare Kapazität des Systems von 432 TB nicht überschreiten ES30-SATA-Einschübe (1-TB-, 2-TB- oder 3 TB-Festplatten) werden für Systemcontrollerupgrades unterstützt.

Wenn DD Extended Retention auf einem DD7200 aktiviert ist, ist die maximal nutzbare Speicherkapazität eines aktiven Tier 432 TB. Der Aufbewahrungs-Tier kann über eine maximal nutzbare Kapazität von 432 TB verfügen. Der aktive und der Aufbewahrungs-Tier haben eine nutzbare Gesamtspeicherkapazität von 864 TB. Externe Verbindungen werden für DD Extended Retention-Konfigurationen bis zu 32 Einschüben unterstützt.

DD9300

- 384 GB RAM
- 1 NVRAM-IO-Modul (8 GB)
- 3 Quad-Port-SAS-IO-Module
- 1 1-GbE-Port auf der Hauptplatine
- 0 bis 4 1/10-GbE-NIC-Karten für externe Verbindungen
- 0 bis 4 FC-HBA-IO-Karten mit zwei Ports für externe Verbindungen
- 0 bis 4 kombinierte NIC- und FC-Karten
- Einschubkombinationen sind im Installations- und Konfigurationshandbuch für Ihr DD-System und den Hardwareleitfäden für die entsprechenden Erweiterungseinschübe dokumentiert.

Wenn DD Extended Retention auf einem DD9300 aktiviert ist, ist die maximal nutzbare Speicherkapazität eines aktiven Tier 720 TB. Der Aufbewahrungs-Tier kann über eine maximal nutzbare Kapazität von 720 TB verfügen. Der aktive und der Aufbewahrungs-Tier haben eine nutzbare Gesamtspeicherkapazität von 1,4 PB. Externe Verbindungen werden für DD Extended Retention-Konfigurationen bis zu 28 Einschüben unterstützt.

DD9500

- 512 GB RAM
- 1 NVRAM-IO-Modul (8 GB)
- 4 Quad-Port-SAS-IO-Module
- 1 1-GbE-Quad-Port auf der Hauptplatine
- 0 bis 4 10-GbE-NIC-Karten für externe Verbindungen
- 0 bis 4 16-GbE-FC-HBA-Karten mit zwei Ports für externe Verbindungen
- Einschubkombinationen sind im Installations- und Konfigurationshandbuch für Ihr DD-System und den Hardwareleitfäden für die entsprechenden Erweiterungseinschübe dokumentiert.

Wenn DD Extended Retention auf einem DD9500 aktiviert ist, ist die maximal nutzbare Speicherkapazität eines aktiven Tier 864 TB. Der Aufbewahrungs-Tier kann über eine maximal nutzbare Kapazität von 864 TB verfügen. Der aktive und der Aufbewahrungs-Tier haben eine nutzbare Gesamtspeicherkapazität von 1,7 PB. Externe Verbindungen werden für DD Extended Retention-Konfigurationen bis zu 56 Einschüben unterstützt.

DD9800

- 768 GB RAM
- 1 NVRAM-IO-Modul (8 GB)
- 4 Quad-Port-SAS-IO-Module
- 1 1-GbE-Quad-Port auf der Hauptplatine
- 0 bis 4 10-GbE-NIC-Karten für externe Verbindungen
- 0 bis 4 16-GbE-FC-HBA-Karten mit zwei Ports für externe Verbindungen
- Einschubkombinationen sind im Installations- und Konfigurationshandbuch für Ihr DD-System und den Hardwareleitfäden für die entsprechenden Erweiterungseinschübe dokumentiert.

Wenn DD Extended Retention auf einem DD9800 aktiviert ist, ist die maximal nutzbare Speicherkapazität eines aktiven Tier 1.008 TB. Der Aufbewahrungs-Tier kann über eine maximal nutzbare Kapazität von 1.008 TB verfügen. Der aktive und der Aufbewahrungs-Tier haben eine nutzbare Gesamtspeicherkapazität von 2,0 PB.

Externe Verbindungen werden für DD Extended Retention-Konfigurationen bis zu 56 Einschüben unterstützt.

Lizenzierung für DD Extended Retention

DD Extended Retention ist eine lizenzierte Softwareoption, die auf einem unterstützten DD-System installiert ist.

Eine separate Kapazitätslizenz für Einschübe ist für jeden Speichereinschub für Einschübe erforderlich, die sowohl im aktiven als auch im Aufbewahrungs-Tier installiert werden. Kapazitätslizenzen für Einschübe gelten spezifisch für die Einschübe des aktiven oder des Aufbewahrungs-Tier.

Eine Expanded-Storage-Lizenz ist zur Erweiterung der Speicherkapazität des aktiven Tier über die ursprüngliche Kapazität hinaus erforderlich, die je nach Data Domain-Modell unterschiedlich ist. Sie können den zusätzlichen Speicher erst verwenden, wenn Sie die entsprechenden Lizenzen angewendet haben.

Hinzufügen von Kapazitätslizenzen für Einschübe für DD Extended Retention

Für jeden Einschub eines DD-Systems mit DD Extended Retention ist eine separate Lizenz erforderlich.

Vorgehensweise

1. Wählen Sie **Administration** > **Licenses**.
2. Klicken Sie auf **Add Licenses**.
3. Geben Sie eine oder mehrere Lizenzen, jeweils eine pro Zeile, ein und drücken Sie nach jeder Lizenz die Eingabetaste. Klicken Sie auf **Add**, wenn Sie fertig sind. Wenn Fehler auftreten, wird eine Zusammenfassung der hinzugefügten Lizenzen angezeigt, in der die Lizenzen aufgeführt sind, die aufgrund des Fehlers nicht hinzugefügt werden konnten. Wählen Sie den fehlerhaften Lizenzschlüssel aus, um ihn zu korrigieren.

Ergebnisse

Die Lizenzen für das DD-System werden in zwei Gruppen angezeigt:

- Softwareoptionslizenzen, die für Optionen wie DD Extended Retention und DD Boost erforderlich sind.
- Kapazitätslizenzen für Einschübe, die die Einschubkapazität (in TiB), das Einschubmodell (z. B. ES30) und den Storage Tier des Einschubs (aktiver oder Aufbewahrungs-Tier) anzeigen.

Um eine Lizenz zu löschen, wählen Sie die Lizenz aus der Liste "Licenses" aus und klicken Sie auf **Delete Selected Licenses**. Wenn Sie zum Bestätigen aufgefordert werden, lesen Sie die Warnung und klicken Sie auf **OK**, um fortzufahren.

Konfigurieren von Speicher für DD Extended Retention

Für zusätzlichen Speicher für DD Extended Retention sind entsprechende Lizenzen erforderlich. Außerdem muss ausreichend Arbeitsspeicher auf dem DD-System installiert sein, um DD Extended Retention zu unterstützen. Es werden Fehlermeldungen angezeigt, wenn mehr Lizenzen oder Arbeitsspeicher benötigt werden.

Vorgehensweise

1. Wählen Sie die Registerkarte **Hardware** > **Storage** aus.

2. Wählen Sie auf der Registerkarte „Overview“ die Option **Configure Storage** aus.
3. Wählen Sie auf der Registerkarte „Configure Storage“ den hinzuzufügenden Speicher aus der Liste „Addable Storage“ aus.
4. Wählen Sie die entsprechende Tier-Konfiguration (**Active** oder **Retention**) aus dem Menü aus. Der aktive Tier entspricht einem DD-Standardsystem und sollte ähnlich dimensioniert werden. Die maximale Speichermenge, die zum aktiven Tier hinzugefügt werden kann, hängt vom verwendeten DD-Controller ab.
5. Aktivieren Sie das Kontrollkästchen für den Einschub, der hinzugefügt werden soll.
6. Klicken Sie auf die Schaltfläche **Add to Tier**.
7. Klicken Sie auf **OK**, um den Speicher hinzuzufügen.
8. Um einen hinzugefügten Einschub zu entfernen, wählen Sie diesen aus der Liste „Tier Configuration“ aus, wählen Sie anschließend die Option **Remove from Tier** aus und klicken Sie auf **OK**.

Vom Kunden bereitgestellte Infrastruktur für DD Extended Retention

Damit Sie DD Extended Retention aktivieren können, müssen Umgebung und Konfiguration bestimmte Anforderungen erfüllen.

- **Spezifikationen, Standortanforderungen, Rackstellfläche und Verkabelung**: Weitere Informationen finden Sie im *Data Domain Installation and Setup Guide* für das entsprechende DD-Systemmodell.
- **Rackaufbau und Verkabelung**: Es wird empfohlen, beim Aufbau des Systems im Rack eine spätere Erweiterung einzuplanen. Alle Einschübe sind mit einem einzigen DD-System verbunden.

  Hinweis

  - Im *Data Domain Expansion Shelf Hardware Guide* für Ihr Einschubmodell (ES20, ES30 oder DS60) erhalten Sie weitere Informationen.

Managen von DD Extended Retention

Für die Einrichtung und Verwendung von DD Extended Retention auf einem DD-System können Sie DD System Manager und/oder die DD-CLI verwenden.

- DD System Manager, zuvor bekannt als Enterprise Manager, ist eine GUI (grafische Benutzeroberfläche), die in diesem Handbuch beschrieben wird.
- Die `archive`-Befehle, die in der DD-CLI (Befehlszeilenoberfläche) eingegeben werden, werden im *Data Domain Operating System Command Reference Guide* beschrieben.

Der einzige Befehl, der bei Verwendung von DD System Manager nicht verfügbar ist, ist der Befehl `archive report`.

Aktivieren von DD-Systemen für DD Extended Retention

Bevor Sie ein DD-System für DD Extended Retention verwenden, muss die richtige Lizenz installiert und das korrekte Dateisystem eingerichtet sein.

Vorgehensweise

1. Vergewissern Sie sich, dass die richtige Lizenz angewendet wurde. Wählen Sie **Administration** > **Licenses**, und prüfen Sie die Liste "Feature Licenses" auf "Extended Retention".
2. Wählen Sie **Data Management** > **File System** > **More Tasks** > **Enable DD Extended Retention**.

   Diese Option ist nur verfügbar, wenn Ihr Data Domain-System DD Extended Retention unterstützt und das Dateisystem noch nicht für DD Extended Retention konfiguriert wurde. Sie sollten wissen, dass DD Extended Retention nach der Aktivierung nicht deaktiviert werden kann, ohne das Dateisystem zu entfernen.

   a. Wenn das Dateisystem bereits aktiviert ist (als System ohne DD Extended Retention), werden Sie aufgefordert, es zu deaktivieren. Klicken Sie hierfür auf **Disable**.

   b. Wenn Sie zur Bestätigung aufgefordert werden, dass Sie das Dateisystem für die Verwendung von DD Extended Retention konvertieren möchten, klicken Sie auf **OK**.

      Nachdem ein Dateisystem in ein DD Extended Retention-Dateisystem konvertiert wurde, wird die Dateisystemseite aktualisiert, um Informationen über beide Tiers darzustellen. Außerdem gibt es eine neue Registerkarte mit der Bezeichnung **Retention Units**.

      #### CLI-Entsprechung

      Über die Befehlszeilenoberfläche können Sie auch prüfen, ob die Extended Retention-Lizenz installiert wurde.

      So verwenden Sie die Legacy-Lizenzierungsmethode:

      ```
      # license show
      ## License Key                   Feature
      --    --------------------       -----------
      1     AAAA-BBBB-CCCC-DDDD        Replication
      2     EEEE-FFFF-GGGG-HHHH        VTL
      --    --------------------       -----------
      ```

      Wenn keine Lizenz vorhanden ist, können Sie der Dokumentation zur jeweiligen Einheit (Übersichtskarte zur schnellen Installation) entnehmen, welche Lizenzen erworben wurden. Geben Sie den folgenden Befehl ein, um den Lizenzschlüssel anzugeben.

      ```
      # license add license-code
      ```

      Aktivieren Sie dann Extended Retention:

      ```
      # archive enable
      ```

      So verwenden Sie die elektronische Lizenzierung:

      ```
      # elicense show
      Feature licenses:
      ## Feature     Count Mode            Expiration Date
      -- ----------- ----- --------------- ---------------
      1  REPLICATION 1     permanent (int) n/a
      2  VTL         1     permanent (int) n/a
      -- ----------- ----- --------------- ---------------
      ```

      Wenn die Lizenz nicht vorhanden ist, aktualisieren Sie die Lizenzdatei mit der neuen Funktionslizenz.

```
# elicense update mylicense.lic
New licenses: Storage Migration
Feature licenses:
```

```
## Feature            Count   Mode             Expiration Date
-- -----------------  -----  ---------------  ---------------
1  REPLICATION        1      permanent (int)  n/a
2  VTL                1      permanent (int)  n/a
3  EXTENDED RETENTION 1      permanent (int)  n/a
-- ------------------ -----  ---------------  ---------------
** This will replace all existing Data Domain licenses on the system with the above
EMC ELMS licenses.
Do you want to proceed? (yes|no) [yes]: yes
eLicense(s) updated.
```

Aktivieren Sie dann Extended Retention:

```
# archive enable
```

Erstellen eines zweistufigen Dateisystems für DD Extended Retention

DD Extended Retention nutzt ein zweistufiges Dateisystem für den aktiven und den Aufbewahrungs-Tier. Auf dem DD-System muss DD Extended Retention aktiviert werden, bevor dieses spezielle Dateisystem aktiviert wird.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System**
2. Wenn ein Dateisystem vorhanden ist, löschen Sie es.
3. Wählen Sie **More Tasks** > **Create file system**.
4. Wählen Sie ein aufbewahrungsfähiges Dateisystem aus und klicken Sie auf **Next**.
5. Wählen Sie im Dialogfeld "File System Create" die Option **Configure** aus.

   Es muss Speicher konfiguriert werden, bevor das Dateisystem erstellt wird.
6. Verwenden Sie das Dialogfeld "Configure Storage", um verfügbaren Speicher zu den aktiven und Aufbewahrungs-Tiers hinzuzufügen und zu entfernen, und klicken Sie auf **OK**, wenn Sie fertig sind.

   Der Speicher in der aktiven Tier wird verwendet, um die aktive Dateisystem-Tier zu erstellen. Der Speicher in der Aufbewahrungs-Tier wird verwendet, um eine Aufbewahrungseinheit zu erstellen.

   Hinweis

   Ab DD OS 5.5.1 ist nur eine Aufbewahrungseinheit pro Aufbewahrungs-Tier zulässig. Vor DD OS 5.5.1 eingerichtete Systeme können zwar mehr als eine Aufbewahrungseinheit enthalten, Sie können ihnen jedoch keine weiteren Aufbewahrungseinheiten hinzufügen.
7. Verwenden Sie das Dialogfeld "File System Create" für Folgendes:
   a. Wählen Sie die Größe der Aufbewahrungseinheit aus der Drop-down-Liste aus.
   b. Wählen Sie die Option **Enable file system after creation**.
   c. Klicken Sie auf **Next**.

   Eine Zusammenfassungsseite zeigt die Größe des aktiven und des Aufbewahrungs-Tier im neuen Dateisystem an.
8. Klicken Sie auf **Finish**, um das Dateisystem zu erstellen.

Der Fortschritt der einzelnen Erstellungsschritte wird angezeigt und ein Fortschrittsbalken überwacht den allgemeinen Status.

9. Klicken Sie nach der Dateisystemausführung auf **OK**.

   CLI-Entsprechung
   Um zusätzliche Einschübe hinzuzufügen, verwenden Sie diesen Befehl einmal für jedes Gehäuse:

   ```
   # storage add tier archive enclosure 5
   ```

   Erstellen Sie eine Archiveinheit und fügen Sie sie dem Dateisystem hinzu. Sie werden aufgefordert, die Anzahl der Gehäuse in der Archiveinheit anzugeben:

   ```
   # filesys archive unit add
   ```

   Überprüfen Sie, ob die Archiveinheit erstellt und dem Dateisystem hinzugefügt wurde:

   ```
   # filesys archive unit list all
   ```

   Prüfen Sie das Dateisystem aus Sicht des Systems:

   ```
   # filesys show space
   ```

Bereich „File System“ für DD Extended Retention

Nachdem Sie ein DD-System für DD Extended Retention aktiviert haben, sieht der Bereich **Data Management** > **File System** etwas anders aus (im Vergleich zu einem System ohne DD Extended Retention).

- **State** zeigt, dass das Dateisystem aktiviert oder deaktiviert ist. Sie können den Status über die Schaltfläche „Disable/Enable“ direkt rechts daneben ändern.
- **Clean Status** zeigt die Zeit an, zu der der letzte Bereinigungsvorgang abgeschlossen wurde, oder den aktuellen Bereinigungsstatus, wenn der Bereinigungsvorgang derzeit ausgeführt wird. Wenn die Bereinigung ausgeführt werden kann, wird die Schaltfläche **Start Cleaning** angezeigt. Wenn die Bereinigung ausgeführt wird, ändert sich die Schaltfläche **Start Cleaning** in die Schaltfläche **Stop Cleaning**.
- **Data Movement Status** zeigt die Zeit an, zu der die letzte Datenverschiebung abgeschlossen wurde. Wenn eine Datenverschiebung ausgeführt werden kann, wird die Schaltfläche **Start** angezeigt. Wenn die Datenverschiebung ausgeführt wird, ändert sich die Schaltfläche **Start** in die Schaltfläche **Stop**.
- **Space Reclamation Status** zeigt die Menge des zurückgewonnenen Speicherplatzes nach dem Löschen von Daten im Aufbewahrungs-Tier. Wenn eine Speicherplatzrückgewinnung ausgeführt werden kann, wird die Schaltfläche **Start** angezeigt. Wenn sie bereits ausgeführt wird, werden die Schaltflächen**Stop** und **Suspend** angezeigt. Wenn die Speicherplatzrückgewinnung zuvor ausgeführt und angehalten wurde, werden die Schaltflächen **Stop** und **Resume** angezeigt. Es gibt außerdem eine Schaltfläche **More Information**, über die detaillierte Informationen zu Start- und Endzeiten, Abschlussprozentsatz, zurückgewonnenen Einheiten, freigegebenem Speicherplatz usw. angezeigt werden.
- Wenn Sie **More Tasks** > **Destroy** auswählen, können Sie alle Daten im Dateisystem einschließlich virtueller Bänder löschen. Dies kann nur von einem Systemadministrator durchgeführt werden.
- Wenn Sie **More Tasks** > **Fast Copy** auswählen, können Sie Dateien und MTrees eines Quellverzeichnisses an ein Zielverzeichnis klonen. Beachten Sie, dass Fastcopy für Systeme, auf denen DD Extended Retention aktiviert ist, keine Daten zwischen dem aktiven und dem Aufbewahrungs-Tier verschiebt.

- Durch Auswahl von **More Tasks** > **Expand Capacity** können Sie den aktiven oder den Aufbewahrungs-Tier erweitern.

Erweitern des aktiven oder des Aufbewahrungs-Tier

Wenn das Dateisystem aktiviert ist, können Sie entweder den aktiven oder den Aufbewahrungs-Tier erweitern.

So erweitern Sie die Tier **Active**:

Vorgehensweise

1. Wählen Sie **Data Management > File System > More Tasks > Expand Capacity**.
2. Wählen Sie im Dialogfeld "Expand File System Capacity" die Option **Active Tier** aus und klicken Sie auf **Next**.
3. Klicken Sie auf **Konfigurieren**.
4. Stellen Sie im Dialogfeld "Configure Storage" sicher, dass "Active Tier" als Auswahl zum Konfigurieren angezeigt wird, und klicken Sie auf **OK**.
5. Wenn die Konfiguration abgeschlossen ist, kehren Sie zurück zum Dialogfeld „File System Capacity“. Wählen Sie **Finish** aus, um die Erweiterung des aktiven Tier abzuschließen.

So erweitern Sie die Tier **retention**:

Vorgehensweise

1. Wählen Sie **Data Management > File System > More Tasks > Expand Capacity**.
2. Wählen Sie im Dialogfeld „Expand File System Capacity“ die Option **Retention Tier** und dann **Next**.
3. Wenn eine Aufbewahrungseinheit verfügbar ist, wird das Dialogfeld **Select Retention Unit** angezeigt. Wählen Sie die Aufbewahrungseinheit aus, die Sie erweitern möchten, und klicken Sie dann auf **Next**. Wenn keine Aufbewahrungseinheit verfügbar ist, wird das Dialogfeld **Create Retention Unit** angezeigt. In diesem Fall müssen Sie eine Aufbewahrungseinheit erstellen, bevor Sie fortfahren können.

   Hinweis

   Um eine optimale Performance für ein DD-System mit aktivierter DD Extended Retention-Option zu ermöglichen, sollten Sie den Aufbewahrungs-Tier immer in Schritten von mindestens zwei Einschüben erweitern. Außerdem sollten Sie nicht warten, bis die Aufbewahrungseinheit fast voll ist, bevor Sie diese erweitern.

4. Wählen Sie die Größe für die Erweiterung der Aufbewahrungseinheit aus und wählen Sie dann **Configure** aus.
5. Wenn die Konfiguration abgeschlossen ist, kehren Sie zurück zum Dialogfeld „File System Capacity“. Wählen Sie **Finish** aus, um die Erweiterung der Aufbewahrungs-Tier abzuschließen.

Rückgewinnen von Speicherplatz im Aufbewahrungs-Tier

Sie können Speicherplatz von gelöschten Daten im Aufbewahrungs-Tier zurückgewinnen, indem Sie die Speicherplatzrückgewinnung (eingeführt in DD

OS 5.3) ausführen. Die Speicherplatzrückgewinnung wird auch während der Dateisystembereinigung durchgeführt.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** aus. Direkt über den Registerkarten wird unter **Space Reclamation Status** die Menge des zurückgewonnenen Speicherplatzes nach dem Löschen der Daten im Aufbewahrungs-Tier angezeigt.
2. Wenn eine Speicherplatzrückgewinnung ausgeführt werden kann, wird die Schaltfläche **Start** angezeigt. Wenn sie bereits ausgeführt wird, werden die Schaltflächen**Stop** und **Suspend** angezeigt. Wenn die Speicherplatzrückgewinnung zuvor ausgeführt und angehalten wurde, werden die Schaltflächen **Stop** und **Resume** angezeigt.
3. Wählen Sie **More Information** aus, um Details zu Zyklusnamen, Start- und Endzeiten, effektiver Laufzeit, abgeschlossenen Prozent (bei Ausführung), zurückgewonnenen Einheiten, in der Zieleinheit freigegebenem Speicherplatz und insgesamt freigegebenem Speicherplatz anzuzeigen.

Hinweis

Wenn Sie den Befehl `archive space-reclamation` verwenden, führt das System eine Speicherplatzrückgewinnung im Hintergrund durch, bis sie manuell gestoppt wird, es sei denn, Sie verwenden die 1-Zyklus-Option. Sie können auch den Befehl `archive space-reclamation schedule set` verwenden, um die Startzeit für die Speicherplatzrückgewinnung festzulegen.

