Dell PowerStore

Schützen von Daten

Version 3.x

Oktober 2023
Rev. A05

DELL Technologies

Anmerkungen, Vorsichtshinweise und Warnungen

ANMERKUNG: HINWEIS enthält wichtige Informationen, mit denen Sie Ihr Produkt besser nutzen können.

VORSICHT: ACHTUNG deutet auf mögliche Schäden an der Hardware oder auf den Verlust von Daten hin und zeigt, wie Sie das Problem vermeiden können.

WARNUNG: WARNUNG weist auf ein potenzielles Risiko für Sachschäden, Verletzungen oder den Tod hin.

Inhaltsverzeichnis

Weitere Ressourcen

Es werden regelmäßig neue Software- und Hardwareversionen veröffentlicht, um das Produkt kontinuierlich zu verbessern. Einige in diesem Dokument beschriebene Funktionen werden eventuell nicht von allen Versionen der von Ihnen derzeit verwendeten Software oder Hardware unterstützt. In den Versionshinweisen zum Produkt finden Sie aktuelle Informationen zu Produktfunktionen. Wenden Sie sich an Ihren Serviceanbieter, wenn ein Produkt nicht ordnungsgemäß oder nicht wie in diesem Dokument beschrieben funktioniert.

Hier erhalten Sie Hilfe

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

- **Produktinformationen**

  Dokumentationen oder Versionshinweise zum Produkt und zu Funktionen finden Sie auf der PowerStore-Seite unter https://www.dell.com/powerstoredocs.

- **Fehlerbehebung:**

  Informationen zu Produkten, Softwareupdates, Lizenzierung und Service finden Sie unter https://www.dell.com/support auf der entsprechenden Produktsupportseite.

- **Technischer Support**

  Für technischen Support und Serviceanfragen gehen Sie zu https://www.dell.com/support und rufen die Seite **Serviceanfragen** auf. Um einen Service-Request stellen zu können, müssen Sie über eine gültige Supportvereinbarung verfügen. Wenden Sie sich an Ihren Vertriebsmitarbeiter, wenn Sie einen gültigen Supportvertrag benötigen oder Fragen zu Ihrem Konto haben.

1

Einleitung

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Datensicherheit

PowerStore bietet verschiedene Möglichkeiten zum Schutz Ihrer Daten:

- Lokaler Schutz – Erstellung von Snapshots (point-in-time copies) von Volumes, Volume-Gruppen, Virtual Machines oder Dateisystemen auf dem PowerStore-System.
- Remoteschutz – Replikation von Daten auf ein Remotesystem oder Spiegelung der Daten mit Metro-Volumes für Redundanz im Notfall.
- Remotebackup – Sicherung von Volumes und Volume-Gruppen direkt von PowerStore auf einer PowerProtect DD.

PowerStore ermöglicht Ihnen die Erstellung nutzerdefinierter Schutz-Policies, bei denen es sich um Sätze von Regeln für die Snapshot-Erstellung, Replikation und Remotebackups handelt, und die Zuweisung von Storage-Ressourcen. Schutz-Policies wenden die festgelegten Regeln auf die Storage-Ressource an, indem sie lokalen Schutz, Remoteschutz und Remotebackups bereitstellen.

ANMERKUNG: Remotebackupregeln können nur auf Volumes und Volume-Gruppen angewendet werden.

ANMERKUNG: Datensicherheits-Policies, die eine Replikationsregel enthalten, können Metro-Volumes nicht zugewiesen werden. Siehe Verwenden von Datensicherheits-Policies mit Metro.

ANMERKUNG: Ab Version 3.x können Datensicherheits-Policies nicht auf Virtual Volumes (vVols) angewendet werden, die auf virtuellen Maschinen basieren. Siehe Replikation von Virtuellen Volumes.

PowerStore ermöglicht Ihnen die Konfiguration von Standardbackups für NAS-Server über die NDMP. Weitere Informationen finden Sie unter *PowerStoreKonfigurieren von SMB* und *PowerStore Konfigurieren von NFS* auf der PowerStore-Dokumentationsseite.

Snapshots

Snapshots sind schreibgeschützte, zeitpunktspezifische Kopien eines Volumes, einer Volume-Gruppe, einer virtuellen Maschine oder eines Dateisystems. Durch das Erstellen eines Snapshots wird der Status der Storage-Ressource zum jeweiligen Zeitpunkt gespeichert. Mithilfe von Snapshots können Sie Ihre Daten lokal schützen und eine Storage-Ressource auf einen vorherigen Status zurücksetzen.

Snapshots können jederzeit manuell erstellt werden. Es ist auch möglich, Snapshot-Regeln als Teil einer Datensicherheits-Policy zu konfigurieren und sie den entsprechenden Storage-Ressourcen zuzuweisen. Das System erstellt automatisch Snapshots der relevanten Ressource gemäß dem in der Datensicherheits-Policy festgelegten Zeitplan.

Ab PowerStore 3.5 können Sie sichere Snapshots erstellen, die von einem Administrator nicht manuell gelöscht werden können und automatisch gelöscht werden, wenn sie ablaufen. Sichere Snapshots bieten zusätzlichen Schutz vor Ransomware-Angriffen.

Wenn Daten beschädigt oder versehentlich gelöscht werden, können Sie die Daten aus den Snapshots, das Volume oder Volume-Gruppe auf den Zeitpunkt zurücksetzen, zu dem der Snapshot erstellt wurde.

Für Dateisysteme können Sie zwei Zugriffstypen von schreibgeschützten Datei-Snapshots erstellen: „Protokoll“ und „.snapshot“. Der standardmäßige Zugriffstyp ist „Protokoll“, der als SMB-Freigabe und/oder NFS-Export exportiert werden kann. Sie können die

Snapshots wie jedes andere Dateisystem auf einem Client freigeben und mounten. Für .snapshot-Zugriffstypen können Sie auf die Dateien im Snapshot über das Produktionsdateisystem im Unterordner `.snapshot` jedes Verzeichnisses zugreifen.

Sie können auch Snapshots mit konsistenter Schreibreihenfolge und anwendungskonsistente Snapshots von Volumes erstellen:

- Snapshots mit konsistenter Schreibreihenfolge: PowerStore enthält alle Schreibvorgänge auf den Volume-Gruppe-Mitgliedern, um eine einheitliche point-in-time copy bereitzustellen, und gewährleistet einen konsistenten Schutz auf allen Mitglieds-Volumes. Sie können Snapshots mit konsistenter Schreibreihenfolge über PowerStore Manager erstellen.
- Anwendungskonsistente Snapshots – Sie können anwendungskonsistente Snapshots eines Volumes oder einer Volume-Gruppe mit AppSync erstellen. Wenn Sie einen anwendungskonsistenten Snapshot erstellen, werden alle eingehenden I/O für eine bestimmte Anwendung stillgelegt, während der Snapshot erstellt wird.

Um zu überprüfen, ob es sich um einen Snapshot mit konsistenter Schreibreihenfolge oder um einen anwendungskonsistenten Snapshot handelt, sehen Sie sich die Spalten **Übereinstimmende Schreibreihenfolge** und **Übereinstimmende Anwendung** in den Snapshot-Tabellen für ein Volume oder Volume-Gruppe in PowerStore Manager an.

ANMERKUNG: Wenn diese Spalten nicht angezeigt werden, können Sie sie mithilfe der Option **Tabellenspalten anzeigen/ausblenden** hinzufügen.

Das Zuordnen von Snapshots zu Hosts wird in PowerStore nicht unterstützt. Um einem verbundenen Host den Zugriff auf einen Snapshot zu ermöglichen, können Sie einen Thin Clone, eine beschreibbare, speicherplatzsparende Kopie des Snapshots, erstellen und einem Host zuweisen. Sie können den Thin Clone mithilfe des Aktualisierungsvorgangs von verschiedenen Snapshots aktualisieren.

Weitere Informationen zu den möglichen Snapshot-bezogenen Vorgängen, die Sie mit PowerStore Manager durchführen können, finden Sie im Kapitel Snapshots.

Replikation

Bei der Datenreplikation handelt es sich um einen Prozess, bei dem Daten auf ein Remotesystem dupliziert werden. Dies sorgt für eine höhere Redundanz, falls das Hauptproduktionssystem ausfällt. Die Replikation minimiert die mit Ausfallzeiten verknüpften Kosten eines Systemausfalls und vereinfacht die Recovery nach einer Naturkatastrophe oder menschlichem Versagen.

PowerStore unterstützt die asynchrone Remotereplikation für Volumes und Volume-Gruppen, NAS-Server und Virtual Volumes.

So konfigurieren Sie die Replikation für Volumes und Volume-Gruppen:

1. Erstellen Sie eine Remoteverbindung zwischen den Quell- und Zielsystemen.
2. Konfigurieren Sie eine Datensicherheits-Policy mit einer Replikationsregel, die Ihre Geschäftsanforderungen am besten erfüllt.
3. Weisen Sie dem Volume oder Volume-Gruppen eine Datensicherheits-Policy zu.