CLI-Entsprechung
So aktivieren Sie die Speicherrückgewinnung:

```
# archive space-reclamation start
```

So deaktivieren Sie die Speicherrückgewinnung:

```
# archive space-reclamation stop
```

So zeigen Sie den Status der Speicherrückgewinnung an:

```
# archive space-reclamation status-detailed
Space-reclamation will start when 'archive data-movement'
completes.

Previous Cycle:
---------------
Start time                 : Feb 21 2014 14:17
End time                   : Feb 21 2014 14:49
Effective run time         : 0   days, 00:32.
Percent completed          : 00 % (was stopped by user)
Units reclaimed            : None
Space freed on target unit : None
Total space freed          : None
```

Registerkarten „File System“ für DD Extended Retention

Nachdem Sie ein DD-System für DD Extended Retention aktiviert haben, sehen auch die Registerkarten **Data Management** > **File System** etwas anders aus (im Vergleich zu einem System ohne DD Extended Retention) und eine zusätzliche Registerkarte ist vorhanden: **Retention Units**

Registerkarte „Summary“
Auf der Registerkarte „Summary“ werden Informationen über die Speicherplatznutzung und Komprimierung für aktive und Aufbewahrungs-Tiers angezeigt.

Space Usage: Zeigt die Gesamtgröße, den belegten Speicherplatz und die Menge des verfügbaren Speicherplatzes sowie kombinierte Gesamtwerte für aktive und Aufbewahrungs-Tiers an. Die Menge des zu bereinigenden Speicherplatzes wird für den aktiven Tier dargestellt.

Active Tier and Retention Tier: Zeigt die Werte vor und nach der Komprimierung an, die derzeit verwendet werden, und die, die in den letzten 24 Stunden geschrieben wurden. Zeigt außerdem die globalen, lokalen und Gesamtkomprimierungsfaktoren (Reduzierungsprozentsatz) an.

Registerkarte „Retention Units“
Auf der Registerkarte „Retention Units“ werden die Aufbewahrungseinheiten angezeigt. Ab DD OS 5.5.1.4 ist nur eine Aufbewahrungseinheit pro Aufbewahrungs-Tier zulässig. Vor DD OS 5.5.1.4 eingerichtete Systeme können zwar mehr als eine Aufbewahrungseinheit enthalten, Sie können ihnen jedoch keine weiteren Aufbewahrungseinheiten hinzufügen.

Die folgenden Informationen werden angezeigt: der Status der Einheit (neu, leer, versiegelt, Ziel oder Bereinigung), der Status (deaktiviert, bereit oder Stand-by), das Startdatum (Datum der Verschiebung auf den Aufbewahrungs-Tier) und die Größe der Einheit. Die Einheit befindet sich im Bereinigungsstatus, wenn eine Speicherplatzrückgewinnung ausgeführt wird. Wenn die Einheit versiegelt wurde, was bedeutet, dass keine Daten mehr hinzugefügt werden können, wird die Option „Sealed Date“ bereitgestellt. Durch Aktivieren des Kontrollkästchens der Aufbewahrungseinheit werden zusätzliche Informationen (Größe, verwendet, verfügbar und zu bereinigen) im Bereich mit detaillierten Informationen angezeigt.

Es gibt zwei Schaltflächen: **Delete** (zum Löschen der Einheit) und **Expand** (zum Hinzufügen von Speicher zu einer Einheit). Die Einheit muss sich zum Erweitern in einem neuen oder einem Zielzustand befinden.

Registerkarte „Konfiguration“
Auf der Registerkarte „Configuration " können Sie Ihr System konfigurieren.

Wenn Sie die Schaltfläche zum **Bearbeiten** von Optionen auswählen, wird das Dialogfeld „Modify Settings“ angezeigt, in dem Sie den Typ für die lokale Komprimierung [Optionen sind „None“, „lz“ (Standard), „gz“ und „gzfast“] und die lokale Komprimierung für den Aufbewahrungs-Tier [Optionen sind „None“, „lz“, „gz“ (Standard) und „gzfast“] ändern und die Option „Report Replica Writable“ aktivieren können.

Wenn Sie die Schaltfläche zum **Bearbeiten** der Bereinigunsplanung auswählen, wird das Dialogfeld „Modify Schedule“ angezeigt, in dem Sie die Bereinigungsplanung und den Prozentsatz für die Drosselung ändern können.

Wenn Sie die Schaltfläche zum **Bearbeiten** der Datenverschiebungs-Policy auswählen, wird das Dialogfeld „Data Movement Policy“ angezeigt, indem Sie verschiedene Parameter festlegen können. „File Age Threshold“ ist ein systemweiter Standardwert, der für alle MTrees gilt, für die Sie keinen benutzerdefinierten Standardwert festgelegt haben. Der Mindestwert beträgt 14 Tage. Mithilfe der Option „Data Movement Schedule“ können Sie einrichten, wie häufig die Datenverschiebung ausgeführt wird. Die empfohlene Planung ist alle zwei Wochen. Mit der Option „File System Cleaning“ können Sie auswählen, dass ein System nach der Datenverschiebung nicht bereinigt wird. Es wird jedoch dringend empfohlen, diese Option ausgewählt zu lassen.

File Age Threshold per MTree Link
Wenn Sie den Link **File Age Threshold per MTree** auswählen, gelangen Sie vom Bereich „File System“ zum Bereich „MTree“ (auf den Sie auch über **Data Management** > **MTree** zugreifen können), in dem Sie einen benutzerdefinierten Schwellenwert für das Dateialter für jeden Ihrer MTrees festlegen können.

Wählen Sie den MTree und dann **Edit** neben „Data Movement Policy“ aus. Geben Sie im Dialogfeld „Modify Age Threshold“ einen neuen Wert für die Option „File Age Threshold“ ein und wählen Sie dann **OK**. Ab DD OS 5.5.1 beträgt der Mindestwert 14 Tage.

Registerkarte „Encryption“
Auf der Registerkarte „Encryption“ können Sie die Data-at-Rest-Verschlüsselung aktivieren oder deaktivieren, die nur für Systeme mit einer einzigen Aufbewahrungseinheit unterstützt wird. Ab Version 5.5.1 unterstützt DD Extended Retention nur eine einzige Aufbewahrungseinheit, sodass unter Version 5.5.1 oder höher eingerichtete Systeme diese Einschränkung problemlos einhalten. Systeme, die vor Version 5.5.1 eingerichtet wurden, können jedoch über mehr als eine Aufbewahrungseinheit verfügen. Diese können aber erst mit der Data-at-Rest-Verschlüsselung genutzt werden, bis alle Aufbewahrungseinheiten bis auf eine entfernt wurden oder Daten in eine Aufbewahrungseinheit verschoben oder migriert wurden.

Registerkarte „Space Usage“
Auf der Registerkarte „Space Usage“ können Sie einen von drei Diagrammtypen auswählen [(gesamtes) File System; Aktiv (Tier); Archiv (Tier)], um die Speicherplatznutzung über die Zeit in MIB anzuzeigen. Sie können im oberen rechten Bereich auch einen Wert für die Dauer (7, 30, 60 oder 120 Tage) auswählen. Die Daten werden (mit Farbcodierung) als vor der Komprimierung geschrieben (blau), nach der Komprimierung verwendet (rot) und mit dem Komprimierungsfaktor (schwarz) dargestellt.

Registerkarte „Consumption“
Auf der Registerkarte „Consumption“ können Sie einen von drei Diagrammtypen auswählen [(gesamtes) File System, Aktiv (Tier), Archiv (Tier)], um die Menge des verwendeten Speichers nach der Komprimierung und die Komprimierungsrate über die Zeit anzuzeigen, wodurch Sie Verbrauchstrends anzeigen können. Sie können im oberen rechten Bereich auch einen Wert für die Dauer (7, 30, 60 oder 120 Tage) auswählen. Über das Kontrollkästchen „Capacity“ können Sie auswählen, ob der Speicher nach der Komprimierung im Vergleich zur Gesamtsystemkapazität angezeigt werden soll.

Registerkarte „Daily Written“
Auf der Registerkarte „Daily Written“ können Sie eine Dauer (7, 30, 60 oder 120 Tage) auswählen, um die Menge der pro Tag geschriebenen Daten anzuzeigen. Die Daten werden (mit Farbcodierung) im Diagramm- und Tabellenformat als vor der Komprimierung geschrieben (blau), nach der Komprimierung verwendet (rot) und mit dem Komprimierungsfaktor (schwarz) dargestellt.

Erweitern einer Aufbewahrungseinheit

Um eine optimale Performance zu ermöglichen, warten Sie nicht, bis eine Aufbewahrungseinheit fast voll ist, bevor Sie sie erweitern und erweitern Sie sie nicht in Schritten von einem Gehäuse. Speicher kann nicht vom aktiven Tier in den Aufbewahrungs-Tier verschoben werden, nachdem das Dateisystem erstellt wurde. Nur ungenutzte Gehäuse können dem Aufbewahrungs-Tier hinzugefügt werden.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Retention Units**.
2. Wählen Sie die Aufbewahrungseinheit aus.

   Beachten Sie Folgendes: Wenn eine Bereinigung ausgeführt wird, kann keine Aufbewahrungseinheit erweitert werden.
3. Klicken Sie auf **Expand**.

   Das System zeigt die aktuelle Größe der Aufbewahrungs-Tier, eine geschätzte Erweiterungsgröße und eine erweiterte Gesamtkapazität an. Wenn zusätzlicher Speicher verfügbar ist, können Sie auf den Link "Configure" klicken.
4. Klicken Sie auf **Next**.

   Das System zeigt eine Warnung an, dass Sie das Dateisystem nach diesem Vorgang nicht auf die ursprüngliche Größe zurücksetzen können.
5. Klicken Sie auf **Expand**, um das Dateisystem zu erweitern.

Löschen einer Aufbewahrungseinheit

Wenn alle Dateien in einer Aufbewahrungseinheit nicht mehr benötigt werden, führt das Löschen der Dateien dazu, dass die Einheit zur Wiederverwendung verfügbar ist. Sie können einen Dateistandortbericht erzeugen, um sicherzustellen, dass die Aufbewahrungseinheit tatsächlich leer ist, die Aufbewahrungseinheit löschen und sie dann als neue Aufbewahrungseinheit hinzufügen.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** und klicken Sie auf **Disable**, um das Dateisystem zu deaktivieren, wenn es ausgeführt wird.
2. Wählen Sie **Data Management** > **File System** > **Retention Units**.
3. Wählen Sie die Aufbewahrungseinheit aus.
4. Klicken Sie auf **Delete**.

Ändern der lokalen Komprimierung der Aufbewahrungs-Tiers

Sie können den lokalen Komprimierungsalgorithmus für eine nachfolgende Datenverschiebung zum Aufbewahrungs-Tier ändern.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Configuration** aus.
2. Klicken Sie auf **Edit** rechts neben **Options**.
3. Wählen Sie eine der Komprimierungsoptionen aus dem Menü "Retention Tier Local Comp" aus und klicken Sie auf **OK**.

   Der Standard ist „gz“, eine Komprimierung im Zip-Stil, bei der die geringste Menge an Speicherplatz für Daten verwendet wird (durchschnittlich 10 % bis 20 % weniger als „lz“; wobei einige Datasets jedoch eine sehr viel höhere Komprimierung erzielen).

Verstehen der Datenverschiebungs-Policies

Eine Datei wird basierend auf dem Datum, an dem sie das letzte Mal geändert wurde, aus dem aktiven in den Aufbewahrungs-Tier verschoben. Für die Integrität der Daten wird zu diesem Zeitpunkt die gesamte Datei verschoben. Die *Datenverschiebungs-Policy* legt zwei Dinge fest: einen *Schwellenwert für das Alter von Dateien* und eine *Planung für die Datenverschiebung*. Wenn die Daten sich nicht während des Zeitraums

geändert haben, der durch den Schwellenwert für das Alter von Dateien festgelegt ist, werden sie an dem Datum aus dem aktiven in den Aufbewahrungs-Tier verschoben, das durch die Planung für die Datenverschiebung festgelegt ist.

Hinweis

Ab DD OS 5.5.1 muss der Schwellenwert für das Alter von Dateien mindestens 14 Tage betragen.

Sie können verschiedene Schwellenwerte für das Alter von Dateien für jeden definierten MTree angeben. Ein MTree ist eine Unterstruktur innerhalb des Namespace, der eine logische Datenmenge für Managementzwecke ist. Sie können beispielsweise Finanzdaten, E-Mails und technische Daten in separaten MTrees ablegen.

Um die Funktion zur *Speicherplatzrückgewinnung* zu nutzen, wird ab DD OS 5.3 empfohlen, dass Sie die Datenverschiebung und Dateisystembereinigung alle 14 Tage planen. Standardmäßig wird die Bereinigung immer ausgeführt, nachdem die Datenverschiebung abgeschlossen ist. Sie sollten diesen Standard auf keinen Fall ändern.

Vermeiden Sie die folgenden häufigen Dimensionierungsfehler:

- Festlegen einer Datenverschiebungs-Policy, die sehr aggressiv ist; Daten werden zu früh verschoben.
- Festlegen einer Datenverschiebungs-Policy, die zu konservativ ist: Wenn der aktive Tier voll ist, können Sie keine Daten mehr auf das System schreiben.
- Vorhalten eines zu kleinen aktiven Tier und dann Überkompensierung durch eine extrem aggressive Datenverschiebungs-Policy.

Beachten Sie die folgenden Einschränkungen, die mit Snapshot- und Dateisystembereinigung verbunden sind:

- Dateien in Snapshots werden selbst dann nicht bereinigt, wenn sie in den Aufbewahrungs-Tier verschoben wurden. Speicherplatz kann nicht zurückgewonnen werden, bis die Snapshots gelöscht wurden.
- Es empfiehlt sich, einen Schwellenwert für das Alter von Dateien für Snapshots auf mindestens 14 Tagen festzulegen.

Es folgen zwei Beispiele für die Einrichtung einer Datenverschiebungs-Policy.

- Sie können Daten mit verschiedenen Änderungsgraden in zwei unterschiedliche MTrees trennen und den Schwellenwert für das Alter von Dateien so festlegen, dass Daten bald verschoben werden, nachdem die Daten stabilisiert sind. Erstellen Sie MTree A für tägliche inkrementelle Backups und MTree B für wöchentliche vollständige Backups. Legen Sie den „File Age Threshold“ für MTree A so fest, dass seine Daten *nie* verschoben werden, legen Sie aber den „File Age Threshold“ MTree B auf 14 Tage fest (den minimalen Schwellenwert).
- Bei Daten, die nicht in unterschiedlichen MTrees getrennt werden können, können Sie Folgendes tun. Nehmen wir an, dass die Aufbewahrungsfrist von täglichen inkrementellen Backups acht Wochen beträgt und die Aufbewahrungsfrist für wöchentliche vollständige Backups drei Jahre. In diesem Fall wäre es ratsam, den Schwellenwert für das Alter von Dateien auf neun Wochen festzulegen. Wenn er niedriger festgelegt würde, würden Sie tägliche inkrementelle Daten verschieben, die tatsächlich bald gelöscht werden sollen.

Ändern der Datenverschiebungs-Policy

Sie können verschiedene Datenverschiebungs-Policies für jeden MTree festlegen.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Configuration**.
2. Wählen Sie **Edit** rechts von **Data Movement Policy** aus.
3. Geben Sie im Dialogfeld „Data Movement Policy“ den systemweiten Wert für „File Age Threshold“ in der Anzahl der Tage an. Ab DD OS 5.5.1 muss dieser Wert mindestens 14 Tage betragen. Dieser Wert gilt für neu erstellte MTrees und MTrees, denen noch kein Altersschwellenwert per MTree mit dem Link **File Age Threshold per MTree** zugewiesen wurde (siehe Schritt 7). Wenn die Datenverschiebung beginnt, werden alle Dateien, die nicht in der im Schwellenwert angegebenen Anzahl von Tagen geändert wurden, aus dem aktiven in den Aufbewahrungs-Tier verschoben.
4. Geben Sie eine Planung für die Datenverschiebung ein, geben Sie also an, wann die Datenverschiebung stattfinden sollte, beispielsweise täglich, wöchentlich, alle 14 Tage, monatlich oder am letzten Tag des Monats. Sie können auch einen bestimmten Tag oder bestimmte Tage und die Zeit in Stunden und Minuten auswählen. Es wird nachdrücklich empfohlen , dass Sie die Datenverschiebung und Dateisystembereinigung alle 14 Tage planen, um die Funktion zur Speicherplatzrückgewinnung zu nutzen (eingeführt in DD OS 5.3).
5. Geben Sie eine Datenverschiebungsdrosselung an, das heißt, den Prozentsatz an verfügbaren Ressourcen, die das System für die Datenverschiebung verwendet. Ein Wert von 100 % gibt an, dass die Datenverschiebung nicht gedrosselt wird.
6. Standardmäßig wird die Dateisystembereinigung immer ausgeführt, nachdem die Datenverschiebung abgeschlossen ist. Es wird dringend empfohlen, dass Sie **Start file system clean after Data Movement** ausgewählt lassen.
7. Wählen Sie „OK“ aus.
8. Zurück auf der Registerkarte „Configuration“ können Sie Altersschwellenwerte für einzelne MTrees angeben, indem Sie den Link **File Age Threshold per MTree** in der rechten unteren Ecke verwenden.

   CLI-Entsprechung
   So legen Sie den Altersschwellenwert fest:

   ```
   # archive data-movement policy set age-threshold {days|none}
   mtrees mtree-list
   ```

   So legen Sie bei Bedarf den *standardmäßigen* Altersschwellenwert fest:

   ```
   # archive data-movement policy set default-age-threshold days
   ```

   So überprüfen Sie die Einstellung für den Altersschwellenwert:

   ```
   # archive data-movement policy show [mtree mtree-list]
   ```

   So legen Sie die Migrationsplanung fest:

   ```
   # archive data-movement schedule set days days time time [no-
   clean]
   ```

   Zulässige Planungswerte:

   - days sun time 00:00
   - days mon,tue time 00:00
   - days 2 time 10:00
   - days 2,15 time 10:00
   - days last time 10:00 – letzter Tag des Monats

   So überprüfen Sie die Migrationsplanung:

```
# archive data-movement schedule show
```

So deaktivieren Sie die Dateibereinigungsplanung:

Hinweis

Die Bereinigungsplanung wird deaktiviert, um einen Planungskonflikt zwischen Bereinigung und Datenverschiebung zu beheben. Nach Abschluss der Datenverschiebung wird die Bereinigung automatisch gestartet. Wenn Sie die Datenverschiebung deaktivieren, müssen Sie die Dateisystembereinigung erneut aktivieren.

```
# filesys clean set schedule never
```

Starten oder Beenden der Datenverschiebung nach Bedarf

Auch wenn Sie eine Policy für regelmäßige Datenverschiebungen verwenden, können Sie eine Datenverschiebung *nach Bedarf* starten oder beenden.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System**
2. Klicken Sie auf **Start** rechts neben **Data Movement Status**.
3. Im Dialogfeld „Start Data Movement“ werden Sie gewarnt, dass Daten vom aktiven zum Aufbewahrungs-Tier verschoben werden sollen, wie von Ihrer Datenverschiebungs-Policy definiert, gefolgt von einer Dateisystembereinigung. Wählen Sie **Start** aus, um die Datenverschiebung zu starten.

   Falls bereits eine Dateisystembereinigung durchgeführt wird, erfolgt die Datenverschiebung nach Abschluss dieser Bereinigung. Es wird jedoch auch automatisch eine weitere Bereinigung gestartet, nachdem die Datenverschiebung nach Bedarf abgeschlossen ist.
4. Die Schaltfläche **Start** wird durch die Schaltfläche **Stop** ersetzt.
5. Wählen Sie jederzeit, wenn Sie eine Datenverschiebung beenden möchten, **Stop** und dann **OK** im Dialogfeld „Stop Data Movement“ aus, um das Beenden zu bestätigen.

Verwenden der Datenverschiebungskomprimierung

Daten werden in der Zielpartition nach jeder Dateimigration komprimiert (ab DD OS 5.2). Standardmäßig ist diese Funktion, die als *Datenverschiebungskomprimierung* bezeichnet wird, aktiviert.

Wenn diese Funktion aktiviert ist, verbessert sich die Gesamtkomprimierung des Aufbewahrungs-Tier, wobei sich jedoch die Migrationszeit leicht erhöht.

Wählen Sie **Data Management** > **File System** > **Configuration** aus, um festzustellen, ob diese Funktion aktiviert ist.

Der aktuelle Wert für **Packing data during Retention Tier data movement** kann „Enabled“ oder „Disabled“ sein. Wenden Sie sich zwecks Änderung dieser Einstellung an einen Systemtechniker.

Upgrades und Recovery mit DD Extended Retention

In den folgenden Abschnitten werden das Durchführen von Software- und Hardwareupgrades und das Wiederherstellen von Daten bei DD-Systemen mit aktivierter DD Extended Retention beschrieben.

Durchführen eines Upgrades auf DD OS 5.7 mit DD Extended Retention

Die Upgrade-Policy für ein DD Extended Retention-fähiges DD-System ist identisch mit der eines standardmäßigen DD-Systems.

Upgrades von bis zu zwei wichtigen früheren Versionen werden unterstützt. Anweisungen zum Durchführen eines Upgrades des DD OS finden Sie im Abschnitt mit den Upgrade-Anweisungen in den *Versionshinweisen* der Ziel-DD OS-Version.

Stellen Sie beim Durchführen eines Upgrades eines DD Extended Retention-fähigen DD-Systems auf DD OS 5.7 sicher, dass Sie vorhandene Planungen für die Datenverschiebung alle 14 Tage aktualisieren, um die Funktion zur Speicherplatzrückgewinnung zu nutzen.

DD Extended Retention-fähige DD-Systeme führen nach Abschluss der Datenverschiebung automatisch eine Bereinigung durch. Planen Sie daher die Bereinigung nicht separat mit dem DD System Manager oder der Befehlszeilenoberfläche (CLI).

Wenn der aktive Tier verfügbar ist, führt der Prozess ein Upgrade des aktiven Tier und der Aufbewahrungseinheit durch und versetzt das System in einen Status, dass der Abschluss des früheren Upgrades noch nicht verifiziert wurde. Dieser Status wird durch das Dateisystem entfernt, nachdem das Dateisystem aktiviert wurde und verifiziert hat, dass der Aufbewahrungs-Tier aktualisiert wurde. Ein nachfolgendes Upgrade ist nicht zulässig, bis dieser Status gelöscht ist.

Wenn der aktive Tier nicht verfügbar ist, führt der Upgradeprozess ein Upgrade des Systemgehäuses durch und versetzt es in einen Status, in dem es bereit ist, ein Dateisystem zu erstellen oder zu akzeptieren.

Wenn die Aufbewahrungseinheit verfügbar wird, nachdem der Upgradeprozess beendet wurde, wird die Einheit automatisch aktualisiert, wenn sie an das System angeschlossen wird, oder beim nächsten Systemstart.