So konfigurieren Sie die Replikation für NAS-Server:

1. Konfigurieren Sie das Dateimobilitätsnetzwerk und ordnen Sie es zu. Details finden Sie unter *PowerStore-Netzwerkleitfaden für PowerStore T-Modelle* auf https://www.dell.com/powerstoredocs.
2. Erstellen Sie eine Remoteverbindung zwischen den Quell- und Zielsystemen.
3. Konfigurieren Sie eine Datensicherheits-Policy mit einer Replikationsregel, die Ihre Geschäftsanforderungen am besten erfüllt.
4. Weisen Sie dem NAS-Server eine Datensicherheits-Policy zu.

   ANMERKUNG: Es wird nicht empfohlen, das Dateimobilitätsnetzwerk zu ändern, wenn das Peer-System nicht erreichbar ist. Wenn das Peer-System wieder verfügbar ist, kann es sein, dass sich beide NAS-Server im Produktionsmodus befinden.

So konfigurieren Sie die Replikation für Virtual Volumes (vVols):

1. Erstellen Sie eine Remoteverbindung zwischen den Quell- und Zielsystemen.
2. Datensicherheits-Policies werden auf vSphere erstellt und Virtuelle Volumes zugewiesen. Siehe Replikation von Virtuellen Volumes.

Zur Replikation von Volumes und Dateien können Sie mit PowerStore die Kontrolle per Failover an das Remotesystem übergeben und die Richtung einer Sitzung für Remoteschutz umkehren. Ein Failover kann in folgenden Fällen erforderlich sein:

- Wenn Sie Daten in ein neues System migrieren und dann von dort aus arbeiten möchten, ohne Daten zu verlieren. In diesem Fall kann ein Failover ohne Datenverluste durchgeführt werden.
- Wenn kein Zugriff auf die Daten im Quellsystem besteht, können Sie zum Remotesystem wechseln und mithilfe der neuesten Point-in-Time-Kopie für Remoteschutz weiterarbeiten. Dies kann jedoch zu einem Datenverlust führen, da die neueste Kopie im Remotesystem keine Datenänderungen enthält, die zwischen dem Zeitpunkt der Erstellung dieser Kopie und dem Zeitpunkt vorgenommen wurden, an dem die Daten im System nicht mehr zugänglich waren.
- Wenn die Daten im Quellsystem zugänglich sind, aber ihre Integrität möglicherweise beeinträchtigt wurde. In einem solchen Fall sollten Sie auf die neueste Point-in-Time-Kopie für Schutz zurücksetzen, die erstellt wurde, bevor die Daten beeinträchtigt wurden.

Sie können einen Failover-Test für die Disaster-Recovery-Bereitschaft des Systems durchführen, um die Disaster-Recovery-Bereitschaft des Systems zu testen.

Ausführliche Informationen zu den durchführbaren replikationsbezogenen Verfahren finden Sie im Kapitel Replikation.

Schutz-Policies

Eine Datensicherheits-Policy besteht aus Snapshot-Regeln, Replikationsregeln und Remotebackupregeln, die Sie erstellen können, um eine konsistente Data Protection für alle Storage-Ressourcen zu schaffen. Nach dem Konfigurieren einer Datensicherheits-Policy können Sie sie neuen oder vorhandenen Storage-Ressourcen zuweisen.

Eine Datensicherheits-Policy kann eine Replikationsregel, eine Remotebackupregel und bis zu vier Snapshot-Regeln enthalten. Alle Regeltypen können in mehreren Policies sein.

Schutz-Policies managen die Snapshot-Erstellung, Replikationssitzungen und Remotebackups basierend auf den darin enthaltenen Regeln. Sie können Policies mit verschiedenen Regeln erstellen, die unterschiedliche Schutzebenen zur Erfüllung ihrer Anforderungen an den lokalen und den Remoteschutz bieten, und einer Policy mehrere Storage-Ressourcen zuweisen, um denselben Schutz für diese Ressourcen zu bieten.

Sie können relevante Regeln und Policies basierend auf Ihren Nutzerberechtigungen erstellen oder ändern.

Wenn Sie eine Regel erstellen möchten, sollten Sie die Parameter und Ihre geschäftlichen Anforderungen vorab mit einem Administrator durchgehen. Dies kann dazu beitragen, konsistente Policies im gesamten System zu erreichen und aufrechtzuerhalten.

Ausführliche Informationen zu Datensicherheits-Policy-bezogenen Verfahren, die Sie durchführen können, finden Sie im Kapitel „Datensicherheits-Policies“.

Metro-Schutz

Metro ermöglicht die bidirektionale synchrone Replikation (Aktiv/Aktiv) über zwei PowerStore-Systeme. Ein Metro-Volume wird mithilfe von zwei unterschiedlichen Systemen bereitgestellt, die sich in der Regel in zwei verschiedenen Rechenzentren, bis zu 96 km (oder 60 Meilen) voneinander entfernt oder an zwei entfernten Standorten innerhalb desselben Rechenzentrums befinden. Die beiden Systeme arbeiten zusammen, um Anwendungshosts ein einziges Metro-Volume zur Verfügung zu stellen, indem sie dasselbe SCSI-Image und dieselben Daten bereitstellen. Die Hosts und die Anwendung nehmen die beiden physischen Volumes, die von den beiden Systemen gehostet werden, als ein einziges Volume mit mehreren Pfaden wahr.

Metro-Schutz bietet eine bessere Verfügbarkeit und Vermeidung von Notfällen, einen Ressourcenausgleich zwischen Rechenzentren und eine Storage-Migration zwischen zwei PowerStore-Systemen.

Wenn Sie ein Metro-Volume konfigurieren, wird der Inhalt eines Metro-Volumes auf das Remotesystem repliziert. Datensicherheits-Policies werden verwendet, um zusätzlichen Schutz zu konfigurieren, z. B. lokale Snapshots.

Eine Metro-Sitzung besteht aus zwei PowerStore-Systemen und optional einem Witness-Server.

Der Witness-Server ist ein passiver Drittanbieter, der auf einem eigenständigen Host installiert ist (vorzugsweise in einem anderen Rechenzentrum, sodass er nicht von Stromausfällen betroffen ist, die bei den PowerStore-Systemen auftreten). Der Witness beobachtet den Status der beiden Systeme. Wenn ein Fehler auftritt, bestimmt der Witness-Server, welches System für Hosts zugänglich bleibt, und bedient weiterhin I/O-Vorgänge. Ein Witness, der an einem dritten Standort installiert ist, bietet Schutz vor einzelnen Ausfallszenarien.

Eines der Systeme wird als „bevorzugt“ und das andere als „nicht bevorzugt“ konfiguriert. Wenn kein Witness konfiguriert oder der Witness nicht verfügbar ist, kann das Systemverhalten in Fehlersituationen anhand dieser Rollen gesteuert werden. Wenn ein Fehler auftritt (entweder auf einem der Systeme oder in der Verbindung zwischen den Systemen), wird die Metro-Sitzung „aufgeteilt“ und das nicht bevorzugte System verarbeitet keine I/O mehr.

Metro wechselt zwischen der Verwendung des Witness und der Systemrolle als Mittel zur Wiederherstellung nach einem einzigen Ausfall (wenn der Witness nicht konfiguriert oder nicht verfügbar ist, erfolgt die Recovery nach einem einzigen Ausfall manuell).

In der folgenden Tabelle sind die zulässigen Aktionen zusammengefasst, die Sie abhängig vom aktuellen Metro-Status und dem System, von dem die Aktion initiiert wird, auf einem Metro-Volume durchführen können.

ANMERKUNG: Die Tabelle enthält häufige Anwendungsbeispiele und keine seltenen Fehlerszenarien.

Tabelle 1. Zulässige Metro-Aktionen

Position	Metro-Status	Rolle ändern	Übernehmen	Herunterstufen	Pause	Wiederaufnehmen	Metro beenden
Im bevorzugtem System	Läuft normal	Ja	Nein	Nein	Ja	Nein	Ja
	Angehalten	Nein	Nein	Ja	Nein	Ja	Ja

Tabelle 1. Zulässige Metro-Aktionen (fortgesetzt)

Position	Metro-Status	Rolle ändern	Übernehmen	Herunterstufen	Pause	Wiederaufnehmen	Metro beenden
	Unterteilt	Nein	Nein	Ja	Ja	Nein	Ja
	Wechsel zu Metro-Synchronisation	Nein	Nein	Nein	Ja	Nein	Ja
Auf einem nicht bevorzugten System	Läuft normal	Ja	Nein	Nein	Ja	Nein	Ja
	Angehalten	Nein	Ja (wenn das andere System nicht erreichbar ist)	Nein	Nein	Ja	Ja
	Unterteilt	Nein	Ja (wenn das andere System nicht erreichbar ist)	Nein	Ja	Nein	Ja
	Wechsel zu Metro-Synchronisation	Nein	Nein	Nein	Ja	Nein	Ja

Remotebackup

Mit Remotebackup können Sie Volumes und Volume-Gruppen direkt von PowerStore auf einer PowerProtect DD sichern.

PowerStore unterstützt Backups auf einer physischen PowerProtect Appliance oder auf einer PowerProtect DD Virtual Edition (DDVE).

Ein Remotebackup erstellt einen Snapshot eines Volumes oder einer Volume-Gruppe auf dem PowerProtect-System. Die erstellten Snapshots sind absturzkonsistent und es gibt keine Anwendungsintegration.