Upgrade von Hardware mit DD Extended Retention

Sie können ein DD-System mit aktivierter DD Extended Retention auf ein höheres oder leistungsfähigeres DD-System mit Performance DD Extended Retention aktualisieren. Beispielsweise können Sie ein DD860 mit aktivierter DD Extended Retention durch ein DD990 mit aktivierter DD Extended Retention ersetzen.

Hinweis

Wenden Sie sich an Ihren vertraglich festgelegten Serviceprovider und lesen Sie dann die Anweisungen im entsprechenden *System-Controller-Upgradeleitfaden*.

Diese Art von Upgrade beeinflusst DD Extended Retention wie folgt:

- Wenn das neue System über eine neuere Version von DD OS als die aktiven und Aufbewahrungs-Tiers verfügt, werden die aktiven und Aufbewahrungs-Tiers auf die Version des neuen Systems aktualisiert. Andernfalls wird das neue System auf die Version der aktiven und Aufbewahrungs-Tiers aktualisiert.
- Die aktiven und Aufbewahrungs-Tiers, die mit dem neuen System verbunden sind, werden durch das neue System übernommen.
- Wenn ein aktiver Tier vorhanden ist, wird die Registrierung im aktiven Tier im neuen System installiert. Andernfalls wird die Registrierung im Aufbewahrungs-Tier mit der zuletzt aktualisierten Registrierung im neuen System installiert.

Wiederherstellen eines Systems mit aktivierter DD Extended Retention

Wenn der aktive Tier und eine Untersammlung der Aufbewahrungseinheiten auf einem DD-System mit aktivierter DD Extended Retention verloren gehen und kein Replikat verfügbar ist, kann der Support möglicherweise alle verbleibenden versiegelten Aufbewahrungseinheiten in ein neues DD-System wiederherstellen.

Ein DD-System mit aktivierter DD Extended Retention ist darauf ausgelegt, für die Verarbeitung von Lese- und Schreibanforderungen verfügbar zu bleiben, wenn eine oder mehrere Aufbewahrungseinheiten verloren gehen. Das Dateisystem erkennt möglicherweise erst, dass eine Aufbewahrungseinheit verloren gegangen ist, wenn das Dateisystem neu gestartet wird oder versucht, auf Daten zuzugreifen, die in der Aufbewahrungseinheit gespeichert sind. Bei Letzterem wird möglicherweise ein Dateisystemneustart ausgelöst. Nachdem das Dateisystem erkannt hat, dass eine Aufbewahrungseinheit verloren gegangen ist, gibt sie einen Fehler in Reaktion auf Anforderungen für in dieser Einheit gespeicherte Daten zurück.

Wenn die verloren gegangenen Daten nicht durch ein Replikat wiederhergestellt werden können, kann der Support möglicherweise das System bereinigen, indem die verloren gegangene Aufbewahrungseinheit und alle Dateien entfernt werden, die sich komplett oder teilweise darin befinden.

Verwenden der Replikations-Recovery

Das Replikations-Recovery-Verfahren für ein DD Extended Retention-fähiges DD-System hängt vom Replikationstyp ab.

- Sammelreplikation: Die neue Quelle muss als DD Extended Retention-fähiges DD-System mit mindestens derselben Anzahl von Aufbewahrungseinheiten wie das Ziel konfiguriert werden. Das Dateisystem darf erst auf der neuen Quelle aktiviert werden, wenn die Aufbewahrungseinheiten hinzugefügt wurden und die Replikations-Recovery initiiert wurde.

  Hinweis

  Wenn Sie nur einen Teil eines Systems, wie beispielsweise eine Aufbewahrungseinheit, von einem Sammlungsreplikat wiederherstellen müssen, wenden Sie sich an den Support.

- MTree-Replikation: siehe den Abschnitt *MTree-Replikation* im Kapitel *Arbeiten mit DD Replicator*.
- DD Boost Managed File Replication: siehe *Data Domain Boost for OpenStorage Administration Guide*.

Wiederherstellen nach einem Systemausfall

Ein DD-System mit aktivierter DD Extended Retention enthält Tools, mit denen Ausfälle in verschiedenen Bereichen des Systems behoben werden können.

Vorgehensweise

1. Setzen Sie die Verbindung zwischen dem System-Controller und dem Speicher zurück. Wenn der System-Controller verloren gegangen ist, ersetzen Sie ihn durch einen neuen System-Controller.
2. Wenn es zu einem Datenverlust gekommen ist und ein Replikat verfügbar ist, versuchen Sie, die Daten aus dem Replikat wiederherzustellen. Wenn kein Replikat verfügbar ist, grenzen Sie die Datenverluste ein, indem Sie die

Fehlerisolierungsfunktionen von DD Extended Retention über den Support nutzen.

KAPITEL 20

DD Retention Lock

Dieses Kapitel enthält die folgenden Themen:

Überblick über DD Retention Lock

Wenn Daten auf einem MTree gesperrt sind, auf dem DD Retention Lock aktiviert ist, können Sie mit DD Retention Lock die Datenintegrität aufrechterhalten. Die gesperrten Daten können während einer benutzerdefinierten Aufbewahrungsfrist von bis zu 70 Jahren nicht überschrieben, geändert oder gelöscht werden.

Es gibt zwei DD Retention Lock-Editionen:

- *Data Domain Retention Lock Governance Edition* behält die Funktionen von Data Domain Retention Lock vor DD OS 5.2 bei. Sie können die Data Domain Retention Lock Governance verwenden, um Aufbewahrungs-Policies für Daten zu definieren, die für einen bestimmten Zeitraum aufbewahrt werden sollen, um die internen IT-Governance-Policies zu erfüllen, die vom Systemadministrator implementiert werden.
- *Data Domain Retention Lock Compliance Edition* ermöglicht Ihnen die Einhaltung der strengsten Datenaufbewahrungsanforderungen von behördlichen Standards wie denen von SEC 17a-4(f). Die vollständige Liste der behördlichen Standards umfasst die folgenden:
  - CFTC Rule 1.31b
  - FDA 21 CFR Part 11
  - Sarbanes-Oxley Act
  - IRS 98025 und 97-22
  - ISO-Standard 15489-1
  - MoREQ2010

  Zertifizierungsinformationen finden Sie unter *Compliance Assessments - Summary and Conclusions – EMC Data Domain Retention Lock Compliance Edition* unter:

  https://www.emc.com/collateral/analyst-reports/cohasset-dd-retention-lock-assoc-comp-assess-summ-ar.pdf

  (Anmeldung erforderlich)

  Die Einhaltung dieser Standards sorgt dafür, dass die Dateien, die mit der Data Domain Retention Lock Compliance Edition auf einem Data Domain-System gesperrt werden, nicht geändert oder gelöscht werden können, bevor die Aufbewahrungsfrist abgelaufen ist. Für Data Domain Retention Lock Compliance Edition ist ein Security Officer für die Implementierung von Policies erforderlich. Der Zugriff auf eine Auditprotokolldatei kann vom Administrator oder Security Officer erfolgen.

Für jede Version ist eine separate Add-on-Lizenz erforderlich und eine oder beide können auf einem einzigen Data Domain-System verwendet werden.

Das Protokoll für die Aufbewahrungssperre ist für die DD Retention Lock Governance und die Compliance Edition gleich. Die verwendeten Unterschiede sind im Systemverhalten für die DD Retention Lock Compliance Edition begründet, da sie strenge Einschränkungen auferlegt, um Complianceanforderungen gerecht zu werden. Eine Übersicht finden Sie im Whitepaper *EMC Data Domain Retention Lock Software – A Detailed Review* unter:

https://www.emc.com/collateral/hardware/white-papers/h10666-data-domain-retention-lock-wp.pdf

(Anmeldung erforderlich)

Für die DD Retention Lock Governance Edition ist kein Security Officer erforderlich und sie bietet ein höheres Maß an Flexibilität für die Aufbewahrung von Archivdaten auf Data Domain-Systemen.

Für Archivcompliance-Speicheranforderungen erfordern die SEC-Regeln, dass eine separate Kopie von Daten mit Aufbewahrungssperre mit denselben Aufbewahrungsanforderungen wie das Original gespeichert werden muss. Dateien mit Aufbewahrungssperre können mit DD Replicator zu einem anderen Data Domain-System repliziert werden. Wenn eine Datei mit Aufbewahrungssperre repliziert wird, bleibt die Aufbewahrungssperre auf dem Zielsystem mit demselben Schutzlevel wie bei der Quelldatei erhalten.

DD Retention Lock Governance Edition wird für lokale, cloudbasierte und DD3300-DD VE-Instanzen unterstützt. DD Retention Lock Compliance Edition wird nicht für lokale, cloudbasierte oder DD3300-DD VE-Instanzen unterstützt.

In den folgenden Themen finden Sie zusätzliche Informationen über DD Retention Lock.

DD Retention Lock-Protokoll

Nur Dateien, die ausdrücklich mit einer Aufbewahrungssperre versehen sind, erhalten auf dem Data Domain-System eine Aufbewahrungssperre. Dateien erhalten die Aufbewahrungssperre über clientseitige Befehle, die bei aktivierter DD Retention Lock Governance oder Compliance auf dem MTree, der die Dateien enthält, ausgegeben werden.

Hinweis

Linux-, Unix- und Windows-Clientumgebungen werden unterstützt.

Dateien, die in Shares geschrieben werden, oder Exporte, die nicht mit einer Aufbewahrungssperre versehen werden (selbst wenn DD Retention Lock Governance oder Compliance auf dem MTree aktiviert ist, der die Dateien enthält), können jederzeit geändert oder gelöscht werden.

Die Aufbewahrungssperre verhindert, dass Dateien mit Aufbewahrungssperre während der durch einen clientseitigen *atime*-Updatebefehl angegebenen Aufbewahrungsfrist direkt von CIFS-Shares oder NFS-Exporten geändert oder gelöscht werden. Einige Archivierungsanwendungen und Backupanwendungen können diesen Befehl ausgeben, wenn sie entsprechend konfiguriert sind. Anwendungen oder Dienstprogramme, die diesen Befehl nicht ausführen, können Dateien nicht mithilfe von DD Retention Lock sperren.

Dateien mit Aufbewahrungssperre werden immer vor Änderung und vorzeitiger Löschung geschützt, selbst wenn die Aufbewahrungssperre später deaktiviert wird oder wenn die Retention Lock-Lizenz nicht mehr gültig ist.

Sie können nicht leere Ordner oder Verzeichnisse innerhalb von MTrees mit aktivierter Aufbewahrungssperre nicht umbenennen oder löschen. Sie können jedoch leere Ordner oder Verzeichnisse umbenennen oder löschen und neue erstellen.

Die Aufbewahrungsfrist einer Datei mit Aufbewahrungssperre kann durch Aktualisieren der *atime* der Datei verlängert, jedoch nicht verkürzt werden.

Sowohl in DD Retention Lock Governance als auch in Compliance kann die Datei bei einmal abgelaufener Aufbewahrungsfrist der Datei mithilfe eines clientseitigen Befehls, Skripts oder einer Anwendung gelöscht werden. Allerdings kann die Datei selbst nach Ablauf der Aufbewahrungsfrist der Datei nicht geändert werden. Das Data Domain-System löscht niemals automatisch eine Datei, deren Aufbewahrungsfrist abgelaufen ist.

DD Retention Lock-Ablauf

Allgemeiner Ablauf von Aktivitäten mit DD Retention Lock:

1. Aktivieren Sie MTrees für die DD Retention Lock Governance- oder Compliance-Aufbewahrungssperre mithilfe von DD System Manager oder DD OS-Befehlen, die von der Systemkonsole ausgegeben werden.
2. Legen Sie Dateien für die Aufbewahrungssperre auf dem Data Domain-System über clientseitige Befehle fest, die durch eine entsprechend konfigurierte Archivierungs- oder Backupanwendung manuell oder über Skripte ausgegeben werden.

   Hinweis

   Windows-Clients müssen möglicherweise Dienstprogramme für die DD OS-Kompatibilität herunterladen.

3. Optional können Sie mithilfe von clientseitigen Befehlen Dateiaufbewahrungszeiten erweitern.
4. Sie können optional Dateien mit abgelaufen Aufbewahrungsfristen über clientseitige Befehle löschen.

Unterstützte Datenzugriffsprotokolle

DD Retention Lock ist mit NAS-basierten WORM-Protokollen (Write-Once-Read-Many) nach Branchenstandard kompatibel und die Integration wird mit Archivierungsanwendungen wie Symantec Enterprise Vault, SourceOne, Cloud Tiering Appliance, DiskXtender usw. qualifiziert. Kunden, die Backupanwendungen wie CommVault verwenden, können auch benutzerdefinierte Skripte entwickeln, um Data Domain Retention Lock zu nutzen.

Wenn Sie prüfen möchten, ob eine Anwendung für DD Retention Lock getestet und zertifiziert ist, lesen Sie den *Data Domain Archive Application Compatibility Guide*.

DD Retention Lock unterstützt die folgenden Protokolle:

- NFS wird von DD Retention Lock Governance und Compliance unterstützt.
- CIFS wird von DD Retention Lock Governance und Compliance unterstützt.
- DD VTL wird mit DD Retention Lock Governance, nicht jedoch mit DD Retention Lock Compliance unterstützt.
  Virtuelle Bänder, nachfolgend als *Bänder* bezeichnet, werden als Dateien im Dateisystem dargestellt.
  - Wenn Sie einen Speicherpool erstellen, eine Sammlung von Bändern, die zu einem Verzeichnis auf dem Dateisystem zugeordnet sind, erstellen Sie einen MTree, es sei denn, Sie möchten ausdrücklich den Verzeichnispool mit einem älteren Stil erstellen (für Abwärtskompatibilität). Sie können auch Speicherpools, die vor DD OS 5.3 erstellt wurden, in MTrees konvertieren. Diese MTrees können mit einer Aufbewahrungssperre versehen und repliziert werden.
  - Sie können ein oder mehrere Bänder mit einer Aufbewahrungssperre versehen, indem Sie den Befehl `vtl tape modify` verwenden, wie im *Data Domain Operating System Command Reference Guide* beschrieben.
    Der Befehl `mtree retention-lock revert`*path* kann dazu verwendet werden, den Status der Aufbewahrungssperre von Bändern, die mit dem Befehl

`vtl tape modify` gesperrt wurden, zurückzusetzen. Nachdem das Band entsperrt wurde, können Aktualisierungen vorgenommen werden. Der entsperrte Status ist erst über den DD System Manager oder die Befehlszeilenoberfläche sichtbar, nachdem der DD VTL-Service deaktiviert und wieder aktiviert wurde. Aktualisierungen werden jedoch auf das entsperrte Band angewendet. Diese Funktion ist nur für die DD Retention Lock Governance Edition verfügbar.

  - Die Aufbewahrungszeit für Bänder kann mithilfe des Befehls `vtl tape show` und dem Argument `time-display retention` angezeigt werden.
  - Sie können mithilfe des DD System Manager eine Aufbewahrungssperre für ein einzelnes Band festlegen.

- DD Boost wird von DD Retention Lock Governance und Compliance unterstützt. Beachten Sie Folgendes: Wenn clientseitige Skripte für die Festlegung einer Aufbewahrungssperre für Backupdateien oder Backup-Images verwendet werden und außerdem eine Backupanwendung (z. B. Veritas NetBackup) über DD Boost auf dem System verwendet wird, gibt die Backupanwendung den Kontext der clientseitigen Skripte eventuell nicht frei. Wenn also eine Backupanwendung versucht, Dateien ablaufen zu lassen oder zu löschen, die über clientseitige Skripte mit einer Aufbewahrungssperre versehen wurden, wird kein Speicherplatz auf dem Data Domain-System freigegeben.

  Data Domain empfiehlt Administratoren, ihre Policies für Aufbewahrungsfristen zu ändern und mit der Retention Lock-Zeit abzustimmen. Dies gilt für viele der Backupanwendungen, die in DD Boost integriert sind, einschließlich Veritas NetBackup, Veritas Backup Exec und NetWorker.

  Das Festlegen einer Aufbewahrungssperre während der Datenaufnahme in eine DD BOOST-Datei im DSP-Modus ist nicht zulässig und der Client, der die Sperre festlegt, erhält eine Fehlermeldung. Die Aufbewahrungssperre sollte festgelegt werden, nachdem die Datenaufnahme abgeschlossen ist.

  Das Festlegen einer Aufbewahrungssperre während der Datenaufnahme in eine DD BOOST-Datei im OST-Modus oder in eine NFS-Datei ist nicht zulässig und der Client, der die Daten schreibt, erhält eine Fehlermeldung, sobald die Aufbewahrungssperre festgelegt wird. Die partielle Datei, die vor dem Festlegen der Aufbewahrungssperre erstellt wird, wird auf dem Datenträger als Worm-Datei committet.

Aktivieren von DD Retention Lock auf einem MTree

Nur für Dateien, die sich in MTrees mit aktivierter DD Retention Lock Governance oder DD Retention Lock Compliance befinden, kann eine Aufbewahrungssperre eingerichtet werden.

MTrees mit aktivierter DD Retention Lock Compliance können nicht in MTrees mit aktivierter DD Retention Lock Governance konvertiert werden und umgekehrt.

Im nachfolgenden Verfahren wird gezeigt, wie Sie DD Retention Lock Governance oder DD Retention Lock Compliance für MTrees aktivieren können.

Aktivieren von DD Retention Lock Governance auf einem MTree

Fügen Sie eine DD Retention Lock Governance-Lizenz zu einem System hinzu und aktivieren Sie anschließend DD Retention Lock Governance auf einem oder mehreren MTrees.

Vorgehensweise

1. Fügen Sie die DD Retention Lock Governance-Lizenz hinzu, wenn sie nicht unter „Feature Licenses“ aufgeführt ist.
   a. Wählen Sie **Administration** > **Licenses**.
   b. Klicken Sie im Bereich „Licenses“ auf **Add Licenses**.
   c. Geben Sie in das Textfeld „License Key“ den Lizenzschlüssel ein.

      Hinweis

      Bei Lizenzschlüsseln wird nicht zwischen Groß- und Kleinschreibung unterschieden. Schließen Sie die Bindestriche bei der Eingabe der Schlüssel ein.

   d. Klicken Sie auf **Hinzufügen**.
2. Wählen Sie einen MTree für die Aufbewahrungssperre aus.
   a. Wählen Sie **Data Management** > **MTree**.
   b. Wählen Sie den MTree für die Aufbewahrungssperre aus. Sie können auch einen leeren MTree erstellen und später Dateien zu diesem hinzufügen.
3. Klicken Sie auf die Registerkarte „MTree Summary“, um Informationen für den ausgewählten MTree anzuzeigen.
4. Blättern Sie nach unten zum Bereich „Retention Lock“ und klicken Sie rechts neben „Retention Lock“ auf **Edit**.
5. Aktivieren Sie DD Retention Lock Governance auf dem MTree und ändern Sie bei Bedarf die minimalen und maximalen Standard-Aufbewahrungssperrfristen für den MTree.

   Führen Sie die folgenden Aktionen im Dialogfeld „Modify Retention Lock“ aus:

   a. Aktivieren Sie **Enable**, um DD Retention Lock Governance auf dem MTree zu aktivieren.
   b. Zum Ändern der minimalen und maximalen Aufbewahrungsfrist für den MTree ändern Sie den minimalen oder maximalen Zeitraum:

      Geben Sie eine Zahl für das Intervall in das Textfeld ein (z. B. `5` oder `14`).

      Wählen Sie aus der Drop-down-Liste ein Intervall aus (Minuten, Stunden, Tage, Jahre).

      Hinweis

      Wenn Sie eine minimale Aufbewahrungsfrist von weniger als 12 Stunden oder eine maximale Aufbewahrungsfrist von mehr als 70 Jahren angeben, führt dies zu einem Fehler.

   c. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

      Nachdem Sie das Dialogfeld „Modify Retention Lock“ geschlossen haben, werden aktualisierte MTree-Informationen im Bereich „Retention Lock“ angezeigt.
6. Überprüfen Sie die Informationen zur Aufbewahrungssperre für den MTree.

   Beachten Sie die folgenden Felder für die Aufbewahrungssperre:

- Im oberen Bereich:
  - Im Feld „Status“ werden der Lese-/Schreibzugriff für den MTree, die Art der Aufbewahrungssperre für den MTree und die Tatsache angezeigt, ob eine Aufbewahrungssperre aktiviert oder deaktiviert ist.
- Im unteren Bereich:
  - Im Feld „Status“ wird angezeigt, ob eine Aufbewahrungssperre für den MTree aktiviert ist.
  - Im Feld „Retention Period“ werden die minimalen und maximalen Aufbewahrungsfristen für den MTree angezeigt. Die für eine Datei im MTree angegebene Aufbewahrungsfrist muss größer oder gleich der minimalen Aufbewahrungsfrist und kleiner oder gleich der maximalen Aufbewahrungsfrist sein.
  - Das UUID-Feld ist eine eindeutige Identifikationsnummer, die für den MTree erzeugt wird.

Hinweis

Zum Überprüfen der Konfigurationseinstellungen für die Aufbewahrungssperre eines beliebigen MTree wählen Sie den MTree im Navigationsbereich aus und klicken Sie dann auf die Registerkarte „Summary“.

Weitere Erfordernisse

Dateien mit Aufbewahrungssperre in einem MTree mit Aufbewahrungssperre

Aktivieren von DD Retention Lock Compliance auf einem MTree

Sie können eine DD Retention Lock Compliance-Lizenz zu einem System hinzufügen, einen Systemadministrator und einen oder mehrere Security Officer einrichten, das System so konfigurieren und aktivieren, dass es DD Retention Lock Compliance-Software verwendet, und anschließend DD Retention Lock Compliance auf einem oder mehreren MTrees aktivieren.

Vorgehensweise

1. Fügen Sie die DD Retention Lock Compliance-Lizenz auf dem System hinzu, wenn sie nicht vorhanden ist.
   a. Überprüfen Sie zunächst, ob die Lizenz bereits installiert ist.

      ```
      license show
      ```

   b. Wenn die Funktion RETENTION LOCK COMPLIANCE nicht angezeigt wird, installieren Sie die Lizenz.

      ```
      license add Lizenzschlüssel
      ```

      Hinweis

      Bei Lizenzschlüsseln wird nicht zwischen Groß- und Kleinschreibung unterschieden. Schließen Sie die Bindestriche bei der Eingabe der Schlüssel ein.

2. Richten Sie ein oder mehrere Security Officer-Benutzerkonten gemäß den RBAC-Regeln (Rolle Base Access Control) ein.

a. Fügen Sie in der Systemadministrator-Rolle ein Security Officer-Konto hinzu.

```
user add Benutzer role security
```

b. Aktivieren Sie die Security Officer-Autorisierung.

```
authorization policy set security-officer enabled
```

3. Konfigurieren und aktivieren Sie das System, das DD Retention Lock Compliance verwenden soll.

Hinweis

Die Aktivierung von DD Retention Lock Compliance erzwingt viele Einschränkungen für den Zugriff auf niedriger Ebene auf Systemfunktionen, die beim Troubleshooting verwendet werden. Nach der Aktivierung besteht die einzige Möglichkeit, DD Retention Lock Compliance zu deaktivieren, darin, das System zu initialisieren und neu zu laden, wodurch alle Daten auf dem System gelöscht werden.

a. Konfigurieren Sie das System so, dass es DD Retention Lock Compliance verwendet.

```
system retention-lock compliance configure
```

Das System wird automatisch neu gestartet.

b. Wenn der Neustart abgeschlossen ist, aktivieren Sie DD Retention Lock Compliance auf dem System.

```
system retention-lock compliance enable
```

4. Aktivieren Sie Compliance auf einem MTree, der die mit einer Aufbewahrungssperre versehenen Dateien enthält.

```
mtree retention-lock enable mode compliance mtree Mtree-Pfad
```

Hinweis

Compliance kann nicht für /backup oder Pool-MTrees aktiviert werden.

5. Um die standardmäßigen minimalen und maximalen Aufbewahrungssperrfristen für einen compliancefähigen MTree zu ändern, geben Sie die folgenden Befehle mit Security Officer-Autorisierung ein.

```
mtree retention-lock set min-retention-
period Zeitraum mtree Mtree-Pfad
mtree retention-lock set max-retention-
period Zeitraum mtree Mtree-Pfad
```

Hinweis

Die *Aufbewahrungsfrist* wird im Format [Zahl] [Einheit] angegeben. Beispiel: 1 min, 1 hr, 1 day, 1 mo oder 1 year. Wenn Sie eine minimale Aufbewahrungsfrist von weniger als 12 Stunden oder eine maximale Aufbewahrungsfrist von mehr als 70 Jahren angeben, führt dies zu einem Fehler.

Wiederholen Sie die Schritte 4 und 5, um weitere MTrees zu aktivieren.

Weitere Erfordernisse

Dateien mit Aufbewahrungssperre befinden sich in einem MTree mit Aufbewahrungssperre.

Clientseitige Retention Lock-Dateikontrolle

Dieser Abschnitt beschreibt die Befehlsschnittstelle des DD Retention Lock-Clients für das Sperren von Dateien, die auf Data Domain-Systemen gespeichert sind. Die Clientbefehle sind für DD Retention Lock Governance und Compliance gleich. Linux-, Unix- und Windows-Clientumgebungen werden unterstützt. Möglicherweise müssen Windows-Clients jedoch Dienstprogramme mit Befehlen herunterladen, um Dateien zu sperren.

Hinweis

Wenn Ihre Anwendung bereits branchenübliches WORM unterstützt, sperrt das Schreiben einer WORM-Datei in einen DD Retention Lock Governance- oder Compliance-fähigen MTree die Datei auf dem Data Domain-System. Die Aufbewahrungszeit in der Anwendung sollte mit den DD Retention Lock-Einstellungen übereinstimmen. Sie müssen die in diesem Abschnitt beschriebenen Befehle nicht verwenden. Wenn Sie prüfen möchten, ob eine Anwendung für DD Retention Lock getestet und zertifiziert ist, lesen Sie den *Data Domain Archive Application Compatibility Guide*.

Hinweis

Einige Clientrechner, die NFS verwenden, aber ein älteres Betriebssystem ausführen, können die Aufbewahrungszeit nicht höher als 2038 festlegen. Das NFS-Protokoll enthält die Begrenzung von 2038 nicht und gestattet die Angabe von Zeiten bis 2106. Außerdem gilt die Begrenzung von 2038 in DD OS nicht.

Clientseitige Befehle werden verwendet, um die Aufbewahrungssperrung einzelner Dateien zu verwalten. Diese Befehle gelten für alle Data Domain-Systeme mit Retention Lock und müssen zusätzlich zur Einrichtung und Konfiguration von DD Retention Lock auf dem Data Domain-System ausgeführt werden.

Erforderliche Tools für Windows-Clients

Sie benötigen den Befehl `touch.exe`, um die Aufbewahrungssperrung von einem Windows-basierten Client durchzuführen.

Um diesen Befehl zu erhalten, laden Sie Dienstprogramme für Linux-/Unix-basierte Anwendungen gemäß Ihrer Windows-Version herunter und installieren Sie sie. Diese Dienstprogramme sind Empfehlungen von Data Domain und sollten je nach Kundenumgebung genutzt werden.

- Bei Windows 8, Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003 und Windows XP:
  http://sourceforge.net/projects/unxutils/files/latest
- Für Windows Server 2008, Windows Vista Enterprise, Windows Vista Enterprise 64-Bit-Edition, Windows Vista SP1, Windows Vista Ultimative und Windows Vista Ultimative 64-Bit-Edition:
  http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=23754
- Für Windows Server 2003 SP1 und Windows Server 2003 R2:
  http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=20983

Hinweis

Der Befehl `touch` für Windows kann ein anderes Format als die Linux-Beispiele in diesem Kapitel aufweisen.

Befolgen Sie die bereitgestellten Installationsanweisungen und legen Sie den Suchpfad nach Bedarf auf dem Clientrechner fest.

Clientzugriff auf Data Domain-Systemdateien
Nachdem ein MTree für DD Retention Lock Governance oder Compliance aktiviert ist, können Sie:

- Erstellen Sie eine CIFS-Share basierend auf einem MTree. Diese CIFS-Share kann auf einem Clientcomputer verwendet werden.
- Erstellen Sie einen NFS-Mount-Punkt für einen MTree und greifen Sie über den NFS-Mount-Punkt auf die Dateien auf einem Clientcomputer zu.

Hinweis

Die Befehle, die in diesem Abschnitt aufgeführt werden, können nur auf dem Client verwendet werden. Sie können nicht über den DD System Manager oder die Befehlszeilenoberfläche eingegeben werden. Die Befehlssyntax kann variieren, abhängig vom Dienstprogramm, das Sie verwenden.

Die folgenden Themen beschreiben, wie Sie die clientseitige Retention Lock-Dateikontrolle verwalten.

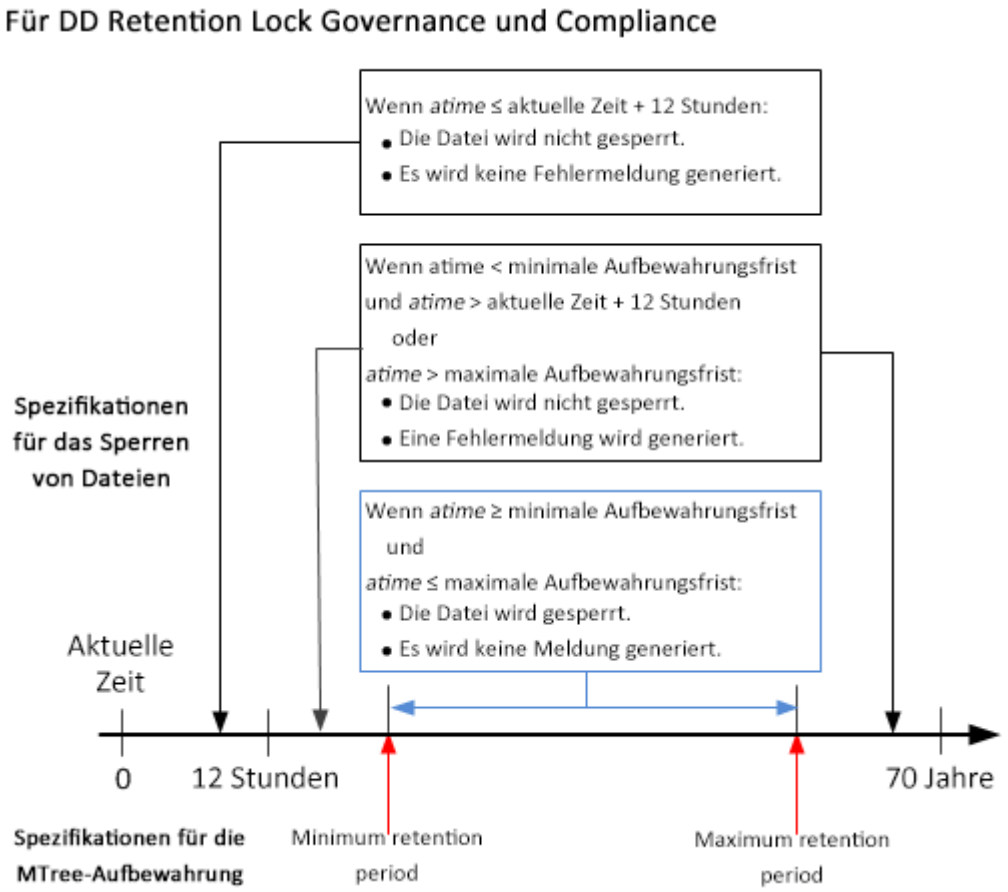
Festlegen einer Aufbewahrungssperre für eine Datei

Um eine Datei mit einer Aufbewahrungssperre zu versehen, ändern Sie die letzte Zugriffszeit (*atime*) der Datei in die gewünschte Aufbewahrungszeit der Datei, d. h. die Zeit, zu der die Datei gelöscht werden kann.

Diese Aktion wird im Allgemeinen durch die Archivierungsanwendung ausgeführt und alle Archivierungsanwendungen, die momentan für Data Domain-Systeme qualifiziert sind (siehe *Data Domain Archive Application Compatibility Guide*) befolgen das grundlegende Sperrprotokoll, das hier dargestellt wird.

Die zukünftige Zugriffszeit (*atime*), die Sie angeben, muss die Mindest- und Höchstaufbewahrungsfristen des MTree der Datei respektieren (als Offsets von der aktuellen Zeit), wie in der nächsten Abbildung gezeigt.

Abbildung 15 Gültige und ungültige *atimes* für Dateien mit Aufbewahrungssperre



Hinweis

Einige Clientrechner, die NFS verwenden, aber ein älteres Betriebssystem ausführen, können die Aufbewahrungszeit nicht höher als 2038 festlegen. Das NFS-Protokoll enthält die Begrenzung von 2038 nicht und gestattet die Angabe von Zeiten bis 2106. Außerdem gilt die Begrenzung von 2038 in DD OS nicht.

Fehler treten bei verweigerter Berechtigung auf (nachfolgend als EACCESS bezeichnet, ein POSIX-Standardfehler). Diese werden an das Skript oder die Archivierungsanwendung zurückgegeben, das bzw. die *atime* festlegt.

Hinweis

Eine Datei muss vollständig in das Data Domain-System geschrieben werden, bevor sie mit einer Aufbewahrungssperre versehen werden kann.

Der folgende Befehl kann auf Clients angewendet werden, um *atime* festzulegen:

```
touch -a -t [atime] [filename]
```

Das Format von *atime* lautet:

```
[[YY]YY] MMDDhhmm[.ss]
```

Angenommen, das aktuelle Datum und die aktuelle Uhrzeit lauten 13 Uhr am 18. Januar 2012 (also 201201181300) und die minimale Aufbewahrungsfrist beträgt 12 Stunden. Wenn Sie die minimale Aufbewahrungsfrist von 12 Stunden diesem Datum

und dieser Uhrzeit hinzufügen, erhalten Sie einen Wert von 201201190100. Wenn *atime* für eine Datei also auf einen Wert über 201201190100 festgelegt ist, wird diese Datei mit einer Aufbewahrungssperre versehen.

Der folgende Befehl:

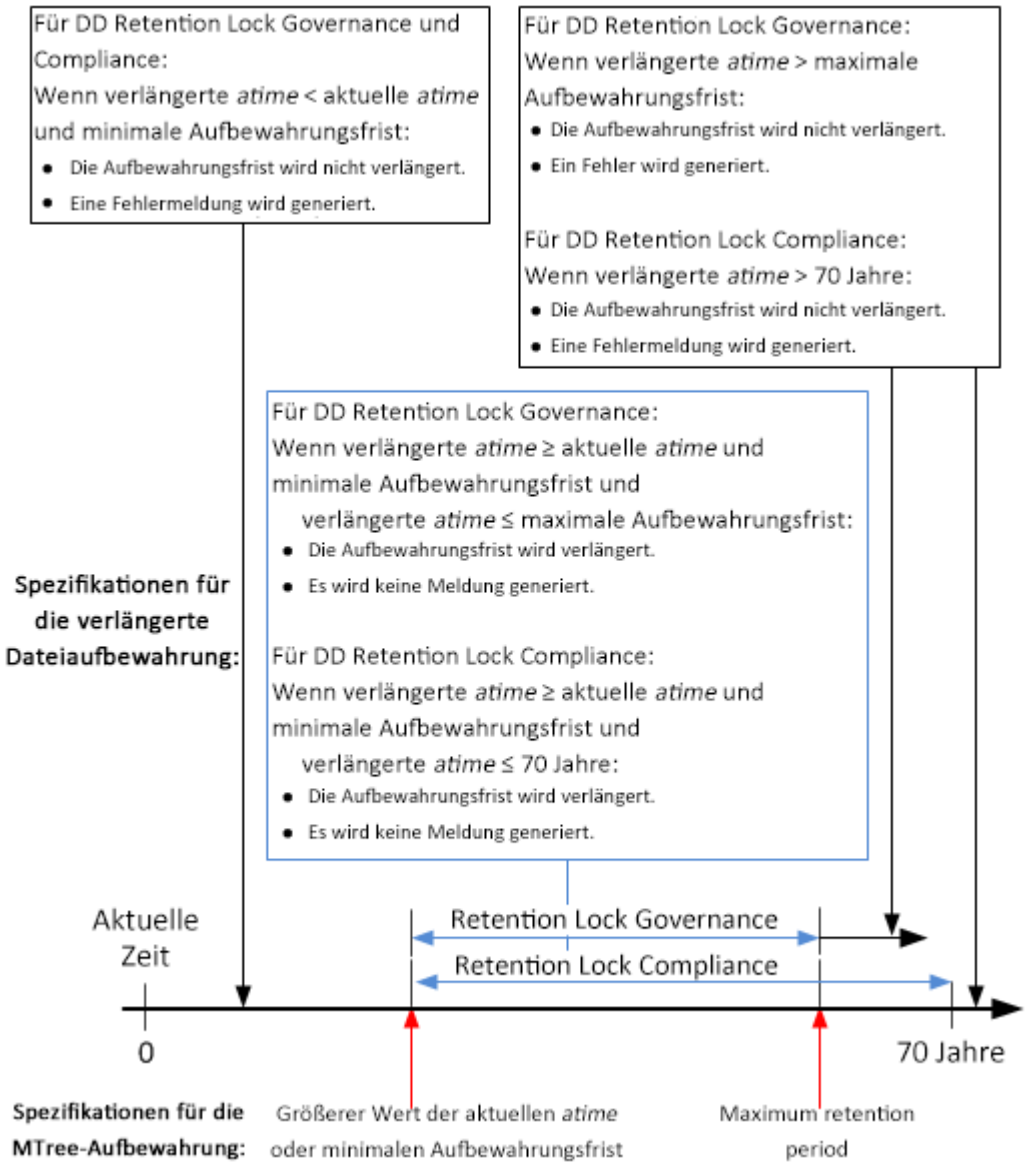
```
ClientOS# touch -a -t 201412312230 SavedData.dat
```

sperrt Datei `SavedData.dat` bis 22:30 Uhr am 31. Dezember 2014.

Erweitern der Aufbewahrungssperre für eine Datei

Zum Verlängern der Aufbewahrungszeit einer Datei mit Aufbewahrungssperre legen Sie den Wert *atime* der Datei auf einen größer Wert als die aktuelle *atime* der Datei fest. Der Wert sollte dabei aber kleiner als die maximale Aufbewahrungsfrist des MTree der Datei sein (als ein Offset der aktuellen Zeit), wie in der nächsten Abbildung gezeigt.

Abbildung 16 Gültige und ungültige *atimes*-Werte für das Erweitern der Aufbewahrungssperre für Dateien



Das Ändern des *atime*-Werts von `201412312230` zu `202012121230` über den folgenden Befehl:

```
ClientOS# touch -a -t 202012121230 SavedData.dat
```

führt beispielsweise dazu, dass die Datei bis 12:30 Uhr am 12. Dezember 2020 gesperrt ist.

Hinweis

Einige Clientmaschinen, die NFS verwenden, aber sehr altes Betriebssystem ausführen, können die Aufbewahrungszeit nicht später als 2038 festlegen. Das NFS-Protokoll enthält die Begrenzung von 2038 nicht und gestattet die Angabe von Zeiten bis 2106. Außerdem gilt die Begrenzung von 2038 in DD OS nicht.

Fehler treten bei verweigerter Berechtigung auf (nachfolgend als EACCESS bezeichnet, ein POSIX-Standardfehler). Diese werden an das Skript oder die Archivierungsanwendung zurückgegeben, das *atime* festlegt.

Erkennen einer Datei mit Aufbewahrungssperre

Der *atime*-Wert für eine Datei mit Aufbewahrungssperre ist ihre Aufbewahrungszeit. Wenn Sie ermitteln möchten, ob eine Datei über eine Aufbewahrungssperre verfügt, versuchen Sie, den *atime*-Wert der Datei auf einen früheren Wert als den aktuellen *atime*-Wert festzulegen. Diese Aktion schlägt mit einem Fehler wegen fehlender Berechtigungen fehl, wenn und nur wenn die Datei eine Datei mit Aufbewahrungssperre ist.

Listen Sie zunächst den aktuellen *atime*-Wert auf und führen Sie dann den Befehl `touch` mit einem früheren *atime*-Wert über die folgenden Befehle aus:

```
ls -l --time=atime [filename]
touch -a -t [atime] [filename]
```

Das folgende Beispiel zeigt die Befehlsfolge:

```
ClientOS# ls -l --time=atime SavedData.dat
202012121230
ClientOS# touch -a -t 202012111230 SavedData.dat
```

Wenn der *atime*-Wert von `SavedData.dat` 202012121230 (12:30 Uhr am 12. Dezember 2020) ist und der Befehl `touch` einen früheren *atime*-Wert, 202012111230 (12:30 Uhr am 11. Dezember 2020), angibt, schlägt der Befehl `touch` fehl, was darauf hinweist, dass `SavedData.dat` eine Aufbewahrungssperre hat.

Hinweis

Die Option `--time=atime` wird nicht in allen Versionen von Unix unterstützt.

Angeben eines Verzeichnisses und ausschließliches Verwenden dieser Dateien

Verwenden Sie die Befehlszeile, um ein Stammverzeichnis mit den Dateien zu erstellen, deren Zugriffszeiten sich ändern.

In dieser Routine enthält *das Stammverzeichnis, von dem gestartet wird*, die Dateien, für die Sie Zugriffszeiten mithilfe des folgenden Clientsystembefehls ändern möchten:

```
find [root directory to start from] -exec touch -a -t
[expiration time] {} \;
```

Beispiel:

```
ClientOS# find [/backup/data1/] -exec touch -a -t 202012121230 {} \;
```

Lesen einer Dateiliste und ausschließliches Verwenden dieser Dateien

In dieser Routine ist *name of file list* der Name einer Textdatei, die die Namen der Dateien enthält, für die Sie die Zugriffszeiten ändern möchten. Jede Zeile enthält den Namen einer Datei.

Hier sehen Sie die Befehlssyntax des Clientsystems:

```
touch -a -t [expiration time] 'cat [name of file list]'
```

Beispiel:

```
ClientOS# touch -a -t 202012121230 ‘cat /backup/data1/filelist.txt‘
```

Löschen oder Ablauf einer Datei

Sie können eine Datei mit einer abgelaufenen Aufbewahrungssperre mithilfe einer Clientanwendung löschen oder ablaufen lassen oder eine Datei mithilfe eines Standardbefehls zum Löschen von Dateien löschen.

Durch das Ablaufen einer Datei über eine Anwendung kann die Anwendung nicht mehr auf die Datei zugreifen. Die Datei wird durch den Ablaufvorgang möglicherweise vom Data Domain-System entfernt, möglicherweise aber auch nicht. Wenn sie nicht entfernt wird, stellt die Anwendung oft einen separaten Löschvorgang bereit. Sie müssen über die entsprechenden Zugriffsrechte verfügen, um die Datei zu löschen, unabhängig von DD Retention Lock.

Hinweis

Wenn die Aufbewahrungsfrist der Datei mit Aufbewahrungssperre nicht abgelaufen ist, führt der Löschvorgang zu einem Fehler wegen abgelehnter Berechtigungen.

Privileged delete

Für DD Retention Lock Governance (ausschließlich) können Sie Dateien mit Aufbewahrungssperre durch Ausführen der folgenden beiden Schritte löschen.

Vorgehensweise

1. Verwenden Sie den Befehl `mtree retention-lock revert` *path*, um die Datei mit Aufbewahrungssperre zurückzusetzen.
2. Löschen Sie die Datei auf dem Clientsystem mit dem Befehl `rm` *filename*.

Verwenden von ctime oder mtime bei Dateien mit Aufbewahrungssperre

ctime ist der letzte Zeitpunkt einer Metadatenänderung einer Datei.

ctime
ctime wird auf die aktuelle Zeit festgelegt, wenn eines der folgenden Events eintritt:

- Eine Datei mit Aufbewahrungssperre ist nicht für die Aufbewahrung gesperrt.
- Die Aufbewahrungszeit einer Datei mit Aufbewahrungssperre wird erweitert.
- Eine Datei mit Aufbewahrungssperre wird zurückgesetzt.

Hinweis

Benutzerzugriffsberechtigungen für eine Datei mit Aufbewahrungssperre werden mit dem Linux-Befehlszeilentool `chmod` aktualisiert.

mtime
mtime ist der letzte Zeitpunkt einer Änderung einer Datei. Es wird nur geändert, wenn der Inhalt der Datei geändert wird. So kann sich mtime einer Datei mit Aufbewahrungssperre nicht ändern.

Systemverhalten mit DD Retention Lock

Themen rund um das Systemverhalten werden in den folgenden Abschnitten separat für DD Retention Lock Governance und DD Retention Lock Compliance dargestellt.

DD Retention Lock Governance

Bestimmte DD OS-Befehle verhalten sich anders, wenn sie DD Retention Lock Governance verwenden. In den folgenden Abschnitten werden die Unterschiede für jeden Befehl beschrieben.

Replikation

Bei der Sammelreplikation, der MTree-Replikation und der Verzeichnisreplikation wird der gesperrte oder der entsperrte Status von Dateien repliziert.

Die Dateien, die in der Quelle von der Governance-Aufbewahrung gesperrt wurden, sind auch auf dem Ziel von der Governance-Aufbewahrung gesperrt und haben den gleichen Schutz. Für die Replikation muss auf dem Quellsystem eine DD Retention Lock Governance-Lizenz installiert sein. Auf dem Zielsystem ist keine Lizenz erforderlich.

Die Replikation wird zwischen folgenden Systemen unterstützt:

- Auf den Systemen wird dieselbe DD OS-Hauptversion ausgeführt (z. B. wird auf beiden Systemen DD OS 5.5.*x.x* ausgeführt).
- Auf den Systemen werden DD OS-Versionen innerhalb der nächsten zwei aufeinanderfolgenden höheren oder niedrigeren Hauptversionen ausgeführt (z. B. 5.3.*x.x* bis 5.5.*x.x* oder 5.5.*x.x* bis 5.3.*x.x*). Eine versionsübergreifende Replikation wird nur für die Verzeichnis- und die MTree-Replikation unterstützt.