Sobald sie sich auf der PowerProtect DD befinden, können Backups auf einem vorhandenen oder neuen PowerStore-Cluster abgerufen werden. Sie können auch den Inhalt eines Backups auf der DD mit dem sofortigen Zugriff durchsuchen und schnellen temporären Zugriff auf die gesicherten Snapshots erhalten, ohne sie auf dem PowerStore-Cluster abzurufen.

Wenn eine Ressource zum ersten Mal gesichert wird, wird eine vollständige Kopie erstellt. Die nachfolgenden Backups sind inkrementell – nur die Änderungen aus dem letzten Backup werden kopiert, um die Effizienz zu verbessern.

Wenn Sie einem Volume oder einer Volume-Gruppe eine Schutz-Policy zuweisen, die eine Remotebackupregel enthält, wird eine Remotebackupsitzung erstellt. Pro Ressource kann nur eine Remotebackupsitzung erstellt werden. Remotebackupsitzungen werden auf der Registerkarte **Backupsitzungen** der Seite **Remotebackup** angezeigt.

Das Remotebackup wird über PowerStoreinitiiert. Der Remotebackupworkflow wird unter Grundlegender Remotebackup-Workflow beschrieben.

Eine Remotesitzung verfolgt jeden der Vorgänge (Backup, Abruf und Instant Access). Sie können den Sitzungsfortschritt überwachen und Aktionen über die Seiten der Remotesitzungen durchführen.

2

Remotesysteme

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Übersicht

Der Metro-Schutz erfordert eine Remotesystemverbindung zwischen zwei PowerStore-Systemen. In PowerStore ist die Remotesystemverbindung mit der Replikationsregel verknüpft. Sie können eine Remotesystemverbindung erstellen, bevor Sie die Remotereplikation konfigurieren. Wenn Sie PowerStore Manager verwenden, können Sie während der Erstellung einer Replikationsregel eine Remotesystemverbindung erstellen. Es ist auch möglich, ein Remotesystem zu erstellen, wenn Metro auf einem Volume konfiguriert wird.

Es ist möglich, eine Remoteverbindung zwischen Systemen zu erstellen, auf denen verschiedene Versionen (1.x, 2.x) ausgeführt werden. Die Systemversionen bestimmen die unterstützten Funktionen. Beide Systeme müssen die erforderliche PowerStore-Version ausführen, damit eine Funktion in dieser Version unterstützt werden kann. Die folgenden Bedingungen sollten für die Replikation von Storage-Objekten erfüllt sein:

- Volume-Replikation
  - Auf den gekoppelten Systemen muss Version 1.x oder höher ausgeführt werden.
- Dateireplikation
  - Auf den gekoppelten Systemen muss Version 3.x oder höher ausgeführt werden.
  - Verbindungstyp: TCP
- Replikation von Virtuellen Volumes
  - Auf den gekoppelten Systemen muss Version 3.x oder höher ausgeführt werden.
  - Verbindungstyp: TCP
- Metro
  - Auf den gekoppelten Systemen muss Version 3.x oder höher ausgeführt werden.
  - Verbindungstyp: TCP (siehe Metro Voraussetzungen und Einschränkungen)
  - Netzwerklatenz – Niedrig (unter 5 Millisekunden)

Wenn Sie Jumbo-Frames verwenden, stellen Sie sicher, dass diese auf beiden Seiten der Remotesystemverbindung (PowerStore-Ports und -Switch-Ports) sowie auf allen Ports zwischen den beiden Storage-Arrays konfiguriert sind. Eine Nichtübereinstimmung der MTU-Größe führt in den folgenden Fällen zu einer Warnmeldung:

- Konfigurieren einer Verbindung zum Remotesystem
- Ändern der Einstellungen für die Remotesystemverbindung
- Verwenden der Option **Überprüfen und Aktualisieren**

ANMERKUNG: Es wird nicht empfohlen, die MTU-Größe eines Storage-Netzwerks zu ändern, wenn eine Replikationssitzung aktiv ist.

ANMERKUNG: Wenn die MTU-Größe nach der Erstellung des Remotesystems geändert wurde, müssen die Netzwerkports des Switches, der mit den für die Replikation markierten PowerStore-Ports verbunden ist, deaktiviert und wieder aktiviert werden (Bouncing), um die Änderung auf dem Remotesystem anzuwenden.

So ändern Sie die MTU-Größe:

1. Halten Sie die Replikationssitzung an.
2. Ändern Sie die MTU-Größe des Storage-Netzwerks (**Settings** > **Networking** > **Cluster MTU**).
3. Führen Sie **Überprüfen und aktualisieren** auf dem Remotesystem aus, um zu überprüfen, ob keine Warnung ausgegeben wurde.
4. Nehmen Sie die Replikationssitzung wieder auf.

Das Remotebackup erfordert eine Remotesystemverbindung zwischen einem PowerStore-System und einem PowerProtect DD-System. Die Remoteverbindung ist einer Remotebackupregel zugeordnet und das PowerProtect DD-System kann während der Erstellung der Regel konfiguriert werden.

Für Remotebackups müssen die folgenden Bedingungen erfüllt sein:

- Auf dem PowerStore-System muss Version 3.x oder höher ausgeführt werden.
- Es muss die PowerProtect DDOS Version 6.2.1 oder höher verwendet werden.
- Das PowerStore Storage-Netzwerk muss in der Lage sein, mit dem PowerProtect DD-Datenübertragungsnetzwerk zu kommunizieren.

Die Tabelle „Remotesysteme“ (unter **Schutz**) zeigt die konfigurierten Verbindungen des Remotesystems an. In der Remotesystemtabelle können Sie die folgenden Aktionen ausführen:

- Remotesysteminformationen anzeigen, z. B. den Namen und die IP-Adresse des Remotesystems, den Systemtyp (Storage-System oder PowerProtect DD), unterstützte Funktionen (nur sichtbar, wenn von beiden Systemen unterstützt) und den Status der Datenverbindung. Die detaillierte Ansicht bietet den IP-Konnektivitätsstatus für alle Initiatoren.
- Wählen Sie ein Remotesystem aus und klicken Sie auf **Modify**, um dessen Attribute zu bearbeiten. Sie können die Management-IP-Adresse, die Beschreibung und die Netzwerklatenz einer Remotesystemverbindung ändern.
- Wählen Sie ein Remotesystem aus, und klicken Sie auf **Löschen** , um es zu entfernen. Sie können ein Remotesystem in den folgenden Fällen nicht löschen:
  - Wenn aktive Replikationssitzungen vorhanden sind, die dem Remotesystem zugeordnet sind.
  - Wenn aktive Remotebackupsitzungen vorhanden sind, die dem Remotesystem zugeordnet sind.
  - Wenn eine Replikationsregel vorhanden ist, die dem Remotesystem zugeordnet ist.
  - Wenn eine Remotebackupregel vorhanden ist, die dem Remotesystem zugeordnet ist.
  - Wenn Metro-Volumes vorhanden sind.
- Überwachen Sie den Status der Management- und Datenverbindung zu Troubleshooting-Zwecken.
- Wählen Sie ein Remotesystem aus, und klicken Sie auf **Weitere Aktionen** > **Verifizieren und aktualisieren**, um die Verbindung zum Remotesystem zu überprüfen und zu aktualisieren. Dabei können Änderungen in den lokalen und Remotesystemen erkannt und Datenverbindungen wiederhergestellt werden, wobei auch die CHAP-Einstellungen (Challenge Handshake Authentication Protocol) berücksichtigt werden.
- Für PowerProtect DD-Remotesysteme:
  - Bei einem Verbindungsverlust von weniger als zehn Minuten wird das Remotesystem automatisch wiederhergestellt, wenn die Netzwerkverbindung wiederhergestellt ist. Wenn der Verbindungsverlust länger als zehn Minuten dauert, klicken Sie auf **More Actions** > **Verify and Update**, nachdem die Verbindung wiederhergestellt wurde, um den Status des Remotesystems in „OK“ zu ändern.
  - Wählen Sie ein Remotesystem aus und klicken Sie auf **More Actions** > **Kapazitätsdetails anzeigen**, um die Nutzungs- und historischen Kennzahlen für dieses System über einen ausgewählten Zeitraum anzuzeigen.
  - Sie können in den Spalten „Management/File System“ und „Data Connection“ der Tabelle **Remotesysteme** nach Konnektivitätsproblemen suchen.

Hinzufügen einer Remotesystemverbindung für die Replikation und Metro

Konfigurieren Sie eine Remotesystemverbindung zwischen den PowerStore-Quell- und -Zielsystemen, um die asynchrone Replikation und den Metro-Schutz zu aktivieren.

Voraussetzungen

Stellen Sie vor dem Herstellen einer Verbindung zum Remotesystem sicher, dass Sie die folgenden Details zum Remotesystem abgerufen haben:

- System-IP-Adresse
- Benutzerauthentifizierungsinformationen zum Herstellen einer Verbindung zum System

Schritte

1. Wählen Sie **Protection** > **Remotesysteme** aus.
2. Klicken Sie im Fenster **Remotesysteme** auf **Add**.
3. Konfigurieren Sie im Slide-Out-Fenster **Remotesystem hinzufügen** die folgenden Felder:
   - Remote-Systemtyp: Wählen Sie **PowerStore** aus.
   - Management-IP-Adresse

- Beschreibung (optional)
- Netzwerklatenz
- Benutzername und Passwort

4. Klicken Sie auf **Hinzufügen**.
5. Überprüfen Sie im Bereich **User Authorization** das Remote-Systemzertifikat und klicken Sie auf **Confirm**.