Hinweis

Die MTree-Replikation wird nicht für DD OS 5.0 und früher unterstützt.

HINWEIS:

- Bei der Sammelreplikation und der MTree-Replikation werden die minimalen und maximalen Aufbewahrungsfristen, die auf MTrees konfiguriert sind, an das Zielsystem repliziert.
- Bei der Verzeichnisreplikation werden die minimalen und maximalen Aufbewahrungsfristen nicht an das Zielsystem repliziert.

Das Verfahren für die Konfiguration und Verwendung der Sammel-, MTree- und Verzeichnisreplikation ist dasselbe wie für Data Domain-Systeme, die keine DD Retention Lock Governance-Lizenz haben.

Neusynchronisierung der Replikation

Der Befehl `replication resync`*destination* versucht, das Ziel mit der Quelle zu synchronisieren, wenn der MTree- oder Verzeichnisreplikationskontext zwischen Ziel- und Quellsystemen unterbrochen wurde. Dieser Befehl kann nicht mit der Sammelreplikation verwendet werden. Hinweis:

- Wenn Dateien auf den Cloud-Tier migriert werden, bevor der Kontext unterbrochen ist, überschreibt die Resynchronisation der MTree-Replikation alle Daten auf dem Ziel, weshalb Sie die Dateien erneut in den Cloud-Tier migrieren müssen.
- Wenn auf dem Zielverzeichnis DD Retention Lock aktiviert ist, auf dem Quellverzeichnis dagegen nicht, schlägt eine Resynchronisation einer Verzeichnisreplikation fehl.
- Mit Mtree-Replikation schlägt die Neusynchronisation fehl, wenn für den Quell-MTree keine Aufbewahrungssperre und für den Ziel-MTree eine Aufbewahrungssperre aktiviert ist.
- Mit Mtree-Replikation schlägt die Neusynchronisation fehl, wenn für die Quell- und Ziel-MTrees eine Aufbewahrungssperre aktiviert, die Option zum Propagieren der Aufbewahrungssperre aber auf FALSE eingestellt ist.

Fastcopy

Wenn der Befehl `filesys fastcopy [retention-lock] source`*src*`destination`*dest* auf einem System mit einem DD Retention Lock Governance-aktivierten MTree ausgeführt wird, wird das Retention Lock-Attribut während des FastCopy-Vorgangs beibehalten.

Hinweis

Wurde auf dem Ziel-MTree Retention Lock nicht aktiviert, wird das Retention Lock-Dateiattribut nicht beibehalten.

Filesys destroy

Auswirkungen des Befehls `filesys destroy` auf einem System mit einem DD Retention Lock Governance-aktivierten MTree:

- Alle Daten werden gelöscht, einschließlich Daten mit Aufbewahrungssperre.
- Alle `filesys`-Optionen werden auf die Standardwerte zurückgesetzt. Das bedeutet, dass die Aufbewahrungssperre deaktiviert wird und die minimalen und maximalen Aufbewahrungsfristen auf dem neu erstellten Dateisystem auf ihre Standardwerte festgelegt werden.

Hinweis

Dieser Befehl ist nicht zulässig, wenn DD Retention Lock Compliance auf dem System aktiviert ist.

MTree delete

Wenn der Befehl `mtree delete` *mtree-path* versucht, einen DD Retention Lock Governance-fähigen (oder früher fähigen) MTree zu entfernen, der derzeit Daten enthält, gibt der Befehl einen Fehler zurück.

Hinweis

Das Verhalten von `mtree delete` ähnelt einem Befehl zum Löschen eines Verzeichnisses: Ein MTree mit aktivierter (oder zuvor aktivierter) Aufbewahrungssperre kann nur gelöscht werden, wenn der MTree leer ist.

DD Retention Lock Compliance

Bestimmte DD OS-Befehle verhalten sich anders, wenn DD Retention Lock Compliance verwendet wird. In den folgenden Abschnitten werden die Unterschiede für jeden Befehl erläutert.

Replikation

Ein MTree mit DD Retention Lock Compliance kann nur über MTree-Replikation und Sammelreplikation repliziert werden. Verzeichnisreplikation wird nicht unterstützt.

MTree und Sammelreplikation replizieren den gesperrten oder entsperrten Status von Dateien. Die Dateien, die in der Quelle von der Compliance-Aufbewahrung gesperrt wurden, sind auch auf dem Ziel von der Compliance-Aufbewahrung gesperrt und haben den gleichen Schutz. Die minimalen und maximalen Aufbewahrungsfristen, die auf MTrees konfiguriert sind, werden auf dem Zielsystem repliziert.

Um die Sammelreplikation auszuführen, muss der gleiche Security Officer-Anwender auf dem Quell- und Zielsystem vorhanden sein, bevor die Replikation auf dem Zielsystem gestartet werden kann, sowie danach über die Lebensdauer des Quellen-/Replikatpaars.

Neusynchronisierung der Replikation

Der Befehl `replication resync`*destination* kann mit MTree-Replikation verwendet werden, jedoch nicht bei der Sammelreplikation.

- Wenn der Ziel-MTree aufbewahrungsgesperrte Dateien enthält, die nicht in der Quelle vorhanden sind, schlägt die Neusynchronisierung fehl.
- Quell- und Ziel-MTrees müssen für DD Retention Lock Compliance aktiviert sein oder die Neusynchronisierung schlägt fehl.

Replikationsverfahren

In den Themen in diesem Abschnitt werden die MTree- und Sammelreplikationsverfahren beschrieben, die für DD Retention Lock Compliance unterstützt werden.

Hinweis

Vollständige Beschreibungen der Befehle, die in den folgenden Themen referenziert werden, finden Sie im *Data Domain Operating System Command Reference Guide*.

Replikation eines MTree: 1:1-Topologie

Replizieren Sie einen MTree mit aktivierter DD Retention Lock Compliance von einem Quellsystem auf ein Zielsystem.

Bevor Sie beginnen

Aktivieren Sie DD Retention Lock auf einem MTree und konfigurieren Sie die clientseitige Retention Lock-Dateikontrolle vor der Replikation.

Vorgehensweise

1. Bis Sie aufgefordert werden, anders zu verfahren, führen Sie die folgenden Schritte nur auf dem Zielsystem aus.
2. Fügen Sie die DD Retention Lock Compliance-Lizenz auf dem System hinzu, wenn sie nicht vorhanden ist.
   a. Überprüfen Sie zunächst, ob die Lizenz bereits installiert ist.
      ```
      license show
      ```
   b. Wenn die Funktion RETENTION LOCK COMPLIANCE nicht angezeigt wird, installieren Sie die Lizenz.
      ```
      license add Lizenzschlüssel
      ```
      Hinweis

      Bei Lizenzschlüsseln wird nicht zwischen Groß- und Kleinschreibung unterschieden. Schließen Sie die Bindestriche bei der Eingabe der Schlüssel ein.
3. Richten Sie ein oder mehrere Security Officer-Benutzerkonten gemäß den RBAC-Regeln (Rolle Base Access Control) ein.
   a. Fügen Sie in der Systemadministrator-Rolle ein Security Officer-Konto hinzu.
      ```
      user add Benutzer role security
      ```
   b. Aktivieren Sie die Security Officer-Autorisierung.
      ```
      authorization policy set security-officer enabled
      ```
4. Konfigurieren und aktivieren Sie das System, das DD Retention Lock Compliance verwenden soll.
   Hinweis

   Die Aktivierung von DD Retention Lock Compliance erzwingt viele Einschränkungen für den Zugriff auf niedriger Ebene auf Systemfunktionen, die beim Troubleshooting verwendet werden. Nach der Aktivierung besteht die einzige Möglichkeit, DD Retention Lock Compliance zu deaktivieren, darin, das System zu initialisieren und neu zu laden, wodurch alle Daten auf dem System gelöscht werden.
   a. Konfigurieren Sie das System so, dass es DD Retention Lock Compliance verwendet.
      ```
      system retention-lock compliance configure
      ```
      Das System wird automatisch neu gestartet.
   b. Wenn der Neustart abgeschlossen ist, aktivieren Sie DD Retention Lock Compliance auf dem System.
      ```
      system retention-lock compliance enable
      ```
5. Erstellen Sie einen Replikationskontext.
   ```
   replication add source mtree://source-system-name/data/
   col1/mtree-name destination mtree://destination-system-
   name/data/col1/mtree-name
   ```

6. Führen Sie die folgenden Schritte nur auf dem Quellsystem aus.
7. Erstellen Sie einen Replikationskontext.

   ```
   replication add source mtree://source-system-name/data/
   col1/mtree-namedestination mtree://destination-system-
   name/data/col1/mtree-name
   ```

8. Initialisieren Sie den Replikationskontext.

   ```
   replication initialize mtree://destination-system-name/
   data/col1/mtree-name
   ```

9. Bestätigen Sie, dass die Replikation abgeschlossen ist.

   ```
   replication status mtree://destination-system-name/data/
   col1/mtree-namedetailed
   ```

   Nach Abschluss der Replikation meldet dieser Befehl 0 verbleibende vorkomprimierte Bytes.

Replikation eines MTree: 1:n-Topologie

Replizieren Sie einen MTree mit aktivierter DD Retention Lock Compliance von einem Quellsystem auf mehrere Zielsysteme.

Bevor Sie beginnen

Aktivieren Sie DD Retention Lock Compliance auf einem MTree und konfigurieren Sie vor der Replikation die clientseitige Retention Lock-Dateisteuerung.

Vorgehensweise

1. Bis Sie aufgefordert werden, anders zu verfahren, führen Sie die folgenden Schritte nur auf dem Zielsystem aus.
2. Fügen Sie die DD Retention Lock Compliance-Lizenz auf dem System hinzu, wenn sie nicht vorhanden ist.
   a. Überprüfen Sie zunächst, ob die Lizenz bereits installiert ist.

      ```
      license show
      ```

   b. Wenn die Funktion RETENTION LOCK COMPLIANCE nicht angezeigt wird, installieren Sie die Lizenz.

      ```
      license addLizenzschlüssel
      ```

      Hinweis

      Bei Lizenzschlüsseln wird nicht zwischen Groß- und Kleinschreibung unterschieden. Schließen Sie die Bindestriche bei der Eingabe der Schlüssel ein.

3. Richten Sie ein oder mehrere Security Officer-Benutzerkonten gemäß den RBAC-Regeln (Rolle Base Access Control) ein.
   a. Fügen Sie in der Systemadministrator-Rolle ein Security Officer-Konto hinzu.

      ```
      user addBenutzerrole security
      ```

   b. Aktivieren Sie die Security Officer-Autorisierung.

      ```
      authorization policy set security-officer enabled
      ```

4. Konfigurieren und aktivieren Sie das System, das DD Retention Lock Compliance verwenden soll.

Hinweis

Die Aktivierung von DD Retention Lock Compliance erzwingt viele Einschränkungen für den Zugriff auf niedriger Ebene auf Systemfunktionen, die beim Troubleshooting verwendet werden. Nach der Aktivierung besteht die einzige Möglichkeit, DD Retention Lock Compliance zu deaktivieren, darin, das System zu initialisieren und neu zu laden, wodurch alle Daten auf dem System gelöscht werden.

a. Konfigurieren Sie das System so, dass es DD Retention Lock Compliance verwendet.

```
system retention-lock compliance configure
```

Das System wird automatisch neu gestartet.

b. Wenn der Neustart abgeschlossen ist, aktivieren Sie DD Retention Lock Compliance auf dem System.

```
system retention-lock compliance enable
```

5. Erstellen Sie einen Replikationskontext.

```
replication add source mtree://source-system-name/data/
col1/mtree-namedestination mtree://destination-system-
name/data/col1/mtree-name
```

6. Führen Sie die folgenden Schritte nur auf dem Quellsystem aus.
7. Erstellen Sie einen Replikationskontext für jedes Zielsystem.

```
replication add source mtree://source-system-name/data/
col1/mtree-namedestination mtree://destination-system-
name/data/col1/mtree-name
```

8. Initialisieren Sie den Replikationskontext für jeden Zielsystem-MTree.

```
replication initialize mtree://destination-system-name/
data/col1/mtree-name
```

9. Vergewissern Sie sich, dass die Replikation für jedes Zielsystem abgeschlossen ist.

```
replication status mtree://destination-system-name/data/
col1/mtree-namedetailed
```

Nach Abschluss der Replikation meldet dieser Befehl 0 verbleibende vorkomprimierte Bytes.

Hinzufügen von DD Retention Lock Compliance-Schutz zu einem vorhandenen MTree-Replikationspaar

Sie können einen DD Retention Lock Compliance-Schutz zu einem vorhandenen MTree-Replikationspaar hinzufügen, das nicht für Retention Lock aktiviert ist.

Vorgehensweise

1. Bis Sie anders angewiesen werden, führen Sie die folgenden Schritte auf dem Quell- und Zielsystem aus.
2. Melden Sie sich beim DD System Manager an.

Das DD System Manager-Fenster wird mit **DD Network** im Navigationsbereich angezeigt.

3. Wählen Sie ein Data Domain-System aus.

   Blenden Sie im Navigationsbereich **DD Network** ein und wählen Sie ein System aus.

4. Fügen Sie die DD Retention Lock Governance-Lizenz hinzu, wenn sie nicht unter „Feature Licenses“ aufgeführt ist.

   a. Wählen Sie **Administration** > **Licenses**.

   b. Klicken Sie im Bereich „Licenses“ auf **Add Licenses**.

   c. Geben Sie in das Textfeld „License Key“ den Lizenzschlüssel ein.

   Hinweis

   Bei Lizenzschlüsseln wird nicht zwischen Groß- und Kleinschreibung unterschieden. Schließen Sie die Bindestriche bei der Eingabe der Schlüssel ein.

   d. Klicken Sie auf **Hinzufügen**.

5. Unterbrechen Sie den aktuellen MTree-Kontext auf dem Replikationspaar.

   `replication break mtree://destination-system-name/data/col1/mtree-name`

6. Erstellen Sie den neuen Replikationskontext.

   `replication add source mtree://source-system-name/data/col1/mtree-namedestination mtree://destination-system-name/data/col1/mtree-name`

7. Führen Sie die folgenden Schritte nur auf dem Quellsystem aus.

8. Wählen Sie einen MTree für die Aufbewahrungssperre aus.

   Klicken Sie auf die Registerkarte **Data Managemen** > **MTree** und aktivieren Sie dann das Kontrollkästchen für den MTree, den Sie für die Aufbewahrungssperre verwenden möchten. (Sie können auch einen leeren MTree erstellen und später Dateien zu diesem hinzufügen.)

9. Klicken Sie auf die Registerkarte „MTree Summary“, um Informationen für den ausgewählten MTree anzuzeigen.

10. Sperren Sie Dateien im complianceaktivierten MTree.

11. Vergewissern Sie sich, dass die Quell- und Ziel-MTrees (Replikat) identisch sind.

    `replication resync mtree://destination-system-name/data/col1/mtree-name`

12. Überprüfen Sie den Fortschritt der Neusynchronisierung.

    `replication watch mtree://destination-system-name/data/col1/mtree-name`

13. Bestätigen Sie, dass die Replikation abgeschlossen ist.

    `replication status mtree://destination-system-name/data/col1/mtree-namedetailed`
    Nach Abschluss der Replikation meldet dieser Befehl 0 verbleibende vorkomprimierte Bytes.

Konvertieren eines Sammelreplikationspaars in ein MTree-Replikationspaar

Dieses Verfahren eignet sich für Kunden, die Sammelreplikation unter DD Retention Lock Compliance in DD OS 5.2 verwendet haben und compliancefähige MTrees im Sammelreplikationspaar in MTree-Replikationspaare aktualisieren möchten.

Vorgehensweise

1. Nur auf dem Quellsystem:
   a. Erstellen Sie einen Snapshot für jeden DD Retention Lock Compliance-fähigen MTree.
      `snapshot create`*`snapshot-name`* `/data/col1/`*`mtree-name`*
   b. Synchronisieren Sie das Sammelreplikationspaar.
      `replication sync col://`*`destination-system-name`*
   c. Bestätigen Sie, dass die Replikation abgeschlossen ist.
      `replication status col://`*`destination-system-name`*`detailed`
      Nach Abschluss der Replikation meldet dieser Befehl 0 verbleibende vorkomprimierte Bytes.
   d. Zeigen Sie Snapshot-Informationen für jeden DD Retention Lock Compliance-fähigen MTree an.
      `snapshot list mtree /data/col1/`*`mtree-name`*
      Notieren Sie die Snapshot-Namen zur späteren Verwendung.
2. Nur auf dem Zielsystem:
   a. Vergewissern Sie sich, dass die Replikation abgeschlossen ist.
      `replication status mtree://`*`destination-system-name`*`/data/col1/`*`mtree-name`*`detailed`
      Nach Abschluss der Replikation meldet dieser Befehl 0 verbleibende vorkomprimierte Bytes.
   b. Zeigen Sie jeden replizierten MTree-Snapshot an, der auf das Zielsystem repliziert wird.
      `snapshot list mtree /data/col1/`*`mtree-name`*
   c. Vergewissern Sie sich, dass alle DD Retention Lock Compliance-MTree-Snapshots repliziert wurden, indem Sie die Snapshot-Namen, die hier erzeugt werden, mit denen vergleichen, die auf dem Quellsystem erzeugt werden.
      `snapshot list mtree /data/col1/`*`mtree-name`*
3. Sowohl auf dem Quell- als auch auf dem Zielsystem:
   a. Deaktivieren Sie das Dateisystem.
      `filesys disable`
   b. Unterbrechen Sie den Sammelreplikationskontext.
      `replication break col://`*`destination-system-name`*
   c. Aktivieren Sie das Dateisystem. (Security Officer-Autorisierung ist möglicherweise erforderlich.)
      `filesys enable`

d. Fügen Sie einen Replikationskontext für jeden DD Retention Lock Compliance-fähigen MTree hinzu.

```
replication add source mtree://source-system-name/data/col1/mtree-namedestination mtree://destination-system-name/data/col1/mtree-name
```

Hinweis

Quell- und Ziel-MTree-Namen müssen identisch sein.

4. Nur auf dem Quellsystem:

a. Vergewissern Sie sich, dass Quell- und Ziel-MTrees identisch sind.

```
replication resync mtree://destination-system-name
```

b. Überprüfen Sie den Fortschritt der Neusynchronisierung.

```
replication watchdestination
```

c. Bestätigen Sie, dass die Replikation abgeschlossen ist.

```
replication status mtree://destination-system-name/data/col1/mtree-namedetailed
```

Nach Abschluss der Replikation meldet dieser Befehl 0 verbleibende vorkomprimierte Bytes.

Durchführen einer Sammelreplikation

Replizieren Sie /data/col1 von einem compliancefähigen Quellsystem auf ein compliancefähiges Zielsystem.

Hinweis

Für die Sammelreplikation muss dasselbe Security Officer-Konto auf Quell- und Zielsystem verwendet werden.

Vorgehensweise

1. Bis Sie aufgefordert werden, anders zu verfahren, führen Sie die folgenden Schritte nur auf dem Quellsystem aus.
2. Melden Sie sich beim DD System Manager an.

   Das DD System Manager-Fenster wird mit **DD Network** im Navigationsbereich angezeigt.
3. Wählen Sie ein Data Domain-System aus.

   Blenden Sie im Navigationsbereich **DD Network** ein und wählen Sie ein System aus.
4. Fügen Sie die DD Retention Lock Governance-Lizenz hinzu, wenn sie nicht unter „Feature Licenses“ aufgeführt ist.

   a. Wählen Sie **Administration** > **Licenses**.

   b. Klicken Sie im Bereich „Licenses“ auf **Add Licenses**.

   c. Geben Sie in das Textfeld „License Key“ den Lizenzschlüssel ein.

Hinweis

Bei Lizenzschlüsseln wird nicht zwischen Groß- und Kleinschreibung unterschieden. Schließen Sie die Bindestriche bei der Eingabe der Schlüssel ein.

d. Klicken Sie auf **Hinzufügen**.

5. Erstellen Sie den Replikationskontext.

   ```
   replication add source col://source-system-name
   destination col://destination-system-name
   ```

6. Bis Sie aufgefordert werden, anders zu verfahren, führen Sie die folgenden Schritte nur auf dem Zielsystem aus.
7. Löschen Sie das Dateisystem.

   ```
   filesys destroy
   ```

8. Melden Sie sich beim DD System Manager an.

   Das DD System Manager-Fenster wird mit **DD Network** im Navigationsbereich angezeigt.

9. Wählen Sie ein Data Domain-System aus.

   Blenden Sie im Navigationsbereich **DD Network** ein und wählen Sie ein System aus.

10. Erstellen Sie ein Dateisystem, aktivieren Sie es aber nicht.

    ```
    filesys create
    ```

11. Erstellen Sie den Replikationskontext.

    ```
    replication add source col://source-system-name
    destination col://destination-system-name
    ```

12. Konfigurieren und aktivieren Sie das System, das DD Retention Lock Compliance verwenden soll.

    ```
    system retention-lock compliance configure
    ```

    (Das System wird automatisch neu gestartet und führt den Befehl `system retention-lock compliance enable` aus.)

13. Führen Sie die folgenden Schritte nur auf dem Quellsystem aus.
14. Initialisieren Sie den Replikationskontext.

    ```
    replication initialize source col://source-system-
    namedestination col://destination-system-name
    ```

15. Bestätigen Sie, dass die Replikation abgeschlossen ist.

    ```
    replication status col://destination-system-namedetailed
    ```

    Nach Abschluss der Replikation meldet dieser Befehl 0 verbleibende vorkomprimierte Bytes.

Hinzufügen von DD Retention Lock Compliance-Schutz zu einem vorhandenen Sammlungsreplikationspaar

Sie können DD Retention Lock Compliance-Schutz zu einem Sammelreplikationspaar hinzufügen, das ohne aktivierte DD Retention Lock Compliance auf den Quell- und Zielsystemen erstellt wurde.

Vorgehensweise

1. Bis Sie anders angewiesen werden, führen Sie die folgenden Schritte auf dem Quell- und Zielsystem aus.
2. Deaktivieren Sie die Replikation.

   `replication disable col://`*`destination-system-name`*
3. Melden Sie sich beim DD System Manager an.

   Das DD System Manager-Fenster wird mit **DD Network** im Navigationsbereich angezeigt.
4. Wählen Sie ein Data Domain-System aus.

   Blenden Sie im Navigationsbereich **DD Network** ein und wählen Sie ein System aus.
5. Bis Sie aufgefordert werden, anders zu verfahren, führen Sie die folgenden Schritte nur auf dem Quellsystem aus.
6. Konfigurieren und aktivieren Sie das System, das DD Retention Lock Compliance verwenden soll.

   `system retention-lock compliance configure`

   (Das System wird automatisch neu gestartet, indem der Befehl `system retention-lock compliance enable` ausgeführt wird.)
7. Aktivieren Sie den Replikationskontext.