Hinzufügen einer Remotesystemverbindung für Remotebackups

Konfigurieren Sie eine Remotesystemverbindung zwischen einem PowerStore-System und einem PowerProtect DD-System, um Remotebackups zu aktivieren.

Voraussetzungen

Stellen Sie vor dem Hinzufügen der Remoteverbindung sicher, dass Sie die folgenden Details zum PowerProtect DD-System abgerufen haben:

- IP-Adresse der PowerProtect DD Appliance
- Name der Storage-Einheit
- Datenübertragungsparameter

ANMERKUNG: Das Erstellen eines Remotesystems mit ungültigen Nutzerzugangsdaten für die Storage-Einheit führt zu einem Verlust der Datenverbindung. In diesem Fall zeigt die Spalte „Status“ in **Protection** > **Remotesystem** > **[PowerProtect DD]** > **Connectivity** „Authentication Failure“ an. Wählen Sie **Modify** für die PowerProtect DD aus und korrigieren Sie die ungültigen Zugangsdaten. Weitere Informationen finden Sie im Dell Wissensdatenbank-Artikel 000208506.

Info über diese Aufgabe

ANMERKUNG: Sie können eine einzelne PowerProtect DD Appliance mehrmals zum selben PowerStore-Cluster hinzufügen, wobei Sie jedes Mal eine andere Storage-Einheit-ID verwenden. Auf diese Weise können Sie verschiedene Ressourcen an verschiedenen Standorten in einem einzigen PowerProtect DD-System sichern.

ANMERKUNG: Wenn die Storage-Einheit aus dem DD-System entfernt wird, tritt ein vollständiger Datenverbindungsverlust auf und Remotesitzungen und Snapshots müssen bereinigt werden. Weitere Informationen finden Sie im Dell Wissensdatenbank-Artikel 000208497.

Schritte

1. Wählen Sie **Protection** > **Remotesysteme** aus.
2. Klicken Sie im Fenster **Remotesysteme** auf **Add**.
3. Konfigurieren Sie im Slide-Out-Fenster **Remotesystem hinzufügen** die folgenden Felder:
   - Remote-Systemtyp: Wählen Sie **PowerProtect DD** aus.
   - Management-IP-Adresse
   - Beschreibung (optional)
   - Management-Nutzername und -Kennwort
   - Name der Storage-Einheit
   - Datenübertragungs-IP-Adresse, Nutzername und Kennwort
4. Legen Sie die Option „Enable encryption“ fest.
   - Wenn die Verschlüsselung deaktiviert ist, verwendet die Verbindung mit PowerStore nicht TLS und die Authentifizierung.
   - Wenn die Verschlüsselung aktiviert ist, verwendet die PowerStore-Verbindung den Authentifizierungsmodus „DD Boost Two Way Password“ und verhandelt die Verschlüsselungsstufe, die auf den globalen DD Boost-Sicherheitseinstellungen basiert.

   ANMERKUNG: Es wird empfohlen, die Verschlüsselung zu aktivieren, wenn das Remote-System DDVE in der Cloud ist.
5. Klicken Sie auf **Add**.
6. Überprüfen Sie im Bereich **User Authorization** das Remote-Systemzertifikat und klicken Sie auf **Confirm**, um die Remoteverbindung zu erstellen.

Ergebnisse

Das neue System wird der Liste **Remotesysteme** hinzugefügt. Der Typ des Systems ist PowerProtect DD und die Funktion ist „Remotebackup“.

3

Snapshots

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Erstellen eines Snapshot

Beim Erstellen eines Snapshots werden der Status der Storage-Ressource und aller darin enthaltenen Dateien und Daten zum jeweiligen Zeitpunkt gespeichert. Sie können Snapshots verwenden, um die gesamte Storage-Ressource auf einen vorherigen Status zurückzusetzen. Sie können einen Snapshot von einem Volume, einer Volume-Gruppe, einem Dateisystem oder einer virtuellen Maschine erstellen.

Berücksichtigen Sie vor dem Erstellen eines Snapshots Folgendes:

- Snapshots sind keine vollständigen Kopien der Originaldaten. Es wird empfohlen, Snapshots nicht für Spiegelungen, Disaster Recovery oder Hochverfügbarkeitstools zu verwenden. Da Snapshots teilweise von Echtzeitdaten der Storage-Ressourcen abgeleitet werden, kann es sein, dass nicht mehr auf sie zugegriffen werden kann, wenn auf die Storage-Ressource nicht mehr zugegriffen werden kann.
- Obwohl Snapshots speicherplatzsparend sind, verbrauchen Sie die gesamte Storage-Kapazität des Systems. Stellen Sie sicher, dass das System genug Kapazität für Snapshots hat.
- Überprüfen Sie beim Konfigurieren die Aufbewahrungs-Policy von Snapshots, die der Storage-Ressource zugeordnet sind. Sie können je nach Zweck des Snapshots die Aufbewahrungs-Policy in den zugehörigen Regeln ändern oder manuell eine andere Aufbewahrungs-Policy festlegen.
- Manuelle mit PowerStore Manager erstellte Snapshots werden eine Woche nach der Erstellung aufbewahrt (falls nicht anders konfiguriert).
- Wenn die maximale Anzahl von Snapshots erreicht ist, können keine weiteren erstellt werden. Um die Erstellung neuer Snapshots zu ermöglichen, müssen Sie in diesem Fall vorhandene Snapshots löschen.
- Für die Konfiguration sicherer Snapshots (insbesondere wenn sie als Teil einer lokalen Schutz-Policy konfiguriert werden) wird empfohlen, die geschäftlichen Anforderungen mit einem Administrator zu überprüfen, bevor Sie fortfahren. Sichere Snapshots können nicht vor Ende der Aufbewahrungsfrist gelöscht werden. Daher muss vorausschauend geplant werden, um zu vermeiden, dass das maximale Snapshot-Limit erreicht wird. Weitere Informationen zu sicheren Snapshots finden Sie unter Sichere Snapshots.

Wenn Sie die für ein Speicherobjekt erstellten Snapshots nicht anzeigen können, fügen Sie der Tabelle die Spalte „Snapshots“ mithilfe von **Tabellenspalten anzeigen/ausblenden** hinzu. Die Spalte „Snapshots“ zeigt die Anzahl der Snapshots an, die für jedes Objekt erstellt wurden. Durch Klicken auf die Zahl wird das Fenster **Snapshots** geöffnet, das detaillierte Informationen zu jedem Snapshot enthält.

Erstellen eines Snapshot von einem Volume

Info über diese Aufgabe

Wenn Sie einen einzelnen Snapshot eines Volumes erstellen möchten (nicht als Teil einer zugewiesenen Datensicherheits-Policy), verwenden Sie die Option **Snapshot erstellen**.

ANMERKUNG: Sie können das gleiche Verfahren anwenden, um einen Snapshot einer Volume-Gruppe zu erstellen.

Schritte

1. Zum Öffnen des Fensters **Volumes** wählen Sie **Storage** > **Volumes** aus.

2. Aktivieren Sie das Kontrollkästchen neben dem entsprechenden Volume, um es auszuwählen, und wählen Sie dann **Protect** > **Create Snapshot** aus.
3. Geben Sie im Slide-Out-Fenster „**Snapshot erstellen of Volume**“ einen eindeutigen Namen für den Snapshot ein, und legen Sie die **Local Retention Policy** fest.

   ANMERKUNG: Der Aufbewahrungszeitraum ist standardmäßig auf 1 Woche eingestellt. Sie können einen anderen Aufbewahrungszeitraum festlegen oder die Option **Keine automatische Löschung** für eine unbegrenzte Aufbewahrung auswählen.

4. Wenn Sie einen sicheren Snapshot erstellen möchten, legen Sie eine Aufbewahrungsfrist fest und wählen Sie die Option **Sicherer Snapshot** aus.
5. Klicken Sie auf **Snapshot erstellen**.

Erstellen eines Snapshots eines Dateisystems

Info über diese Aufgabe

Wenn Sie einen einzelnen Snapshot eines Dateisystems erstellen möchten (und nicht als Teil einer zugewiesenen Datensicherheits-Policy), verwenden Sie die Option **Snapshot erstellen** .

Schritte

1. Um das Fenster **Dateisysteme** zu öffnen, wählen Sie **Storage** > **Dateisysteme** aus.
2. Aktivieren Sie das Kontrollkästchen neben dem entsprechenden Dateisystem, um es auszuwählen, und wählen Sie dann **Schützen** > **Snapshot erstellen**.
3. Geben Sie im Slide-Out-Fenster „**Snapshot eines Dateisystems erstellen** einen eindeutigen Namen für den Snapshot ein, und legen Sie die **Lokale Aufbewahrungs-Policy** fest.

   ANMERKUNG: Der Aufbewahrungszeitraum ist standardmäßig auf 1 Woche eingestellt. Sie können einen anderen Aufbewahrungszeitraum festlegen oder die Option **Keine automatische Löschung** für eine unbegrenzte Aufbewahrung auswählen.

4. Wählen Sie den Datei-Snapshot-Zugriffstyp aus.
5. Wenn die Ereignisveröffentlichung auf dem NAS-Server konfiguriert wurde, haben Sie die Möglichkeit, die Ereignisveröffentlichung zu aktivieren.
6. Klicken Sie auf **Snapshot erstellen**.

Erstellen eines Snapshots einer virtuellen Maschine

Info über diese Aufgabe

Wenn Sie einen einzelnen Snapshot einer virtuellen Maschine erstellen möchten (und nicht als Teil einer zugewiesenen Datensicherheits-Policy), verwenden Sie die Option **Snapshot erstellen** .

Schritte

1. Um das Fenster **Virtuelle Maschinen** zu öffnen, wählen Sie **Compute** > **Virtuelle Maschinen** aus.
2. Aktivieren Sie das Kontrollkästchen neben der entsprechenden virtuellen Maschine, um es auszuwählen, und wählen Sie dann **Schützen** > **Snapshot erstellen** aus.
3. Geben Sie im Slide-Out-Fenster **Snapshot einer virtuellen Maschine erstellen** einen eindeutigen Namen für den Snapshot ein.
4. Auf Wunsch können Sie eine Kurzbeschreibung eingeben.
5. Klicken Sie auf **Snapshot erstellen**.

Thin Clone erstellen

Thin Clones sind beschreibbare Kopien eines Snapshots, eines Volumes, einer Volume-Gruppe oder eines Dateisystems, auf die Hosts zugreifen können. Im Gegensatz zu einem vollständigen Klon ist ein Thin Clone eine speicherplatzsparende Kopie, die Datenblöcke mit dem

übergeordneten Objekt gemeinsam nutzt, und kein komplettes Backup der ursprünglichen Ressource. Ein Thin Clone kann als Kopie des übergeordneten Objekts direkt oder mithilfe eines Snapshot erstellt werden.

Thin Clones behalten vollständigen Lesezugriff auf die ursprüngliche Ressource. Sie können die Daten innerhalb des Thin Clone ändern, wobei der ursprüngliche Snapshot beibehalten wird.

Mithilfe von Thin Clones können Sie hierarchische Zeitpunkte erstellen, um Daten über verschiedene Phasen von Datenänderungen beizubehalten. Wenn die übergeordnete Ressource gelöscht, migriert oder repliziert wird, bleibt der Thin Clone hiervon unberührt.

Erstellen eines Thin Clone eines Volume oder Volume-Gruppe

Info über diese Aufgabe

Sie können die folgenden Aktionen auf Thin Clones von Volumes und Volume-Gruppen durchführen:

- Zuordnen von Thin Clones zu unterschiedlichen Hosts
- Aktualisieren des Thin Clones.
- Wiederherstellen von Thin Clones aus einem Backup
- Anwenden von Schutz-Policies auf Thin Clones

Schritte

1. Wählen Sie **Storage** > **Volumes** oder **Storage** > **Volume Groups** aus, um das entsprechende Ressourcen-Fenster zu öffnen.
2. Klicken Sie auf das Kontrollkästchen neben dem entsprechenden Volume oder Volume-Gruppe und wählen Sie dann **Neue Verwendung** > **Thin Clone erstellen** aus.
3. Führen Sie im Slide-Out-Fenster **Erstellen Thin Clone** die folgenden Schritte aus:
   - Geben Sie den Thin Clone-Namen ein.
   - Geben Sie eine Beschreibung ein (optional).
   - Legen Sie die Performance-Policy fest (nur für Thin Clones, die aus Volumes erstellt wurden).
   - Legen Sie die Hostkonnektivität fest (nur für Thin Clones, die aus Volumes erstellt werden).
   - Legen Sie die Datensicherheits-Policy fest.
4. Klicken Sie auf **Clone**.

Erstellen eines Thin Clone eines Dateisystems

Info über diese Aufgabe

Sie können die folgenden Aktionen auf Thin Clones von Volumes und Volume-Gruppen durchführen:

- Zuordnen von Thin Clones zu unterschiedlichen Hosts
- Wiederherstellen von Thin Clones aus einem Backup
- Anwenden von Schutz-Policies auf Thin Clones

Schritte

1. Wählen Sie **Storage** > **Dateisysteme** aus, um das Fenster **Dateisysteme** zu öffnen.
2. Aktivieren Sie das Kontrollkästchen neben dem entsprechenden Dateisystem und wählen Sie dann **Schützen** > **Dateisystem klonen** aus.
3. Legen Sie im Slide-Out-Fenster **Thin Clone erstellen** den Namen des Thin Clone und optional eine Beschreibung fest.
4. Wenn die Ereignisveröffentlichung auf dem NAS-Server konfiguriert wurde, haben Sie die Möglichkeit, die Ereignisveröffentlichung zu aktivieren.
5. Klicken Sie auf **Clone**.

Erstellen eines Thin Clone eines Snapshots

Info über diese Aufgabe

Sie können einen Thin Clone eines Snapshots erstellen, der für ein Volume, eine Volume-Gruppe oder ein Dateisystem erstellt wurde.

Schritte

1. Öffnen Sie das entsprechende Storage-Ressource-Fenster.
2. Klicken Sie auf eine Ressource, um das Fenster „Overview“ zu öffnen.
3. Klicken Sie auf die Registerkarte **Protection**.
4. Klicken Sie auf **Snapshots**, um die Liste der Snapshots anzuzeigen, die für die Ressource erstellt wurden.
5. Wählen Sie einen Snapshot aus der Tabelle und dann **More actions** > **Create Thin Clone using Snapshot** aus.

Verwenden von Clones für den Zugriff auf schreibgeschützte Snapshots über Hosts

Das Zuordnen und Aufheben einer Zuordnung von Block-Snapshots zu Hosts wird in PowerStore nicht unterstützt. Um einem verbundenen Host den Zugriff auf einen Snapshot zu ermöglichen, erstellen Sie einen Thin Clone des Snapshots und weisen ihn einem Host zu. Nachdem der Thin Clone erstellt wurde, können Sie mit dem Aktualisierungsvorgang verschiedene Snapshots auf ihn anwenden. Weitere Informationen finden Sie unter Aktualisieren einer Storage-Ressource.

Datei-Snapshots können entweder direkt auf Hosts gemountet werden (um schreibgeschützten Zugriff zu ermöglichen) oder indem ein Thin Clone erstellt wird (um Lese-/Schreibzugriff zu ermöglichen). Um das Dateisystem direkt zu mounten, können die Snapshots als NFS-Export oder SMB-Freigabe exportiert werden.

Snapshots lassen sich mit einem der folgenden Zugriffstypen exportieren:

- Protokoll – Der Snapshot wird mit einem neuen Freigabenamen exportiert.
- .snapshot – Sie können den Snapshot auf UNIX/Linux unter dem. Snapshot-Verzeichnis des Dateisystems und in Windows anzeigen, indem Sie mit der rechten Maustaste auf das Dateisystem klicken und die Option **Previous Version** auswählen.

Wiederherstellen einer Speicherressource

Der Aktualisierungsvorgang wird verwendet, um den Inhalt einer Storage-Ressource durch Inhalte aus einer zugehörigen Ressource (einem Clone oder einem indirekten untergeordneten Snapshot) zu ersetzen. Sie können ein Duplikat der Produktionsumgebung erstellen, das für verschiedene Zwecke verwendet werden soll (z. B. Test und Entwicklung, Reporting usw.). Um die duplizierte Umgebung auf dem neuesten Stand zu halten, sollten sie mit einer Storage-Ressource aktualisiert werden, die die aktuellen Änderungen enthält.

Sie können den Aktualisierungsvorgang in den folgenden Szenarien verwenden:

- Aktualisieren Sie einen Thin Clone über das Basis-Volume.
- Aktualisieren Sie eine Storage-Ressource oder einen Thin Clone über einen anderen Thin Clone in der Produktreihe.
- Aktualisieren Sie eine Storage-Ressource oder einen Thin Clone über den Snapshots eines zugehörigen Thin Clones oder Basis-Volumes.

Bei Dateisystemen können Sie einen Snapshot eines Dateisystems mit seinem direkten übergeordneten Dateisystem aktualisieren.

Wenn Sie den Thin Clone eines Snapshot aktualisieren, der abgeleitete Snapshots aufweist, bleiben die abgeleiteten Snapshots unverändert und die Hierarchie intakt. Wenn Sie eine Volume-Gruppe aktualisieren, wird das Point-in-Time-Image auf allen Mitglieds-Volumes ebenfalls aktualisiert.

Wenn Sie eine Ressource aus einem Snapshot aktualisieren, der von einem Remotesystem repliziert wurde, überprüfen Sie die Werte der Erstellungszeit und der Quelldatenzeit, um sicherzustellen, dass Sie den richtigen Snapshot verwenden. Der Wert der **SQuelldatenzeit** der replizierten Snapshots spiegelt die ursprüngliche Quelldatenzeit wider und der Wert für die **Erstellungszeit** wird auf den Zeitpunkt der Replikation aktualisiert.