   `replication enable col://`*`destination-system-name`*
8. Bis Sie aufgefordert werden, anders zu verfahren, führen Sie die folgenden Schritte nur auf dem Zielsystem aus.
9. Konfigurieren und aktivieren Sie das System, das DD Retention Lock Compliance verwenden soll.

   `system retention-lock compliance configure`

   (Das System wird automatisch neu gestartet, indem der Befehl `system retention-lock compliance enable` ausgeführt wird.)
10. Aktivieren Sie den Replikationskontext.

    `replication enable col://`*`destination-system-name`*

FastCopy

Wenn der Befehl `filesys fastcopy [retention-lock] source`*`src`*`destination`*`dest`* auf einem System mit einem DD Retention Lock Compliance-aktivierten MTree ausgeführt wird, wird das Retention Lock-Attribut während des FastCopy-Vorgangs beibehalten.

Hinweis

Wurde auf dem Ziel-MTree Retention Lock nicht aktiviert, wird das Retention Lock-Dateiattribut nicht beibehalten.

Verwenden der Befehlszeilenoberfläche

Beachten Sie die folgenden Überlegungen bei Data Domain-Systemen mit DD Retention Lock Compliance.

- Befehle, die die Compliance beeinträchtigen, können nicht ausgeführt werden. Die folgenden Befehle sind unzulässig:
  - `filesys archive unit del`*`archive-unit`*
  - `filesys destroy`
  - `mtree delete`*`mtree-path`*
  - `mtree retention-lock reset {min-retention-period`*`period`* `| max-retention-period`*`period`*`} mtree`*`mtree-path`*
  - `mtree retention-lock disable mtree`*`mtree-path`*
  - `mtree retention-lock revert`
  - `user reset`
- Für den folgenden Befehl ist eine Autorisierung durch den Security Officer erforderlich, wenn die zu löschende Lizenz für DD Retention Lock Compliance ist:
  - `license del license-feature [`*`license-feature`* `...] | license-code [`*`license-code`* `...]`
- Für den folgenden Befehl ist eine Autorisierung durch den Security Officer erforderlich, wenn DD Retention Lock Compliance auf einem im Befehl angegebenen Mtree aktiviert ist:
  - `mtree retention-lock set {min-retention-period`*`period`* `| max-retention-period`*`period`*`} mtree`*`mtree-path`*
  - `mtree rename`*`mtree-path new-mtree-path`*
- Für die folgenden Befehle ist eine Autorisierung durch den Security Officer erforderlich, wenn DD Retention Lock Compliance auf dem System aktiviert ist:
  - `alerts notify-list reset`
  - `config set timezone`*`zonename`*
  - `config reset timezone`
  - `cifs set authentication active-directory realm { [`*`dc1`* `[`*`dc2`* `...]]`
  - `license reset`
  - `ntp add timeserver`*`time server list`*
  - `ntp del timeserver`*`time server list`*
  - `ntp disable`
  - `ntp enable`
  - `ntp reset`
  - `ntp reset timeservers`
  - `replication break {`*`destination`* `| all}`
  - `replication disable {`*`destination`* `| all}`
  - `system set date`*`MMDDhhmm`*`[[`*`CC`*`]`*`YY`*`]`

Systemuhr

DD Retention Lock Compliance führt eine interne Sicherheitsuhr ein, um die böswillige Manipulation der Systemuhr zu verhindern.

Die Sicherheitsuhr überwacht die Systemuhr genau und zeichnet sie auf. Wenn innerhalb eines Jahres ein akkumulierter zweiwöchiger Unterschied zwischen der

Sicherheitsuhr und der Systemuhr vorhanden ist, wird das Dateisystem deaktiviert und kann nur von einem Security Officer wieder aufgenommen werden.

Ermitteln des Systemzeitunterschieds

Sie können den DD OS-Befehl (`system retention-lock compliance status` (Autorisierung durch einen Security Officer erforderlich) ausführen, um Informationen zur System- und Sicherheitsuhr abzurufen, einschließlich des letzten aufgezeichneten Sicherheitsuhrwerts und des akkumulierten Systemzeitunterschieds. Dieser Wert wird alle 10 Minuten aktualisiert.

Entfernen der Systemuhrunterschiede

Uhrabweichungen werden jedes Mal aktualisiert, wenn die Sicherheitsuhr einen neuen Wert für die Systemuhr erfasst. Nach einem Jahr wird die Abweichung auf 0 zurückgesetzt.

Sie können jederzeit den DD OS-Befehl `system set date`*MMTThhmm*[[*JJ*]*JJ*] ausführen, um Uhrzeit der Systemuhr festzulegen (Security Officer-Autorisierung erforderlich). Wenn die Uhrabweichung den Standardwert (2 Wochen) überschreitet, wird das Dateisystem deaktiviert. Gehen Sie folgendermaßen vor, um das Dateisystem neu zu starten und die Abweichung zwischen Sicherheits- und Systemuhr zu entfernen.

Vorgehensweise

1. Aktivieren Sie in der Systemkonsole das Dateisystem.

   ```
   filesys enable
   ```

2. Bestätigen Sie in der Eingabeaufforderung, dass Sie den Befehl `filesys enable` beenden und prüfen möchten, ob das Systemdatum korrekt ist.
3. Zeigen Sie das Datum an.

   ```
   system show date
   ```

4. Wenn das Datum nicht korrekt ist, legen Sie das korrekte Datum fest (Security Officer-Autorisierung erforderlich) und bestätigen Sie dieses.

   ```
   system set dateMMTThhmm[[JJ]JJ]
   system show date
   ```

5. Aktivieren Sie das Dateisystem erneut.

   ```
   filesys enable
   ```

6. Fahren Sie in der Eingabeaufforderung mit dem Aktivierungsverfahren fort.
7. Es wird eine Security Officer-Eingabeaufforderung angezeigt. Führen Sie die Security Officer-Autorisierung durch, um das Dateisystem zu starten. Die Sicherheitsuhr wird automatisch auf das aktuelle Systemdatum aktualisiert.

KAPITEL 21

DD Encryption

Inhalt dieses Kapitels:

Übersicht über die DD-Verschlüsselung

Die Datenverschlüsselung schützt Benutzerdaten, wenn das Data Domain-System gestohlen wird oder die physischen Speichermedien während der Übertragung verloren gehen, und eliminiert die versehentliche Gefährdung eines ausgefallenen Laufwerks, wenn es ersetzt wird.

Wenn Daten über eines der unterstützten Protokolle (NFS, CIFS, DD VTL, DD Boost und NDMP Tape Server) in das Data Domain-System eingehen, wird der Stream segmentiert, mit einem Fingerabdruck versehen und dedupliziert (globale Komprimierung). Dann werden sie in Komprimierungsregionen mit mehreren Segmenten gruppiert, lokal komprimiert und verschlüsselt, bevor sie auf der Festplatte gespeichert werden.

Nachdem die Data-at-Rest-Verschlüsselung aktiviert wurde, werden alle Daten, die beim Data Domain-System eingehen, mit dieser Funktion verschlüsselt. Sie können die Verschlüsselung nicht auf einer granulareren Ebene aktivieren.

⚠ ACHTUNG

Daten, die gespeichert wurden, bevor die DD-Verschlüsselungsfunktion aktiviert wird, werden nicht automatisch verschlüsselt. Um alle Daten auf dem System zu schützen, müssen Sie unbedingt die Option zum Verschlüsseln vorhandener Daten aktivieren, wenn Sie die Verschlüsselung konfigurieren.

Weitere Hinweise:
Ab DD OS 5.5.1.0 wird die Data-at-Rest-Verschlüsselung für Systeme mit aktivierter DD Extended Retention-Funktion mit einer einzigen Aufbewahrungseinheit unterstützt. Ab 5.5.1.0 unterstützt DD Extended Retention nur eine einzige Aufbewahrungseinheit, sodass unter 5.5.1.0 oder höher eingerichtete Systeme diese Einschränkung problemlos einhalten. Systeme, die vor 5.5.1.0 eingerichtet wurden, können jedoch über mehr als eine Aufbewahrungseinheit verfügen. Diese können aber erst mit der Data-at-Rest-Verschlüsselung genutzt werden, bis alle Aufbewahrungseinheiten bis auf eine entfernt wurden oder Daten in eine Aufbewahrungseinheit verschoben oder migriert wurden.

Der Befehl `filesys encryption apply-changes` wendet alle Änderungen an der Verschlüsselungskonfiguration während des nächsten Bereinigungszyklus auf alle im Dateisystem vorhandenen Daten an. Weitere Informationen über Befehle finden Sie im *Data Domain Operating System Command Reference Guide*.

Die Data-at-Rest-Verschlüsselung unterstützt alle aktuell unterstützten Backupanwendungen, die in den Backupkompatibilitätsleitfäden beschrieben sind, die über den Onlinesupport unter http://support.emc.com zur Verfügung stehen.

Data Domain Replicator kann mit Verschlüsselung verwendet werden und ermöglicht, dass Daten mithilfe der Sammel-, Verzeichnis-, MTree- oder anwendungsspezifischen Managed File Replication mit den verschiedenen Topologien repliziert werden. Jede Replikationsform arbeitet auf einzigartige Weise mit der Verschlüsselung und bietet dasselbe Maß an Sicherheit. Weitere Informationen finden Sie im Abschnitt zur Verwendung der Data-at-Rest-Verschlüsselung mit Replikation.

Dateien, die mithilfe von Data Domain Retention Lock gesperrt wurden, können gespeichert, verschlüsselt und repliziert werden.

Die AutoSupport-Funktion enthält Informationen über den Status der Verschlüsselung auf dem Data Domain-System:

- Ob die Verschlüsselung aktiviert ist oder nicht
- Der Key Manager wirksam ist und welche Schlüssel verwendet werden
- Der konfigurierte Verschlüsselungsalgorithmus
- Der Status des Dateisystems

Konfigurieren der Verschlüsselung

Dieses Verfahren schließt die Konfiguration eines Schlüsselmanagers ein.

Wenn der Verschlüsselungsstatus auf der Registerkarte **Data Management** > **File System** > **Encryption** als „Not Configured“ angezeigt wird, klicken Sie auf **Configure**, um die Verschlüsselung auf dem Data Domain-System einzurichten.

Hinweis

Die Systempassphrase muss festgelegt werden, um die Verschlüsselung zu aktivieren.

Stellen Sie folgende Informationen bereit:

- Algorithmus
  - Wählen Sie einen Verschlüsselungsalgorithmus aus der Drop-down-Liste aus oder akzeptieren Sie den Standard AES 256-Bit (CBC).
    AES 256-Bit Galois/Counter Mode (GCM) ist der sicherste Algorithmus, ist jedoch deutlich langsamer als der CBC-Modus (Cipher Block Chaining).
  - Legen Sie fest, welche Daten verschlüsselt werden sollen: vorhandene und neue Daten oder nur neue Daten. Vorhandene Daten werden beim ersten Bereinigungszyklus verschlüsselt, nachdem das Dateisystem neu gestartet wurde. Die Verschlüsselung vorhandener Daten kann länger dauern als ein standardmäßiger Bereinigungsvorgang des Dateisystems.
- Key Manager (wählen Sie einen der drei aus)
  - Embedded Key Manager
    Standardmäßig wird der Data Domain Embedded Key Manager verwendet, wenn Sie das Dateisystem neu starten, es sei denn, Sie konfigurieren den RSA DPM Key Manager.

    Sie können die Schlüsselrotation aktivieren oder deaktivieren. Geben Sie bei Aktivierung ein Rotationsintervall zwischen 1 und 12 Monaten ein.
  - RSA DPM Key Manager
  - SafeNet KeySecure Key Manager

  Hinweis

  Informationen über die Funktionsweise des Embedded Key Manager, des RSA DPM Key Manager und des SafeNet KeySecure Key Manager finden Sie im Abschnitt über Key-Management.

In der Übersicht werden die ausgewählten Konfigurationswerte angezeigt. Überprüfen Sie die Werte auf ihre Richtigkeit. Um einen Wert zu ändern, klicken Sie auf **Back**, um zu der Seite zu navigieren, auf der der Wert eingegeben wurde, und ändern Sie ihn.

Es ist ein Systemneustart erforderlich, um die Verschlüsselung zu aktivieren. Um die neue Konfiguration zu übernehmen, starten Sie das Dateisystem neu.

Hinweis

Es kann zu Anwendungsunterbrechungen kommen, während das Dateisystem neu gestartet wird.

Informationen über das Key-Management

Chiffrierschlüssel bestimmen die Ausgabe des kryptografischen Algorithmus. Sie werden zusätzlich durch eine Passphrase geschützt, mit der der Chiffrierschlüssel verschlüsselt wird, bevor er auf mehreren Speicherorten auf der Festplatte abgelegt wird. Die Passphrase wird vom Benutzer erzeugt und kann nur von einem Administrator und einem Security Officer zusammen geändert werden.

Ein Key Manager ist für die Erzeugung, die Verteilung und das Lifecycle-Management mehrerer Chiffrierschlüssel verantwortlich. Ein Data Domain-System kann entweder den Embedded Key Manager oder den RSA Data Protection Manager (DPM) Key Manager oder den SafeNet KeySecure Key Manager verwenden. Unterstützung für das Key Management Interoperability Protocol (KMIP) wird mit DD OS 6.1 eingeführt.

Es kann jeweils nur ein Key Manager verwendet werden. Wenn die Verschlüsselung auf einem Data Domain-System aktiviert wird, ist standardmäßig der Embedded Key Manager aktiv. Wenn Sie den RSA DPM oder SafeNet KeySecure Key Manager konfigurieren, ersetzt er den Embedded Key Manager und bleibt aktiv, bis Sie ihn deaktivieren. Ein Dateisystemneustart ist erforderlich, damit ein neuer Key Manager betriebsbereit ist.

Der Embedded und der DPM Key Manager bieten mehrere Schlüssel, obwohl das System nur jeweils einen Schlüssel verwendet, um die Daten zu verschlüsseln, die in einem Data Domain-System eingehen. Wenn der externe Key Manager konfiguriert und aktiviert ist, nutzen die Data Domain-Systeme die vom RSA DPM Key Manager Server bereitgestellten Schlüssel. Wenn derselbe DPM Key Manager mehrere Data Domain-Systeme verwaltet, verfügen alle Systeme über denselben aktiven Schlüssel (wenn sie dieselbe Schlüsselklasse verwenden), sofern sie synchronisiert sind und das Dateisystem neu gestartet wurde. Der Embedded Key Manager erzeugt die Schlüssel intern.

Beide Key Managers rotieren Schlüssel und unterstützen maximal 254 Schlüssel. Beim Embedded Key Manager können Sie festlegen, wie viele Monate ein Schlüssel wirksam ist, bevor er ersetzt wird (nachdem das Dateisystem neu gestartet wurde). Der RSA DPM Key Manager rotiert Schlüssel regelmäßig, abhängig von der Schlüsselklasse. Im Embedded Key Manager wird die Schlüsselrotation im Data Domain-System verwaltet. Im Key Manager wird die Schlüsselrotation auf dem externen Key Manager-Server verwaltet.

KeySecure

KeySecure 8.5, ein KMIP-kompatibler Key Manager von Safenet Inc/Gemalto KeySecure, wird unterstützt. Um den KMIP Key Manager verwenden zu können, müssen Benutzer den Key Manager und das Data Domain-System/DD VE konfigurieren, sodass sie einander vertrauen. Benutzer müssen vorab Schlüssel im Key Manager erstellen. Ein Data Domain-System ruft diese Schlüssel und ihre Zustände aus KeySecure ab, nachdem eine sichere TLS-Verbindung hergestellt wurde. Im *Data Domain Operating System and Gemalto KeySecure Integration Guide* finden Sie weitere Informationen zur Erstellung von Schlüsseln und ihrer Verwendung in einem Data Domain-System.

Korrigieren verloren gegangener oder beschädigter Schlüssel

Erstellen Sie eine Datei, die alle aktuellen Chiffrierschlüssel des Systems enthält. Ihr Supportanbieter kann mithilfe dieser Datei Schlüssel zurück auf Ihr System importieren, falls diese verloren gehen oder beschädigt werden. Es wird empfohlen, dass Sie regelmäßig eine Exportdatei erstellen.

Sie werden aufgefordert, die Anmeldedaten des Security Officer einzugeben, um Schlüssel zu exportieren. Für zusätzliche Schlüsseldateisicherheit können Sie eine Passphrase verwenden, die sich von der in einem Data Domain-System verwendeten unterscheidet. Nach dem Exportieren wird empfohlen, die Schlüsseldatei in einem sicheren Dateiserver zu speichern, auf den nur autorisierte Benutzer zugreifen können. Sie müssen sich die für die Schlüsseldatei verwendete Passphrase merken. Wenn die Passphrase verloren geht oder vergessen wird, kann das Data Domain-System die Schlüssel nicht importieren und wiederherstellen. Geben Sie Folgendes ein:

```
# filesys encryption keys export
```

Key Manager-Support

Alle Key Manager unterstützen alle DD OS-Dateisystemprotokolle.

Replikation
Wenn Data Domain-Systeme für die Verzeichnis-MTree-Replikation konfiguriert sind, konfigurieren Sie jedes Data Domain-System separat. Die beiden Systeme können entweder dieselbe oder verschiedene Schlüsselklassen und denselben oder verschiedenen Key Managers verwenden.

Für die Sammelreplikationskonfiguration muss das Data Domain-System auf der Quelle konfiguriert werden. Nach einer Replikationsunterbrechung muss das ursprüngliche Data Domain-Systemreplikat für den Key Manager konfiguriert werden. Falls nicht, wird das Data Domain-System auch weiterhin den letzten bekannten Schlüssel verwenden.

Arbeiten mit dem RSA DPM Key Manager

Wenn RSA DPM Key Manager konfiguriert und aktiviert ist, nutzen die Data Domain-Systeme die vom RSA DPM Key Manager Server bereitgestellten Schlüssel. Wenn derselbe DPM Key Manager mehrere Data Domain-Systeme managt, verfügen alle Systeme über denselben aktiven Schlüssel (wenn sie dieselbe Schlüsselklasse verwenden), sofern sie synchronisiert sind und das Dateisystem neu gestartet wurde. Die Schlüsselrotation wird auf dem RSA DPM Key Manager Server gemanagt.

Wenn RSA DPM Key Manager konfiguriert und aktiviert ist, nutzen die Data Domain-Systeme die vom RSA DPM Key Manager Server bereitgestellten Schlüssel. Wenn derselbe DPM Key Manager mehrere Data Domain-Systeme managt, verfügen alle Systeme über denselben aktiven Schlüssel (wenn sie dieselbe Schlüsselklasse verwenden), sofern sie synchronisiert sind und das Dateisystem neu gestartet wurde. Die Schlüsselrotation wird auf dem RSA DPM Key Manager Server gemanagt.

Status des Chiffrierschlüssels
Ein Activated-RW-Schlüssel ist immer gültig. Wenn der aktive Schlüssel beschädigt wird, stellt RSA DPM Key Manager einen neuen Schlüssel bereit. Wenn das Data Domain-System den neuen Schlüssel erkennt, wird eine Warnmeldung ausgegeben, damit der Administrator das Dateisystem neu startet.

Abgelaufene Schlüssel werden zu schreibgeschützten Schlüsseln für die vorhandenen Daten auf dem Data Domain-System und ein neuer aktiver Schlüssel wird auf alle neuen Daten angewendet, die empfangen werden. Wenn ein Schlüssel beschädigt wird, werden die vorhandenen Daten mithilfe des neuen Chiffrierschlüssels erneut verschlüsselt, nachdem das Dateisystem bereinigt wurde. Wenn die Höchstzahl an Schlüsseln erreicht wird, müssen nicht verwendete Schlüssel gelöscht werden, um Speicherplatz für neue Schlüssel freizugeben.

Um Informationen über die Chiffrierschlüssel anzuzeigen, die sich auf dem Data Domain-System befinden, öffnen Sie den DD System Manager und wechseln Sie zur Registerkarte **Data Management** > **File System** > **Encryption** . Schlüssel werden nach ID auf der Registerkarte „Encryption“ im Bereich **Encryption Keys** aufgelistet. Die folgenden Informationen werden für jeden Schlüssel bereitgestellt: wann ein Schlüssel erstellt wurde, wie lange er gültig ist, der Schlüsseltyp (RSA DPM oder Data Domain), der Status (siehe „Von Data Domain unterstützte Status von DPM-Chiffrierschlüsseln“) und die nachkomprimierte Größe. Wenn das System für Extended Retention lizenziert ist, werden außerdem die folgenden Felder angezeigt:

Active Size (post comp)

Die Menge des physischen Speicherplatzes, der auf dem aktiven Tier mit dem Schlüssel verschlüsselt ist.

Retention Size (post comp)

Die Menge des physischen Speicherplatzes, der auf dem Aufbewahrungs-Tier mit dem Schlüssel verschlüsselt ist.

Klicken Sie auf eine Schlüssel MUID und vom System werden die folgenden Informationen zu dem Schlüssel im Dialogfeld „Key Details“ angezeigt: Tier/Einheit (Beispiel: Active, Retention-unit-2), Erstellungsdatum, Gültigkeitsdatum, Status (siehe „Von Data Domain unterstützte Status von DPM-Chiffrierschlüsseln“) und die Größe nach Komprimierung. Klicken Sie auf Close, um das Dialogfeld zu schließen.

Tabelle 191 Von Data Domain unterstützte Status von DPM-Chiffrierschlüsseln

Status	Definition
Pending-Activated	Der Schlüssel wurde gerade erstellt. Nach einem Neustart des Dateisystems erhält der Schlüssel den Status „Activated-RW“.
Activated-RW and Activated-RO	Mit „Activated-RW“ und „Activated-RO“ werden die Daten gelesen, die mit dem entsprechenden Schlüssel verschlüsselt wurden. „Activated-RW“ ist der zuletzt aktivierte Schlüssel.
De-Activated	in Schlüssel wird deaktiviert, wenn die aktuelle Zeit die Gültigkeitsdauer überschreitet. Der Schlüssel wird zum Lesen von Daten verwendet.
Compromised	Der Schlüssel kann nur zur Entschlüsselung verwendet werden. Nachdem alle Daten, die mit dem beschädigten Schlüssel verschlüsselt waren, erneut verschlüsselt wurden, ändert sich der Status auf „Destroyed Compromised“. Die Schlüssel werden erneut verschlüsselt, wenn eine

Tabelle 191 Von Data Domain unterstützte Status von DPM-Chiffrierschlüsseln (Fortsetzung)

Status	Definition
	Dateisystembereinigung ausgeführt wird. Sie können einen „Destroyed Compromised“-Schlüssel löschen, falls erforderlich.
Marked-For-Destroy	Sie haben den Schlüssel als „Destroyed“ markiert, damit die Daten erneut verschlüsselt werden.
Destroyed	Nachdem sämtliche Daten, die mit diesem Schlüssel verschlüsselt waren, erneut verschlüsselt wurden, ändert DD OS den Status von „Marked-For-Destroy“ auf „Destroyed“. Falls der gelöschte Schlüssel beschädigt war, ändert sich der Status auf „Compromised-Destroyed“. Sie können Schlüssel mit dem Status „Destroyed“ und „Compromised-Destroyed“ löschen. **Hinweis** Ein Schlüssel wird erst dann aus dem Data Domain-System gelöscht, wenn ein Bereinigungsvorgang ausgeführt und abgeschlossen wird.