ANMERKUNG: Da der Aktualisierungsvorgang den Inhalt einer Storage-Ressource ersetzt, wird empfohlen, vor der Aktualisierung einen Snapshot der Ressource zu erstellen. Wenn Sie ein Backup erstellen, können Sie auf einen vorherigen Zeitpunkt zurücksetzen.

Vor der Aktualisierung eines Snapshots ist es zwingend erforderlich, die Anwendung herunterzufahren und das Volume oder das Dateisystem, das auf dem Produktionshost ausgeführt wird, unzumounten und dann den Host-Cache zu löschen, um während des Aktualisierungsvorgangs eine Beschädigung der Daten zu vermeiden.

Aktualisieren eines Volumes mithilfe eines Snapshots

Info über diese Aufgabe

So aktualisieren Sie ein Volume mit einem Snapshot:

Schritte

1. Öffnen Sie das Fenster „Volume-Liste“.
2. Wählen Sie das Volume aus, über das der Snapshot erstellt wurde, um das Fenster „Übersicht“ zu öffnen.
3. Klicken Sie auf die Registerkarte **Protection** und dann auf **Snapshots**.
4. Wählen Sie aus der Snapshot-Liste den Snapshot aus, den Sie für den Aktualisierungsvorgang verwenden möchten.
5. Klicken Sie auf **Weitere Aktionen** > **Mit Snapshot aktualisieren**.
6. Wählen Sie im Slide-Out-Fenster **Mit Snapshot aktualisieren** das Volume oder den Clone aus, das/den Sie über die Dropdownliste **Volume being refreshed** aktualisieren möchten.
7. Legen Sie fest, ob Sie einen Backup-Snapshot des aktualisierten Volumes erstellen möchten (die Option ist standardmäßig ausgewählt).
8. Klicken Sie auf **Aktualisieren**.

Aktualisieren eines Volumes von einem verwandten Volume

Info über diese Aufgabe

Sie können ein Volume mit einem verwandten Volume (einem Clone oder einem indirekten untergeordneten Snapshot) aktualisieren.

Schritte

1. Öffnen Sie das Fenster „Volume-Liste“.
2. Wählen Sie ein Volume und anschließend **Neue Verwendung** > **Mit verbundenem Volume aktualisieren** aus.
3. Klicken Sie im Slide-Out-Fenster **Mit verbundenem Volume aktualisieren** auf **Select volume to refresh from**, und wählen Sie das Quell-Volume aus.
4. Klicken Sie auf **Aktualisieren**.

Aktualisieren des Snapshots eines Dateisystems

Info über diese Aufgabe

Sie können einen Snapshot eines Dateisystems mit seinem direkten übergeordneten Dateisystem aktualisieren.

Schritte

1. Öffnen Sie das Listenfenster des Dateisystems.
2. Wählen Sie das Dateisystem aus, über das der Snapshot erstellt wurde, um das Übersichtsfenster zu öffnen.
3. Klicken Sie auf die Registerkarte **Protection** und dann auf **Snapshots**.
4. Wählen Sie aus der Snapshot-Liste den Snapshot aus, den Sie für den Aktualisierungsvorgang verwenden möchten.
5. Klicken Sie auf **Weitere Aktionen** > **Mit Snapshot aktualisieren**.
6. Klicken Sie auf **Aktualisieren**.

Wiederherstellen einer Speicherressource mithilfe eines Snapshot

Der Wiederherstellungsvorgang wird verwendet, um eine Umgebung nach einem Ereignis zu rekonstruieren, das die Daten beeinträchtigt haben könnte. Mithilfe eines Wiederherstellungsvorgangs können Sie den Inhalt einer übergeordneten Storage-Ressource durch Daten aus einem direkten untergeordneten Snapshot überschreiben. Bei der Wiederherstellung werden die Daten in der übergeordneten Speicherressource auf den Zeitpunkt zurückgesetzt, zu dem der Snapshot erstellt wurde.

Vor der Wiederherstellung eines Snapshots ist es zwingend erforderlich, die Anwendung herunterzufahren und das Dateisystem, das auf dem Produktionshost ausgeführt wird, zu unmounten und dann den Host-Cache zu löschen, um während des Wiederherstellungsvorgangs eine Beschädigung der Daten zu vermeiden.

Wenn Sie eine Volume-Gruppe wiederherstellen, werden alle Mitglieds-Volumes auf den Zeitpunkt des Quell-Snapshot zurückgesetzt.

Wenn Sie eine Ressource aus einem Snapshot wiederherstellen, der von einem Remote-System repliziert wurde, überprüfen Sie den Wert der Quelldatenzeit, um sicherzustellen, dass Sie den richtigen Snapshot verwenden.

Wiederherstellen eines Volumes oder einer Volume-Gruppe aus einem Snapshot

Info über diese Aufgabe

ANMERKUNG: Zur Vermeidung von Datenintegritätsproblemen müssen Sie vor der Wiederherstellung eines Volumes Anwendungen herunterfahren, die das Volume verwenden, und das Volume auf dem Host offline setzen.

Schritte

1. Aktivieren Sie das Kontrollkästchen neben dem Volume oder der Volume-Gruppe, das bzw. die Sie wiederherstellen möchten.
2. Wählen Sie **Protect** > **Restore from Snapshot** aus.
3. Wählen Sie im Slide-Out-Fenster **Restore Volume from Snapshot** den Snapshot aus, der für den Wiederherstellungsvorgang verwendet werden soll.
4. Legen Sie fest, ob Sie einen Backup-Snapshot des wiederhergestellten Volumes oder der Volume-Gruppe erstellen möchten (die Option ist standardmäßig ausgewählt).
5. Klicken Sie auf **Wiederherstellen**.

Wiederherstellen eines Dateisystems aus einem Snapshot

Info über diese Aufgabe

Bevor Sie mit dem Wiederherstellungsvorgang fortfahren, sollten Anwendungen, die das Dateisystem verwenden, heruntergefahren und das Dateisystem auf den Hosts offline gesetzt werden, um Datenintegritätsprobleme zu vermeiden.

Schritte

1. Aktivieren Sie das Kontrollkästchen neben dem Dateisystem, das Sie wiederherstellen möchten.
2. Wählen Sie **Protect** > **Restore from Snapshot** aus.
3. Wählen Sie im Slide-Out-Fenster **Dateisystem aus Snapshot wiederherstellen** den Snapshot aus, der für den Wiederherstellungsvorgang verwendet werden soll.
4. Legen Sie fest, ob Sie einen Backup-Snapshot des wiederhergestellten Dateisystems erstellen möchten (Die Option ist standardmäßig ausgewählt.).
5. Klicken Sie auf **Wiederherstellen**.

Sichere Snapshots

Sichere Snapshots können vor ihrem Ablaufdatum nicht gelöscht werden. Verwenden Sie sichere Snapshots, um Ihre Daten vor bösartigen Angriffen zu schützen.

ANMERKUNG: Sichere Snapshots werden nur für Block-Snapshots unterstützt, die für Volumes oder Volume-Gruppen erstellt werden.

PowerStore ermöglicht das Erzeugen sicherer Snapshots. Im Gegensatz zu regulären Snapshots können sichere Snapshots nicht manuell gelöscht werden und werden nur gelöscht, wenn ihre Ablaufzeit erreicht ist.

ANMERKUNG: Wenn Sie sichere Snapshots verwenden möchten, wird empfohlen, die geschäftlichen Anforderungen mit einem Administrator zu überprüfen, bevor Sie fortfahren, um zu vermeiden, dass das maximale Snapshot-Limit erreicht wird.

Sichere Snapshots bieten Schutz vor versehentlichem oder böswilligem Löschen von Backupdaten und sind effektiv gegen Ransomware-Angriffe. Durch das Erzeugen sicherer Snapshots wird sichergestellt, dass Sie Daten auf einen früheren Zeitpunkt wiederherstellen können.

Um manuell einen sicheren Snapshot für ein Volume oder eine Volume-Gruppe zu erzeugen, wählen Sie die Option **Sicherer Snapshot** im Bereich **Create Snapshot** aus. Um sichere Snapshots als Teil einer lokalen Schutz-Policy zu erzeugen, erstellen Sie eine Snapshot-Regel und wählen Sie die Option **Sicherer Snapshot** im Bereich **Create Snapshot Rule** aus.

ANMERKUNG: Achten Sie darauf, eine Aufbewahrungsfrist für die sicheren Snapshots festzulegen. Die Option „Sicherer Snapshot“ ist nicht verfügbar, wenn **No Automatic Deletion** ausgewählt ist.

ANMERKUNG: Wenn ein Volume-Gruppen-Snapshot als sicher konfiguriert ist, werden alle Mitglieder in der Gruppe als sicher festgelegt.

Sie können sichere Snapshots anzeigen und überwachen, indem Sie der Tabelle „Snapshots“ die Spalte „Sichere Snapshots“ hinzufügen. Sie können auch Snapshot-Listen für sichere Snapshots filtern.

Es ist möglich, vorhandene nicht sichere Snapshots in sichere zu ändern, indem Sie die Option **Sicherer Snapshot** im Bereich **Snapshot Details** auswählen. Gleichermaßen können Sie eine nicht sichere Snapshot-Regel in eine sichere ändern, indem Sie die Option **Sicherer Snapshot** im Bereich **Properties** der Snapshot-Regel auswählen.

ANMERKUNG: Nur Snapshots, die von der Regel erstellt wurden, nachdem sie in eine sichere Regel geändert wurde, sind sichere Snapshots. Snapshots, die vor der Änderung erstellt wurden, bleiben nicht sicher.

Wenn eine sichere Snapshot-Regel gelöscht oder aus einer Policy entfernt wird oder wenn die Ressourcenzuordnung einer Richtlinie, die eine sichere Snapshot-Regel enthält, aufgehoben wird, bleiben sichere Snapshots, die von der Regel erstellt wurden, sicher und können nicht gelöscht werden, bis sie ablaufen. Volumes und Clones mit sicheren Snapshots können erst gelöscht werden, wenn die Snapshots ablaufen.

Die Ablaufzeit sicherer Snapshots kann nicht reduziert, aber auf ein späteres Datum und eine spätere Uhrzeit geändert werden.

Sicherer Snapshot und sichere Replikation:

- Bei Clustern mit PowerStore Version 3.5 und höher werden alle sicheren Snapshots, die auf dem lokalen System erzeugt werden, auf dem Remotecluster als sicher repliziert.
- Wenn auf dem Zielcluster eine PowerStore-Version unter 3.5 ausgeführt wird, werden sichere Snapshots auf diesem Cluster als reguläre Snapshots repliziert. In diesem Fall ist die Snapshot-Regel auf dem Zielcluster nicht sicher. Wenn ein Failover auf einem Cluster mit einer PowerStore-Version unter 3.5 auftritt, werden keine sicheren Snapshots für die Storage-Ressource erstellt.

Nach dem Upgrade von PowerStore auf Version 3.5 können vorhandene nicht sichere Snapshots und Snapshot-Regeln in sichere geändert werden.

Wenn Sie einen sicheren Snapshot löschen müssen, dessen Ablaufzeit noch nicht erreicht wurde, wenden Sie sich an den Dell Support.

4

Schutz-Policies

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Snapshot-Regeln

Sie können Snapshot-Regeln erstellen, um Parameter wie die Häufigkeit der Snapshot-Erstellung und den Aufbewahrungszeitraum für Snapshots zu steuern. Sie können auch Snapshot-Regeln zum Erzeugen sicherer Snapshots erstellen. Mit Snapshot-Regeln in Kombination mit Replikations- und Remotebackupregeln können Sie konsistente Data Protection-Policies gemäß Ihren Data Protection-Anforderungen konfigurieren und auf Storage-Ressourcen anwenden.

Wenn Sie eine Snapshot-Regel zusätzlich zu den vorhandenen Regeln erstellen möchten, sollten Sie die geschäftlichen Anforderungen vorab mit einem Administrator durchgehen. Dies kann dazu beitragen, konsistente Policies im gesamten System zu erreichen und aufrechtzuerhalten.

Erstellen einer Snapshot-Regel

Schritte

1. Wählen Sie **Datensicherheit** > **Datensicherheits-Policies** aus.
2. Klicken Sie im Fenster **Datensicherheits-Policies** in der Leiste **Datensicherheit** auf **Snapshot-Regeln**.
3. Klicken Sie im Fenster **Snapshot-Regeln** auf **Erstellen**.
4. Geben Sie im Slide-Out-Fenster **Snapshot-Regel erstellen** einen Namen für die neue Regel ein.
5. Legen Sie Folgendes fest:
   - Wählen Sie die Tage aus, an denen ein Snapshot erstellt werden soll.
   - Festlegen der Häufigkeit/Startzeit:
     - Wenn ein Snapshot in einem festgelegten Intervall erstellt werden soll, wählen Sie diese Option aus, und legen Sie die Anzahl der Stunden fest, nach deren Ablauf ein Snapshot erstellt wird.
     - Um einen Snapshot zu einem bestimmten Zeitpunkt der ausgewählten Tage zu erstellen, wählen Sie die Option **Tageszeit** aus, und legen Sie die Uhrzeit und die Zeitzone fest.
   - Legen Sie den Aufbewahrungszeitraum fest.
   - Um sichere Snapshots zu erstellen, wählen Sie die Option **Sicherer Snapshot** aus. Weitere Informationen zu sicheren Snapshots finden Sie unter Sichere Snapshots.

     ANMERKUNG: Es wird empfohlen, die geschäftlichen Anforderungen mit einem Administrator zu überprüfen, bevor Sie fortfahren, um zu vermeiden, dass das maximale Snapshot-Limit erreicht wird.
   - Wählen Sie für Datei-Snapshots den Datei-Snapshot-Zugriffstyp aus.
6. Klicken Sie auf **Erstellen**.

Replikationsregeln

Eine Replikationsregel ist ein Satz von Parametern, die das System verwendet, um Daten in einer Replikationssitzung zu synchronisieren. Die Parameter umfassen die Auswahl eines Replikationsziels und die Festlegung eines Recovery Point Objective (RPO).

Nachdem Sie eine Replikationsregel konfiguriert haben, können Sie sie in einer neuen oder vorhandenen Datensicherheits-Policy verwenden, die dann automatisch die Parameter für die Replikationssitzung für jede Speicherressource ändert oder anwendet, für die die Datensicherheits-Policy gilt.

Sie können eine Datensicherheits-Policy nicht ändern, um eine andere Replikationsregel mit einem anderen Remotesystem zu verwenden. Um eine Datensicherheits-Policy mit einer Replikationsregel mithilfe eines anderen Remotesystems zu ändern, entfernen Sie die alte Policy, bevor Sie eine neue zuweisen.

ANMERKUNG: Das Ändern eines Remotesystems erfordert eine vollständige Synchronisation.

Wenn Sie eine neue Replikationsregel zusätzlich zu den vorhandenen Regeln erstellen möchten, wird empfohlen, die Parameter und Ihre geschäftlichen Anforderungen vorab mit einem Administrator durchzugehen. Dies kann dazu beitragen, konsistente Policies im gesamten System zu erreichen und aufrechtzuerhalten.

Erstellen einer Replikationsregel

Schritte

1. Wählen Sie **Datensicherheit** > **Datensicherheits-Policies** aus.
2. Klicken Sie im Fenster **Datensicherheits-Policies** in der Leiste **Schutz** auf **Replication Rules**.
3. Klicken Sie im Fenster **Replication Rules** auf **Erstellen**.
4. Geben Sie im Slide-Out-Fenster **Erstellen Replication Rule** einen Namen für die neue Regel ein.
5. Legen Sie Folgendes fest:
   - Wählen Sie ein vorhandenes Replikationsziel aus, oder konfigurieren Sie ein neues Ziel.
   - Legen Sie die RPO fest.
   - Legen Sie den alert threshold fest.
6. Klicken Sie auf **Erstellen**.

Recovery Point Objective

Die Recovery Point Objective (RPO) gibt die akzeptable Datenmenge, die bei einem Ausfall verloren gehen kann, in Zeiteinheiten an. Wenn Sie eine Replikationsregel einrichten, können Sie die automatische Synchronisation basierend auf der RPO konfigurieren. Mögliche RPO-Werte reichen von 5 Minuten bis 24 Stunden. Das Standard-RPO liegt bei einer Stunde.

ANMERKUNG: Ein kleineres RPO-Intervall bietet mehr Schutz und nimmt weniger Speicherplatz in Anspruch. Es hat jedoch eine höhere Auswirkung auf die Performance, was zu mehr Netzwerkverkehr führt. Ein größeres RPO-Intervall kann zu einer höheren Speicherplatzauslastung führen, was sich auf Snapshot-Zeitpläne und Speicherplatz-Schwellenwerte auswirken kann.

Alert threshold

Wenn Sie eine Replikationsregel konfigurieren, können Sie einen Warnmeldungs-Schwellenwert angeben, d. h. die Zeitdauer, die das System vor der Generierung einer Compliance-Warnmeldung wartet, wenn eine Replikationssitzung die RPO nicht erfüllt. Wird der Warnmeldungs-Schwellenwert auf Null festgelegt, bedeutet dies, dass Warnmeldungen generiert werden, wenn die tatsächliche Synchronisationszeit die RPO überschreitet.

Remotebackupregeln

Erstellen Sie eine Remotebackupregel und fügen Sie sie zu einer Policy hinzu, um Remotebackups zu aktivieren.

Eine Remotebackupregel ist ein Satz von Parametern, mit denen das PowerStore-System Volumes und Volume-Gruppen auf einer PowerProtect DD Appliance sichern kann. Die Regel gibt das Zielsystem an, auf dem Backups erstellt werden, die Häufigkeit des Backupvorgangs und die Aufbewahrungszeit der Backups.

ANMERKUNG: Remotebackupregeln unterstützen keine sicheren Snapshots.

Nachdem Sie die Remotebackupregel erzeugt haben, fügen Sie sie zu einer vorhandenen Schutz-Policy hinzu oder erzeugen Sie eine neue Policy.

ANMERKUNG: Eine Schutz-Policy kann nur eine Remotebackupregel enthalten.