Aufrechterhalten der Synchronisierung von Schlüsseln mit dem RSA DPM Key Manager

Eine automatische Schlüsselsynchronisierung wird täglich um Mitternacht durchgeführt. Eine manuelle Schlüsselsynchronisierung ist nur dann erforderlich, wenn Sie nicht auf die geplante Synchronisierung warten können. Wann immer neue Schlüssel auf dem Data Domain-System synchronisiert werden, wird eine Warnmeldung erzeugt. Diese Warnmeldung wird gelöscht, nachdem das Dateisystem neu gestartet wurde.

Nachdem der RSA DPM Key Manager Server neue Schlüssel erzeugt, klicken Sie auf die Schaltfläche **Sync**, damit die Liste „Encryption Key“ auf der Registerkarte „Encryption“ von Data Domain System Manager angezeigt wird.

Hinweis

Ein Dateisystemneustart ist erforderlich, wenn sich Schlüssel seit der letzten Synchronisierung verändert haben.

Vorgehensweise

1. Wählen Sie im DD System Manager das Data Domain-System aus, mit dem Sie im Navigationsbereich arbeiten.

   Hinweis

   Führen Sie stets DD System Manager-Aufgaben auf dem System aus, das Sie im Navigationsbereich ausgewählt haben.

2. Wählen Sie **Data Management** > **File System** > **Encryption**.

3. Wählen Sie im Abschnitt „Encryption Keys“ den Schlüssel **RSA** aus und klicken Sie dann auf **Sync**.

Entfernen eines Schlüssels (RSA DPM Key Manager)

Entfernen Sie einen Schlüssel, wenn Sie keine Daten mit ihm verschlüsseln möchten. Für dieses Verfahren sind Security Officer-Anmeldedaten erforderlich.

Hinweis

Weitere Informationen über den Security Officer finden Sie in den Abschnitten zum Erstellen von lokalen Benutzern und zum Aktivieren der Sicherheitsautorisierung.

So ändern Sie einen RSA DPM-Schlüssel in einen Status, in dem er gelöscht werden kann:

Vorgehensweise

1. Deaktivieren Sie den Schlüssel auf dem RSA DPM-Server.
2. Starten Sie das Dateisystem neu, damit der Schlüssel auf dem Data Domain-System deaktiviert wird.
3. Klicken Sie im DD System Manager auf **Data Management** > **File System** > **Encryption**.
4. Wählen Sie im Abschnitt „Encryption Keys“ den Schlüssel, der gelöscht werden soll, aus der Liste aus.
5. Klicken Sie auf **Destroy...**.

   Das System zeigt das Dialogfeld „Destroy“ an, das den Tier und den Status für den Schlüssel beinhaltet.
6. Geben Sie Ihren Security Officer-Benutzernamen und das entsprechende Passwort ein.
7. Bestätigen Sie, dass Sie den Schlüssel löschen möchten, indem Sie auf **Destroy** klicken.

   Hinweis

   Nachdem eine Dateisystembereinigung ausgeführt wurde, ändert sich der Schlüsselstatus in „Destroyed“.

Löschen eines Schlüssels

Sie können Key Manager-Schlüssel entfernen, die sich im Status „Destroyed“ oder „Compromised-Destroyed“ befinden. Sie müssen einen Schlüssel jedoch nur löschen, wenn die Anzahl der Schlüssel mit maximale Grenze von 254 erreicht hat. Für dieses Verfahren sind Security Officer-Anmeldedaten erforderlich.

Hinweis

Damit der Status „Destroyed“ erreicht wird, muss das Verfahren zum Löschen eines Schlüssels (entweder für den integrierten Key Manager oder den RSA DPM Key Manager) für den Schlüssel durchgeführt und eine Systembereinigung ausgeführt werden.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Encryption**.

2. Wählen Sie im Abschnitt „Encryption Keys“ den oder die zu löschenden Schlüssel aus der Liste aus.
3. Kicken Sie auf **Delete...**.

   Das System zeigt den zu löschenden Schlüssel sowie den Tier und den Status für den Schlüssel an.
4. Geben Sie Ihren Security Officer-Benutzernamen und das entsprechende Passwort ein.
5. Bestätigen Sie, dass Sie den Schlüssel löschen möchten, indem Sie auf **Delete** klicken.

Arbeiten mit dem integrierten Key Manager

Wenn der integrierte Key Manager ausgewählt ist, erstellt das Data Domain-System eigene Schlüssel.

Nachdem die Schlüsselrotations-Policy konfiguriert ist, wird bei der nächsten Rotation automatisch ein neuer Schlüssel erstellt. Sie werden mit einer Warnmeldung über die Erstellung eines neuen Schlüssels informiert. Sie müssen das Dateisystem neu starten, um den neuen Schlüssel zu aktivieren und den alten Schlüssel zu deaktivieren. Sie können die Schlüsselrotations-Policy deaktivieren, indem Sie auf die Schaltfläche zum Deaktivieren klicken, die dem Rotationsstatus des integrierten Key Manager zugeordnet ist.

Erstellen eines Schlüssels (Embedded Key Manager)

Erstellen Sie einen Chiffrierschlüssel für den Embedded Key Manager.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **DD Encryption** aus.
2. Klicken Sie im Abschnitt „Encryption Keys“ auf **Create...**.
3. Geben Sie Ihren Security Officer-Benutzernamen und das entsprechende Passwort ein.
4. Klicken Sie auf **Restart the filesystem now** aus, wenn Sie das Dateisystem neu starten möchten.

   Ein neuer Data Domain-Schlüssel wird erstellt. Nachdem das Dateisystem neu gestartet wurde, wird der vorherige Schlüssel deaktiviert und der neue Schlüssel aktiviert.
5. Klicken Sie auf **Create**.

Löschen eines Schlüssels (integrierter Key Manager)

Löschen Sie einen Chiffrierschlüssel für den integrierten Key Manager.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Encryption**.
2. Wählen Sie im Abschnitt „Encryption Keys“ den Schlüssel, der gelöscht werden soll, aus der Liste aus.
3. Klicken Sie auf **Destroy...**.

   Das System zeigt das Dialogfeld „Destroy“ an, das den Tier und den Status für den Schlüssel beinhaltet.
4. Geben Sie Ihren Security Officer-Benutzernamen und das entsprechende Passwort ein.

5. Bestätigen Sie, dass Sie den Schlüssel löschen möchten, indem Sie auf **Destroy** klicken.

Hinweis

Nachdem ein Bereinigungsvorgang für das Dateisystem ausgeführt wurde, wird der Status des Schlüssels in „Destroyed“ geändert.

Arbeiten mit KeySecure Key Manager

Der KeySecure Key Manager unterstützt externe Key Manager durch die Verwendung des Key Management Interoperability Protocol (KMIP) und managt zentral Chiffrierschlüssel auf einer einzigen, zentralen Plattform.

- Schlüssel werden vorab im Key Manager erstellt.
- Der KMIP Key Manager kann nicht auf Systemen aktiviert werden, für die Verschlüsselung auf einer oder mehreren Cloudeinheiten aktiviert ist.

Verwenden von DD System Manager zum Einrichten und Managen von KeySecure Key Manager

In diesem Abschnitt wird beschrieben, wie Sie Data Domain System Manager (DD SM) verwenden, um KeySecure Key Manager zu managen.

Erstellen eines Schlüssels für KeySecure Key Manager

Erstellen Sie einen Chiffrierschlüssel für KeySecure Key Manager (KMIP).

Vorgehensweise

1. Scrollen Sie nach unten, um die Tabelle **Key Manager Encryption Keys** anzuzeigen.
2. Klicken Sie auf **Add**, um einen neuen Key Manager-Verschlüsselungsschlüssel zu erstellen.
   a. Geben Sie den Benutzernamen und das Passwort für den Security Officer ein.
   b. Klicken Sie auf **Restart the filesystem now**.
   c. Klicken Sie auf **Create**.
3. Klicken Sie auf **Restart the file system now**, damit die Änderungen wirksam werden.

   Ein neuer KIMP-Schlüssel wird erstellt. Nachdem das Dateisystem neu gestartet wurde, wird der vorherige Schlüssel deaktiviert und der neue Schlüssel aktiviert.

Ändern des Status eines vorhandenen Schlüssels in KeySecure Key Manager

Verwenden Sie DD SM, um den Status eines vorhandenen KIMP-Chiffrierschlüssels zu ändern.

Bevor Sie beginnen

Überprüfen Sie die Bedingungen für die Änderung eines Schlüsselstatus:

- Wenn bereits ein Schlüssel vorhanden (aktiv) ist und ein neuer Schlüssel erstellt wird, ändert sich der Status des neuen Schlüssels in `Pending-Activated`, bis der Benutzer das Dateisystem neu startet.
- Benutzer können einen Schlüssel mit dem Status `Activated-RW` nur deaktivieren, wenn ein `Pending-Activated`-Schlüssel als Ersatz vorhanden ist.
- Ein Schlüssel mit dem Status `Pending-Activated` wird nur deaktiviert, wenn ein anderer `Pending-Activated`-Schlüssel als Ersatz vorhanden ist.
- Ein Schlüssel in einem `Activated-RO`-Schlüssel erfordert keine Bedingungen. Sie können ihn jederzeit deaktivieren.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **DD Encryption** aus.
2. Scrollen Sie nach unten, um die Tabelle **Key Manager Encryption Keys** anzuzeigen.
3. Wählen Sie den entsprechenden Schlüssel aus der Tabelle **Key Manager Encryption Keys**.
4. So deaktivieren Sie einen Schlüssel:
   a. Klicken Sie auf einen beliebigen Schlüssel, der den Status `Activated` aufweist.
   b. Geben Sie den Benutzernamen und das Passwort für den Security Officer ein.
   c. Klicken Sie auf **DEACTIVATE**.

Abbildung 17 Ändern des KMIP-Schlüssels in einen deaktivierten Status

5. Klicken Sie auf **Restart the filesystem now**.

Ergebnisse

Der Status eines vorhandenen Schlüssels wird geändert.

Konfigurieren von KeySecure Key Manager

Verwenden Sie DD SM, um die Policy für die Schlüsselrotation aus dem Data Domain-System festzulegen.

Bevor Sie beginnen

Bestätigen Sie den gewünschten Zeitraum für die Schlüsselrotation (Wochen oder Monate), das Startdatum der Schlüsselrotation und das Datum der nächsten Schlüsselrotation.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **DD Encryption** aus.
2. Klicken Sie im Bereich **Key Management** auf **Configure**. Das Dialogfeld **Change Key Manager** wird geöffnet.
3. Geben Sie Ihren Security Officer-Benutzernamen und das entsprechende Passwort ein.
4. Wählen Sie **KeySecure Key Manager** aus dem Drop-Down-Menü **Key Manager Type**. Die Change Key Manager-Informationen werden angezeigt.
5. Legen Sie die Policy für die Schlüsselrotation fest:

   Hinweis

   Die Policy für die Rotation wird in Wochen und Monaten angegeben. Das minimale Inkrement für die Policy für die Schlüsselrotation ist eine Woche und das maximale Inkrement für die Policy für die Schlüsselrotation sind 52 Wochen (oder 12 Monate).

   a. Aktivieren Sie die Policy für die Schlüsselrotation. Ändern Sie die Schaltfläche **Enable Key rotation policy** in „Enable“.
   b. Geben Sie die entsprechenden Datumsangaben im Feld „Key rotation schedule“ ein.
   c. Wählen Sie die entsprechende Anzahl von Wochen oder Monaten im Drop-Down-Menü **Weeks** oder **Months** .
   d. Klicken Sie auf **OK**.
   e. Klicken Sie auf **Restart the filesystem now**, wenn Sie das Dateisystem neu starten möchten, damit die Änderungen sofort wirksam werden (siehe Abbildung 3).

Ergebnisse

Die Policy für die Schlüsselrotation wird festgelegt oder geändert.

Verwenden der Data Domain-CLI zum Managen von KeySecure Key Manager

In diesem Abschnitt wird beschrieben, wie Sie KeySecure Key Manager über die CLI managen.

Erstellen eines neuen aktiven Schlüssels in KeySecure Key Manager

Verwenden Sie die Data Domain-Befehlszeilenoberfläche, um einen neuen aktiven Schlüssel zu erstellen.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie über die entsprechenden Benutzeranmeldedaten verfügen. Die Sicherheitsrolle ist erforderlich, um diese Befehle auszuführen.

Vorgehensweise

1. Melden Sie sich beim Data Domain-System mit der Sicherheitsrolle an:

   Benutzername: `sec`

   Passwort: `<security officer password>`

2. Erstellen Sie einen neuen aktiven Schlüssel:

   ```
   # filesys encryption key-manager keys create
   ```

3. Es wird eine Ausgabe ähnlich der folgenden angezeigt:

   ```
   New encryption key was successfully created.
   The filesystem must be restarted to activate the new key.
   ```

Ergebnisse

Ein neuer aktiver Schlüssel wird erstellt.

Ändern des Status eines vorhandenen Schlüssels in KeySecure Key Manager

Verwenden Sie die Data Domain-Befehlszeilenoberfläche, um den Status eines vorhandenen Schlüssels in einen deaktivierten Status zu ändern.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie über die entsprechenden Benutzeranmeldedaten verfügen. Die Sicherheitsrolle ist erforderlich, um diese Befehle auszuführen.

Vorgehensweise

1. Melden Sie sich beim Data Domain-System mit der Sicherheitsrolle an:

   Benutzername: `sec`

   Passwort: `<security officer password>`

2. Ändern Sie den Status eines vorhandenen Schlüssels:

   ```
   # filesys encryption key-manager keys modify{<key-id> | muid
   <key-muid>}state deactivated
   ```

   Beispiel:

   ```
   # filesys encryption key-manager keys modify muid
   740D711374A8C964A62817B4AD193C8DC44374A6ED534C85642782014F2E9D
   41 state deactivated
   ```

3. Es wird eine Ausgabe ähnlich der folgenden angezeigt:

   ```
   Key state modified.
   ```

Ergebnisse

Der Status eines vorhandenen Schlüssels wird geändert.

Festlegen oder Zurücksetzen einer Policy für die Schlüsselrotation in KeySecure Key Manager

Verwenden Sie die Data Domain-Befehlszeilenoberfläche, um die Policy für die Schlüsselrotation auf dem Data Domain-System festzulegen und so Schlüssel regelmäßig zu rotieren. Beachten Sie, dass die Policy für die Rotation in Wochen und Monaten angegeben wird. Das minimale Inkrement für die Policy für die Schlüsselrotation ist eine Woche und das maximale Inkrement für die Policy für die Schlüsselrotation sind 52 Wochen (oder 12 Monate).

Bevor Sie beginnen

Stellen Sie sicher, dass Sie über die entsprechenden Benutzeranmeldedaten verfügen. Die Sicherheitsrolle ist erforderlich, um diese Befehle auszuführen.

Vorgehensweise

1. Melden Sie sich beim Data Domain-System mit der Sicherheitsrolle an:

   Benutzername: `sec`

   Passwort: `<security officer password>`

2. Legen Sie eine Policy für die Schlüsselrotation zum ersten Mal fest. In unserem Beispiel legen wir die Policy für die Rotation auf **drei Wochen** fest:

```
# filesys encryption key-manager set key-rotation-policy
                  {every <n> {weeks | months} | none}
```

Beispiel:

```
# filesys encryption key-manager set key-rotation-policy
every 3 weeks
```

Output that is similar to the following appears:

```
Key-rotation-policy is set. Encryption key will be rotated
every 3 weeks.
```

3. Anschließend führen Sie diesen Befehl aus, wenn Sie die vorhandene Policy für die Schlüsselrotation ändern möchten. In unserem Beispiel ändern wir die Policy für die Rotation von **drei Wochen** auf **vier Monate**:

Hinweis

Melden Sie sich beim Data Domain-System mit der Sicherheitsrolle an (wobei der Benutzername `sec` und das Passwort <`security officer password`> ist).

```
# filesys encryption key-manager reset [key-rotation-policy]
```

Beispiel:

```
filesys encryption key-manager set key-rotation-policy every
4 months
```

Output that is similar to the following appears:

```
Key-rotation-policy is set. Encryption key will be rotated
every 4 months.
```

4. Zeigen Sie die aktuelle Policy für die Schlüsselrotation an oder überprüfen Sie, ob die Policy korrekt festgelegt ist:

```
# filesys encryption key-manager show
```

Output that is similar to the following appears:

```
The current key-manager configuration is:
Key Manager:                                Enabled
Server Type:                                KeySecure
Server:                                     <IP address of
KMIP server>
Port:                                       5696
Fips-mode:                                  enabled
Status:                                     Online
Key-class:                                  <key-class>
KMIP-user:                                  <KMIP username>
Key rotation period:                        2 months
Last key rotation date:                     03:14:17 03/19
2018
Next key rotation date:                     01:01:00 05/17
2018
```

Ergebnisse

Die Policy für die Schlüsselrotation wird festgelegt oder geändert.

Funktionsweise des Bereinigungsvorgangs

Die Verschlüsselung wirkt sich auf die Performance von Bereinigungsvorgängen aus, wenn die Daten, die mit dem Compromised- oder Marked-For-Destroyed-Schlüssel verschlüsselt sind, erneut über den Activated-RW-Schlüssel verschlüsselt werden.

Am Ende des Bereinigungsvorgangs gibt es keine Daten mehr, die mit dem Comprimised- oder Marked-For-Destroyed-Schlüssel verschlüsselt sind. Außerdem sind alle Daten, die vom Bereinigungsvorgang geschrieben werden, mit dem Activated-RW-Schlüssel verschlüsselt.

Key Manager-Einrichtung

Befolgen Sie die Anweisungen für den Typ des Key Managers, den Sie verwenden.

Weitere Informationen über das SafeNet KeySecure Key Manager-Setup finden Sie im *Data Domain Operating System and Gemalto KeySecure Integration Guide*.

Konfiguration der RSA DPM Key Manager-Verschlüsselung

RSA DPM Key Manager muss sowohl auf dem RSA DPM-Server als auch auf dem Data Domain-System installiert werden.

Ausführen dieser Konfiguration auf dem RSA DPM-Server

Dieser Abschnitt enthält die wichtigsten Schritte zum Konfigurieren des RSA DPM-Servers (mithilfe der grafischen Benutzeroberfläche).

Hinweis

Weitere Informationen zu den einzelnen Schritten in diesem Verfahren finden Sie in der neuesten Version des *RSA Data Protection Manager Server Administrator's Guide*.

Die auf dem RSA DPM Key Manager Server festgelegten Algorithmus- und Cipher-Moduseinstellungen werden vom Data Domain-System ignoriert. Konfigurieren Sie diese Einstellungen auf dem Data Domain-System.

Vorgehensweise

1. Erstellen Sie eine Identität für das Data Domain-System mithilfe des X509-Zertifikats. Basierend auf diesem Zertifikat wird ein sicherer Kanal erstellt.
2. Erstellen Sie eine Schlüsselklasse mit den passenden Attributen:
   - Schlüssellänge: 256 Bit
   - Dauer: Beispielsweise sechs Monate oder eine andere Zeitangabe gemäß Ihrer Policy
   - Automatische Schlüsselgeneration: Wählen Sie aus, dass Schlüssel automatisch erstellt werden.

   Hinweis

   Mehrere Data Domain-Systeme können dieselbe Schlüsselklasse gemeinsam nutzen. Weitere Informationen zu Schlüsselklassen finden Sie im Abschnitt zu RSA DPM-Schlüsselklassen.
3. Erstellen Sie eine Identität, indem Sie das Hostzertifikat des Data Domain-Systems als Identitätszertifikat verwenden. Die Identität und die Schlüsselklasse müssen sich in derselben Identitätsgruppe befinden.
4. Importieren Sie die Zertifikate. Weitere Informationen finden Sie im Abschnitt zum Importieren von Zertifikaten.

Informationen über RSA DPM-Schlüsselklassen

Das Data Domain-System ruft einen Schlüssel von RSA DPM Key Manager nach Schlüsselklasse ab. Eine Schlüsselklasse ist eine spezielle Art von Sicherheitsklasse, die von RSA DPM Key Manager verwendet wird, der krytopgrafische Schlüssel mit ähnlichen Eigenschaften gruppiert.

Der RSA DPM Key Manager Server ermöglicht, dass eine Schlüsselklasse so eingerichtet wird, dass sie entweder den aktuellen Schlüssel zurückgibt oder jedes Mal einen neuen Schlüssel erzeugt. Das Data Domain-System unterstützt nur die Schlüsselklassen, die so konfiguriert sind, dass sie den aktuellen Schlüssel zurückgeben. Verwenden Sie keine Schlüsselklasse, die so konfiguriert ist, dass jedes Mal ein neuer Schlüssel erzeugt wird.

Hinweis

Wenn die Schlüssellänge nicht 256 Bit ist, schlägt die DPM-Konfiguration fehl.

Importieren der Zertifikate

Nach dem Erhalt der Zertifikate müssen Sie diese in das Data Domain-System importieren.

Bevor Sie beginnen

- Das Hostzertifikat sollte das PKCS12-Format aufweisen.
- Das CA-Zertifikat sollte das PEM-Format aufweisen.
- Sie müssen CA- und Hostzertifikate erwerben, die mit dem RSA DPM Key Manager kompatibel sind. Sie können diese Zertifikate von Zertifizierungsstellen von Drittanbietern anfordern oder mithilfe der entsprechenden SSL-Dienstprogramme erstellen.
- Wenn die System-Passphrase nicht festgelegt ist, können Sie das Hostzertifikat nicht importieren. Die Passphrase wird festgelegt, wenn Sie die Verschlüsselung aktivieren. Informationen dazu, wie Sie dies ändern, finden Sie im Abschnitt zum Ändern der System-Passphrase in dem Kapitel „Managen der Data Domain-Systeme“.

DD OS unterstützt Zertifikate ohne Erweiterung und Zertifikate mit Server- und Clienterweiterungen zur Verwendung mit Data DD Manager und RSA DPM Key Manager. Zertifikate mit Clienterweiterungen werden nur von RSA DPM Key Manager unterstützt und Zertifikate mit Servererweiterungen werden nur von DD System Manager unterstützt.

DD OS unterstützt nicht die automatische Registrierungszertifikatfunktion von RSA DPM Key Manager, die ein automatisch registriertes Zertifikat direkt hochlädt oder mehrere Zertifikate importiert. Das bedeutet, dass Sie die CA- und Hostzertifikate für ein Data Domain-System importieren müssen.

Im Folgenden werden die empfohlenen Reaktionen auf einige Warnmeldungen beschrieben, die möglicherweise beim Zertifikatmanagement angezeigt werden.

- Wenn HTTPS aufgrund fehlerhafter Zertifikate nicht neu gestartet werden kann, werden selbstsignierte Zertifikate verwendet. In einem solchen Fall wird eine verwaltete Warnmeldung, UnusableHostCertificate, ausgegeben. Um die Warnmeldung zu löschen, löschen Sie die beschädigten Zertifikate und importieren Sie neue Zertifikate erneut.
- Wenn importierte Zertifikate entfernt (z. B. während eines Hauptsystemaustauschs) und die importierten Zertifikate nicht kopiert werden, wird eine verwaltete Warnmeldung, MissingHostCertificate, ausgegeben. Importieren Sie die Zertifikate erneut, um die Warnmeldung zu löschen.

Nach dem Erhalt der Zertifikate importieren Sie diese wie folgt in das Data Domain-System:

Vorgehensweise

1. Konfigurieren Sie RSA DPM Key Manager Server so, dass er die CA- und Hostzertifikate verwendet. Anweisungen finden Sie im *RSA DPM Key Manager Server Administration Guide*.
2. Importieren Sie die Zertifikate, indem Sie die Zertifikatdateien mithilfe der Befehlssyntax `ssh` umleiten. Weitere Informationen finden Sie im *Data Domain Operating System Command Reference Guide*.

   ssh sysadmin@<*Data-Domain-system*> adminaccess certificate import {host password *password* |ca } < *path_to_the_certificate*
   Wenn Sie beispielsweise das Hostzertifikat host.p12 von Ihrem PC-Desktop in das Data Domain-System DD1 mithilfe von `ssh` importieren möchten, geben Sie Folgendes ein:

   # ssh sysadmin@DD1 adminaccess certificate import host password abc123 < C:\host.p12

3. Importieren Sie das CA-Zertifikat, z. B. ca.pem, von Ihrem Desktop in DD1 über SSH, indem Sie Folgendes eingeben:

   # `ssh sysadmin@DD1` **`adminaccess certificate import ca < C:\ca.pem`**

Ausführen dieser Konfiguration auf dem Data Domain-System

Konfigurieren Sie die Verschlüsselung mit dem DPM Key Manager über Data Domain System Manager.

Vorgehensweise

1. Schließen Sie die Einrichtung von DPM Key Manager auf dem RSA DPM Server ab.
2. Das Data Domain-System muss in der Lage sein, seine eigene IP-Adresse mithilfe des Hostnamens aufzulösen. Wenn diese Zuordnung dem DNS-Server nicht hinzugefügt wurde, verwenden Sie diese Befehlszeile, um den Eintrag in der Datei `/etc/hosts` hinzuzufügen:

   # `net hosts add`*ipaddrhost-list*
   wobei *ipaddr* die IP-Adresse des Data Domain-Systems und *host-list* der Hostname des Data Domain-Systems ist.

   In einer Dual-Stack-Umgebung wird möglicherweise folgende Fehlermeldung angezeigt: „RKM is not configured correctly.“ Verwenden Sie in diesem Fall den Befehl `net hosts add`*ipaddrhost-list*, um die IPv4-Adresse des Data Domain-Systems in die Datei „/etc/hosts“ einzufügen.

   Hinweis

   Ein DPM-Server kann in einer Umgebung ausschließlich mit IPv6-Adressen nicht aktiviert werden.

   Hinweis

   Standardmäßig ist der FIPS-Modus aktiviert. Wenn die PKCS #12-Client-Zugangsdatendatei nicht mit dem FIPS 140-2 genehmigten Algorithmus verschlüsselt ist, wie RC2, müssen Sie den FIPS-Modus deaktivieren. Weitere Informationen zur Deaktivierung des FIPS-Modus finden Sie im *Befehlsreferenzleitfaden für das EMC Data Domain Operating System*.

3. Melden Sie sich beim DD System Manager an und wählen Sie das Data Domain-System, mit dem Sie arbeiten, im Navigationsbereich auszuwählen.

   Hinweis

   Führen Sie stets DD System Manager-Aufgaben auf dem System aus, das Sie im Navigationsbereich ausgewählt haben.

4. Klicken Sie auf die Registerkarte **Data Management** > **File System** > **Encryption**.
5. Befolgen Sie die Anweisungen im Abschnitt zur Konfiguration der Verschlüsselung und wählen Sie den **DPM Key Manager** aus. Wenn die Verschlüsselung bereits eingerichtet wurde, befolgen Sie die Anweisungen im Abschnitt zur Änderung des Key Managers nach der Konfiguration.

Einrichten des KMIP Key Manager

Mit KMIP-Unterstützung kann eine Data Domain-Appliance symmetrische Schlüsselobjekte abrufen, die für Data-at-Rest-Verschlüsselung von KMIP Key Managern verwendet werden.

Vorgehensweise

1. Richten Sie eine KeySecure-Instanz mit der IP-Adresse <IP1> ein.
2. Erstellen und installieren Sie ein SSL-Serverzertifikat auf KeySecure.
3. Aktivieren Sie KMIP durch Navigation zu **Device** > **Key Server**.

   Stellen Sie sicher, dass <IP1> die verwendete Adresse und <Port1> der verwendete Port ist. Ferner sollte das Serverzertifikat aus Schritt 2 verwendet werden.
4. Erstellen Sie eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) für das System auf dem Data Domain-System/DD VE oder dem Linux-Computer.
   a. Melden Sie sich bei Data Domain an.
   b. Geben Sie den Befehl `adminaccess certificate cert-signing-request generate` aus.

   Wenn der Befehl erfolgreich ausgeführt wird, generiert er die Datei `CertificateSigningRequest.csr`, die sich unter `/ddvar/certificates/` befindet.

   Standardmäßig haben NFS-Exporte nicht die Berechtigungen, um auf den Zertifikatordner zuzugreifen, sogar auf einem Root-Benutzer.

```
# mount 16tbddve:/ddvar /mnt/DDVE
# cd /mnt/DDVE/certificates/
bash: cd: /mnt/DDVE/certificates/: Permission denied
# ls -al /mnt/DDVE/
total 800292
drwxr-xr-x 25 root staff      4096 Apr 10 08:32 .
drwxr-xr-x 26 root root       4096 Oct 24 12:11 ..
-rwxr-xr-x  1 root staff       180 Apr 10 08:36 .bashrc
drwxrwsr-x  2 root staff      4096 Aug 18  2016 benchmark
drwxr-sr-x  3 root staff      4096 Apr  4 15:49 cacerts
drwxrwsr-x  2 root staff      4096 Apr  4 12:50 cdes
drwxrws---  2 root staff      4096 Apr 11  2017 certificates
drwxrwsr-x  3 root staff      4096 Jul  1  2016 core
```

5. Diese CSR muss von der CA auf KeySecure ausgestellt/signiert werden.

   Wenn der Befehl erfolgreich ausgeführt wird, generiert er die Datei `CertificateSigningRequest.csr`, die sich unter `/ddvar/certificates/` befindet.
6. Laden Sie dieses signierte Zertifikat (x.509-pem-Datei) auf das Data Domain-System herunter und verwenden Sie den privaten Schlüssel der CSR, um eine pkcs#12-Datei zu erstellen.

   Benennen Sie `csr` in `pem` im Dateinamen um.
7. Laden Sie das CA-Stammzertifikat von der CA von KeySecure herunter (**Security** > **Local CAs**).
8. Verwenden Sie auf dem Data Domain-System/DD VE die `adminaccess`-CLI, um das pkcs#12-Clientzertifikat und das CA-Zertifikat zu installieren. Verwenden Sie **keysecure** als Anwendungstyp.

9. Erstellen Sie auf KeySecure einen symmetrischen Schlüssel mit AES-256 als Algorithmus und Schlüssellänge.
   a. Legen Sie als Eigentümer den Benutzer fest, der KMIP auf dem Data Domain-System/DD VE verwendet.
   b. Wählen Sie die Option `Exportable`.
   c. Legen Sie unter **Security** > **Keys** > **Attributes** für den Schlüssel **Application Namespace** auf **DD_DARE_KEYS** fest. Legen Sie für **Application Data** die Schlüsselklasse fest, die Sie auf dem Data Domain-System/DD VE verwenden möchten.
10. Verwenden Sie den Befehl `filesys encryption key-manager set`, um ALLE Parameter für den Zugriff auf den KeySecure Key Manager zu konfigurieren.
11. Aktivieren Sie den externen Key Manager durch Verwendung des Befehls `filesys encryption key-manager enable`.
12. Aktivieren Sie die Verschlüsselung durch die Befehle `filesys encryption enable` und `filesys restart`.

    Diese Aktion startet das Dateisystem neu.
13. Schlüssel sollten automatisch vom KeySecure Key Manager abgerufen werden und in der lokalen Schlüsseltabelle vorhanden sein.

    Beispielausgabe der lokalen Schlüsseltabelle für `filesys encryption keys show`:

```
Active Tier:

Key   Key                                                              State          Size
Id    MUID                                                                          post-comp

---   ---------------------------------------------------------------  ------------   ---------

0.1   e56                                                              Deactivated       0
0.2   953C694E2128F977FC8B18D7F8A51E44F8847A8D171D0BBDC8C01576FF5DE1D5  Activated-RW      0
---   ---------------------------------------------------------------  ------------  ---------

   * Post-comp size is based on last cleaning of Tue Feb 14 10:02:02 2017.
```

    Der aktuelle aktive Schlüssel dient zum Verschlüsseln von Daten, die aufgenommen werden.
14. Synchronisieren Sie die Schlüsselzustände.
    a. Erstellen Sie auf der KeySecure-Weboberfläche einen neuen aktiven Schlüssel (wie oben beschrieben).
    b. Deaktivieren Sie auf der KeySecure-Weboberfläche den alten Schlüssel durch Klicken auf den Schlüssel und Wechseln zur Registerkarte **Life Cycle**. Klicken Sie auf **Edit State**. Legen Sie **Cryptographic State** auf **Deactivated** fest. Klicken Sie auf **Save**.
15. Synchronisieren Sie auf dem Data Domain-System die lokale Schlüsseltabelle durch Ausführen des Befehls `filesys encryption keys sync`.

    Beispielausgabe der lokalen Schlüsseltabelle für `filesys encryption keys show`:

```
Active Tier:

Key   Key                                                              State          Size
Id    MUID                                                                          post-comp

---   ---------------------------------------------------------------  ------------   ---------

0.1   e56                                                              Deactivated       0
0.2   953C694E2128F977FC8B18D7F8A51E44F8847A8D171D0BBDC8C01576FF5DE1D5  Deactivated       0
0.3   851631E574D6F02886CAEF2795896D4C401EBC57A0997EFE04A146E584E9A99A  Activated-RW      0
---   ---------------------------------------------------------------  ------------  ---------

   * Post-comp size is based on last cleaning of Tue Feb 14 10:12:05 2017.
```

Hinweis

Schlüssel können als versionierte Schlüssel markiert werden. Wenn Version 2 und 3 eines speziellen Schlüssels generiert werden, verwenden KMIP-Abfragen diese Schlüssel aktuell nicht und können ein Problem darstellen, wenn dieser Schlüssel von einem Data Domain-System oder DD VE verwendet wird.

Ändern der Key Manager nach der Konfiguration

Wählen Sie den integrierten Key Manager oder den RSA DPM Key Manager aus.

Bevor Sie beginnen

Um Zertifikate für ein System verwalten zu können, müssen Sie DD System Manager auf diesem System starten.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Encryption**.
2. Klicken Sie unter „Key Management“ auf **Configure**.
3. Geben Sie den Benutzernamen und das Passwort für den Security Officer ein.
4. Wählen Sie aus, welcher Key Manager verwendet werden soll.
   - Integrierter Key Manager: Wählen Sie diesen aus, um die Schlüsselrotation zu aktivieren oder zu deaktivieren. Bei Aktivierung geben Sie ein Rotationsintervall zwischen 1 und 12 Monaten ein. Wählen Sie **Restart the file system now** aus und klicken Sie auf **OK**.
   - RSA DPM Key Manager: Geben Sie den Servernamen, die Schlüsselklasse, den Port (der Standardwert ist 443) ein und legen Sie fest, ob das importierte Hostzertifikat FIPS-vorgabenkonform ist. Der Standardmodus ist „Enabled“. Wählen Sie **Restart the file system now** aus und klicken Sie auf **OK**.
5. Klicken Sie auf **Manage Certificates**, um Zertifikate hinzuzufügen.

Managen von Zertifikaten für RSA Key Manager

Sie müssen Zertifikate des Hosts und der Zertifizierungsstelle mit RSA Key Manager verwenden.

Hinweis

Zertifikate sind nur für RSA Key Manager erforderlich. Der integrierte Key Manager verwendet keine Zertifikate.

Hinzufügen von Zertifizierungsstellenzertifikaten für RSA Key Manager

Sie können Zertifizierungsstellenzertifikate hochladen oder kopieren und einfügen.

Vorgehensweise

1. Wählen Sie eine der folgenden Optionen:
   - Wählen Sie die Option zum Hochladen eines Zertifikats einer Zertifizierungsstelle als .pem-Datei aus und klicken Sie auf **Browse**, um die Datei zu suchen.

- Wählen Sie die Option zum Kopieren und Einfügen des Zertifikats einer Zertifizierungsstelle aus und fügen Sie das Zertifikat einer Zertifizierungsstelle in das Feld ein.

2. Klicken Sie auf **Add**, um das Zertifikat hinzuzufügen.

Hinzufügen eines Hostzertifikats für RSA Key Manager

Laden Sie das Zertifikat als .p12-Datei oder einen öffentlichen Schlüssel als .pem-Datei hoch und verwenden Sie einen erzeugten privaten Schlüssel.

Wählen Sie für den Beginn den ersten oder zweiten der im Folgenden aufgeführten Schritte aus:

Vorgehensweise

1. Wählen Sie die Option zum Hochladen des Zertifikats als .p12-Datei aus.
   a. Geben Sie ein Passwort ein.
   b. Klicken Sie auf **Browse**, um nach der .p12-Datei zu suchen.
2. Wählen Sie die Option zum Hochladen des öffentlichen Schlüssels als .pem-Datei aus und verwenden Sie einen erzeugten privaten Schlüssel.
   a. Klicken Sie auf **Browse**, um nach der .pem-Datei zu suchen.
3. Klicken Sie auf **Add**.

Löschen von Zertifikaten

Wählen Sie ein Zertifikat mit dem korrekten Fingerabdruck aus.

Vorgehensweise

1. Wählen Sie das zu löschende Zertifikat aus.
2. Klicken Sie auf **Delete**.

   Es wird das Dialogfeld „Delete Certificate“ mit dem Fingerabdruck des zu löschenden Zertifikats angezeigt.
3. Klicken Sie auf **OK**.

Prüfen der Einstellungen für die Data-at-Rest-Verschlüsselung

Prüfen Sie die Einstellungen für die DD-Verschlüsselungsfunktion.

Klicken Sie auf die Registerkarten **Data Management** > **File System** > **Encryption**. Der derzeit verwendete Key Manager wird als „Enabled“ angezeigt. Eine Beschreibung der DD-Verschlüsselungseinstellungen finden Sie im Abschnitt zur Verschlüsselungsansicht.

Aktivieren und Deaktivieren der Data-at-Rest-Verschlüsselung

Nachdem DD Encryption konfiguriert wurde, ist der Status „Enabled“ und die Schaltfläche „Disabled“ ist aktiv. Wenn DD Encryption deaktiviert wird, ist die Schaltfläche „Enabled“ aktiv.

Aktivieren der Data-at-Rest-Verschlüsselung

Verwenden Sie den DD System Manager, um die Funktion DD Encryption zu aktivieren.

Vorgehensweise

1. Wählen Sie im DD System Manager das Data Domain-System aus, mit dem Sie im Navigationsbereich arbeiten.
2. Klicken Sie in der Ansicht „Encryption“ auf die Schaltfläche **Enable**.
3. Die folgenden beiden Optionen sind verfügbar:
   - Wählen Sie **Apply to existing data** und klicken Sie auf **OK**. Die Verschlüsselung der vorhandenen Daten tritt während des ersten Bereinigungszyklus auf, nachdem das Dateisystem neu gestartet wurde.
   - Wählen Sie **Restart the file system now** aus und klicken Sie auf **OK**. DD Encryption wird aktiviert, nachdem das Dateisystem neu gestartet wurde.

Weitere Erfordernisse

Hinweis

Es kann zu Anwendungsunterbrechungen kommen, während das Dateisystem neu gestartet wird.

Deaktivieren der Data-at-Rest-Verschlüsselung

Verwenden Sie den DD System Manager, um die Funktion DD Encryption zu deaktivieren.

Vorgehensweise

1. Wählen Sie im DD System Manager das Data Domain-System aus, mit dem Sie im Navigationsbereich arbeiten.
2. Klicken Sie in der Ansicht „Encryption“ auf die Schaltfläche **Disable**.

   Das Dialogfeld „Disable Encryption“ wird angezeigt.

3. Geben Sie im Bereich „Security Officer Credential“ den Benutzernamen und das Passwort eines Security Officer ein.
4. Wählen Sie eine der folgenden Optionen:
   - Wählen Sie **Apply to existing data** und klicken Sie auf **OK**. Die Entschlüsselung der vorhandenen Daten tritt während des ersten Bereinigungszyklus auf, nachdem das Dateisystem neu gestartet wurde.
   - Wählen Sie **Restart the file system now** aus und klicken Sie auf **OK**. DD Encryption wird deaktiviert, nachdem das Dateisystem neu gestartet wurde.

Weitere Erfordernisse

Hinweis

Es kann zu Anwendungsunterbrechungen kommen, während das Dateisystem neu gestartet wird.

Sperren und Entsperren des Dateisystems

Verwenden Sie dieses Verfahren, wenn ein für DD Encryption aktiviertes Data Domain-System (und seine externen Speichergeräte) transportiert werden soll oder Sie eine Festplatte sperren möchten, die ausgetauscht wird. Für das Verfahren sind zwei Konten erforderlich: Security Officer- und Systemadministratorrollen.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Encryption**.

   Im Bereich „File System Lock“ unter „Status“ wird angezeigt, ob das Dateisystem gesperrt oder entsperrt ist.

2. Deaktivieren Sie das Dateisystem, indem Sie im Bereich „File System status“ auf **Disabled** klicken.
3. Verwenden Sie dieses Verfahren, um das Dateisystem zu sperren oder zu entsperren.

Sperren des Dateisystems

Um das Dateisystem zu sperren, muss DD Encryption aktiviert und das Dateisystem deaktiviert sein.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Encryption** und klicken Sie auf **Lock File System**.
2. Geben Sie in den Textfeldern des Dialogfelds „Lock File System“ Folgendes ein:
   - Den Benutzernamen und das Passwort eines Security Officer-Kontos (eines autorisierten Benutzers in der Sicherheitsbenutzergruppe auf diesem Data Domain-System)
   - Die aktuelle und eine neue Passphrase
3. Klicken Sie auf **OK**.

   Durch dieses Verfahren werden die Chiffrierschlüssel mit der neuen Passphrase erneut verschlüsselt. Dabei wird die im Cache gespeicherte Kopie der aktuellen Passphrase gelöscht (sowohl im Arbeitsspeicher als auch auf der Festplatte).

   Hinweis

   Durch Ändern der Passphrase ist eine Authentifizierung durch zwei Benutzer erforderlich, um sich gegen die Möglichkeit zu schützen, dass bösartige Benutzer die Daten zerstören.

   ⚠ ACHTUNG

   Notieren Sie sich die Passphrase. Wenn Sie die Passphrase verlieren, können Sie das Dateisystem nicht entsperren und auf die Daten zugreifen. Die Daten gehen unwiderruflich verloren.

4. Fahren Sie das System herunter:

⚠ ACHTUNG

Verwenden Sie nicht den Gehäusenetzschalter, um das System auszuschalten. Geben Sie stattdessen an der Eingabeaufforderung den folgenden Befehl ein.

```
# system poweroff The 'system poweroff' command shuts down
the system and turns off the power. Continue? (yes|no|?)
[no]:
```

5. Transportieren Sie das System oder entfernen Sie die Festplatte, die ersetzt wird.
6. Schalten Sie das System wieder ein und entsperren Sie das Dateisystem mit diesem Verfahren.

Entsperren des Dateisystems

Dieses Verfahren bereitet ein verschlüsseltes Dateisystem für die Verwendung vor, nachdem es das Ziel erreicht hat.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Encryption** und klicken Sie auf **Unlock File System**.
2. Geben Sie in den Textfeldern die Passphrase ein, mit der das Dateisystem gesperrt wurde.
3. Klicken Sie auf **OK**.
4. Klicken Sie auf **Close**, um den Vorgang zu beenden.

   Wenn die Passphrase falsch ist, wird das Dateisystem nicht gestartet und das System meldet den Fehler. Geben Sie die richtige Passphrase ein, wie im vorherigen Schritt angeleitet.

Ändern des Verschlüsselungsalgorithmus

Sie können den Verschlüsselungsalgorithmus bei Bedarf zurücksetzen oder Optionen auswählen, um neue und vorhandene Daten oder nur neue Daten zu verschlüsseln.

Vorgehensweise

1. Wählen Sie **Data Management** > **File System** > **Encryption**
2. Um den Verschlüsselungsalgorithmus zu ändern, der für die Verschlüsselung des Data Domain-Systems verwendet wird, klicken Sie auf **Change Algorithm**.

   Das Dialogfeld „Change Algorithm“ wird angezeigt. Die folgenden Verschlüsselungsalgorithmen werden unterstützt:

   - AES-128 CBC
   - AES-256 CBC
   - AES-128 GCM
   - AES-256 GCM

3. Wählen Sie einen Verschlüsselungsalgorithmus aus der Drop-down-Liste aus oder akzeptieren Sie den Standard AES 256-Bit (CBC).

   AES 256-Bit Galois/Counter Mode (GCM) ist der sicherste Algorithmus, ist jedoch deutlich langsamer als der CBC-Modus (Cipher Block Chaining).

Hinweis

Um den Algorithmus auf die Standardeinstellung „AES 256-bit (CBC)“ zurückzusetzen, klicken Sie auf „Reset to default“.

4. Legen Sie fest, welche Daten verschlüsselt werden:
   - Um vorhandene und neue Daten auf dem System zu verschlüsseln, wählen Sie **Apply to Existing data, Restart file system now** aus und klicken Sie auf **OK**.
     Vorhandene Daten werden beim ersten Bereinigungszyklus verschlüsselt, nachdem das Dateisystem neu gestartet wurde.

     Hinweis

     Die Verschlüsselung vorhandener Daten kann länger dauern als ein standardmäßiger Bereinigungsvorgang des Dateisystems.

   - Um nur neue Daten zu verschlüsseln, wählen Sie **Restart file system now** aus und klicken Sie auf **OK**.
5. Der Status wird angezeigt. Klicken Sie auf **Close**, wenn der Prozess abgeschlossen ist.

   Hinweis

   Es kann zu Anwendungsunterbrechungen kommen, während das Dateisystem neu gestartet wird.