Erstellen einer Remotebackupregel

Schritte

1. Wählen Sie **Datensicherheit** > **Datensicherheits-Policies** aus.
2. Klicken Sie im Fenster **Datensicherheits-Policies** in der Leiste **Schutz** auf **Remotebackupregeln**.
3. Wählen Sie im Fenster **Remotebackupregeln** die Option **Create** aus.
4. Legen Sie Folgendes fest:
   - Rule name
   - Destination: Wählen Sie eine PowerProtect DD aus der Drop-down-Liste aus oder konfigurieren Sie ein neues System (siehe Hinzufügen einer Remoteverbindung für Remotebackups).
   - Wochentage, an denen das Backup erstellt wird.
   - Frequency/Start time: Wenn Sie **Every** auswählen, wird die Backuphäufigkeit in Stunden oder Tagen festgelegt. Wenn Sie **Time of Day** auswählen, wird die Backuphäufigkeit in Tagen festgelegt.
   - Retention period: Wählen Sie die Anzahl der Stunden oder Tage aus, für die die erzeugten Backups aufbewahrt werden sollen.
     ANMERKUNG: Die maximale Aufbewahrung beträgt 25.550 Tage (70 Jahre).
5. Klicken Sie auf **Create**.

Erstellen einer Datensicherheits-Policy

Info über diese Aufgabe

Erstellen Sie eine Datensicherheits-Policy, um lokalen und/oder Remoteschutz für Ihre Storage-Ressourcen bereitzustellen. Jede Datensicherheits-Policy kann eine Replikationsregel, eine Remotebackupregel und bis zu vier Snapshot-Regeln enthalten. Eine Regel kann in mehreren Policies sein.

Schritte

1. Wählen Sie **Datensicherheit** > **Datensicherheits-Policies** aus.
2. Klicken Sie im Fenster **Datensicherheits-Policies** auf **Erstellen**.
3. Geben Sie im Slide-Out-Fenster **Datensicherheits-Policy erstellen** einen Namen für die neue Policy ein.
4. Wählen Sie optional die Snapshot-Regeln aus, die in die Policy aufgenommen werden sollen, oder erstellen Sie eine Snapshot-Regel (siehe Erstellen einer Snapshot-Regel).
5. Wählen Sie optional eine Replikationsregel aus, die in die Policy aufgenommen werden soll, oder erstellen Sie eine Replikationsregel (siehe Erstellen einer Replikationsregel).
6. Wählen Sie optional eine Remotebackupregel aus, die in die Policy aufgenommen werden soll, oder erstellen Sie eine Remotebackupregel (siehe Erstellen einer Remotebackupregel).
7. Klicken Sie auf **Erstellen**.

Ergebnisse

Wenn Sie eine Datensicherheits-Policy erstellen, die eine Replikationsregel enthält, wird die Policy automatisch auf das Remotesystem repliziert und den Zielressourcen zugewiesen, die von der Policy erstellt wurden. Die replizierte Policy und die zugehörigen Regelnamen bestehen aus der Policy und den Regelnamen auf dem Quellsystem mit dem Namen des Remotesystems, das am Ende angehängt wird. Änderungen an der ursprünglichen Policy oder den enthaltenen Regeln werden auf das Remotesystem repliziert, um die Synchronisation aufrechtzuerhalten. Nach einem Replikations-Failover wird die replizierte Policy auf dem Zielsystem aktiviert.

Die replizierten Policies und Regeln werden vom System verwaltet und nicht in der Zielsystem-Policy- und Regel-Tabelle angezeigt. Sie können die Details der Regeln jedoch auf der Registerkarte **Protection** der replizierten Volumes oder Volume-Gruppen anzeigen, indem Sie mit der Maus auf den Namen der replizierten Policy zeigen. Für Datensicherheits-Policies, die Metro-Volumes zugewiesen sind,

wird eine identische schreibgeschützte Policy auf dem Remotesystem erstellt. Diese kann im Fenster **Datensicherheits-Policies** des PowerStore-Managers im Remotesystem angezeigt werden.

Ändern der Datensicherheits-Policy einer Gruppe

Sie können eine Datensicherheits-Policy ändern, indem Sie Snapshot-, Replikations- und Remotebackupregeln hinzufügen und entfernen.

Info über diese Aufgabe

ANMERKUNG: Beim Ändern der Einstellungen einer Datensicherheits-Policy werden die neuen Einstellungen auf alle Objekte angewendet, denen die Datensicherheits-Policy zugewiesen ist. Wenn Sie die Datensicherheits-Policy für eine Ressource ändern wollen, wird empfohlen, dass Sie eine andere Datensicherheits-Policy erstellen und sie stattdessen dieser Ressource zuweisen.

Sie können das Replikationsziel einer Replikationsregel, die in Schutz-Policies verwendet wird, die einer oder mehreren Storage-Ressourcen zugewiesen sind, nicht ändern. Um die Replikation auf einem anderen Remotesystem neu zu konfigurieren, heben Sie die Zuweisung der Datensicherheits-Policy auf und weisen eine neue mit einer anderen Replikationsregel zu. Wenn die Zuweisung einer Datensicherheits-Policy zu einer Replikationsregel aufgehoben wird, wird die zugehörige Replikationssitzung gelöscht. Und bei der Zuweisung einer neuen Datensicherheits-Policy wird eine Sitzung erstellt, die eine vollständige Synchronisation zum neuen Ziel erfordert.

Schritte

1. Wählen Sie **Protection** > **Protection Policies** aus.
2. Aktivieren Sie das Kontrollkästchen neben der entsprechenden Richtlinie, und klicken Sie auf **Modify**.
3. Im Slide-Out-Fenster **Properties** können Sie die folgenden Parameter ändern:
   - Policy name
   - Ausgewählte Snapshot-Regeln
   - Ausgewählte Replikationsregeln
   - Ausgewählte Remotebackupregeln
4. Klicken Sie auf **Anwenden**.

Zuweisen einer Datensicherheits-Policy

Weisen Sie eine Datensicherheits-Policy mindestens einer Storage-Ressource zu, um die in der Policy enthaltenen Snapshot-, Replikations- und Remotebackupregeln auf die Storage-Ressourcen anzuwenden. Die Datensicherheits-Policy führt automatisch Snapshot-Vorgänge, eine Replikation und ein Remotebackup basierend auf den angegebenen Parametern durch.

Wenn eine Datensicherheits-Policy verfügbar ist, die Ihre Data Protection-Anforderungen erfüllt, können Sie sie jederzeit mit einer Storage-Ressource verknüpfen.

Sie können einer Storage-Ressource während der Ressourcenerstellung oder zu einem späteren Zeitpunkt eine Datensicherheits-Policy zuweisen.

Zum Schutz von Block-Storage:

- Weisen Sie Schutz-Policies mit Snapshot-, Replikations- und/oder Remotebackupregeln zu Volumes und Volume-Gruppen zu.
- Wenn Sie eine neue Datensicherheits-Policy zuweisen, die eine Replikationsregel für die Storage-Ressource enthält, ist eine vollständige Erstsynchronisation erforderlich.
- Beim Remotebackup wird durch das Zuweisen einer Policy, die eine Remotebackupregel enthält, zu einem Volume oder einer Volume-Gruppe automatisch eine Remotebackupsitzung im Status „Idle“ erstellt.
- Wenn eine Policy, die eine Remotebackupregel enthält, einer Ressource zugewiesen wird, die kein Remotebackup unterstützt, wird die Regel ignoriert.
- Mit Metro-Volumes können Sie nur Datensicherheits-Policies zuweisen, die Snapshot-Regeln enthalten. Eine Policy, die eine Replikationsregel enthält, kann keinem Metro-Volume zugewiesen werden.

Zum Schutz von Datei-Storage:

- PowerStore unterstützt lokalen Schutz (Snapshots) auf Dateisystemebene und Remoteschutz (Replikation) auf NAS-Serverebene.
- Sie können eine Datensicherheits-Policy nur dann einem NAS-Server zuweisen, wenn sie eine Replikationsregel enthält. Die Replikationsregel wird auf alle Dateisysteme auf dem NAS-Server angewendet und Snapshot-Regeln (falls vorhanden) werden ignoriert.
- Sie können eine Datensicherheits-Policy nur dann einem Dateisystem zuweisen, wenn sie eine Snapshot-Regel enthält. Die Snapshot-Regel wird auf das Dateisystem angewendet und eine Replikationsregel (falls vorhanden) wird ignoriert.

Zuweisen einer Datensicherheits-Policy zu einer Storage-Ressource

Info über diese Aufgabe

Weisen Sie einem Volume, einer Volume-Gruppe, einem Dateisystem oder einem NAS-Server eine Datensicherheits-Policy zu.

Schritte

1. Aktivieren Sie das Kontrollkästchen der Storage-Ressource, der Sie eine Datensicherheits-Policy zuweisen möchten.
2. Wählen Sie für Volumes, Volume-Gruppen und Dateisysteme **Protect** > **Assign Protection Policy** aus. Wählen Sie für NAS-Server **More Actions** > **Assign Protection Policy** aus.

   ANMERKUNG: Wenn Sie eine ungültige Ressource ausgewählt haben, ist die Zuweisungsoption inaktiv. Wenn Sie den Mauszeiger über **Datensicherheits-Policy zuweisen** fahren, wird eine Kurzinformation mit einem Hinweis angezeigt, warum sie für diese Aktion ungültig ist.

3. Wählen Sie im Slide-Out-Fenster **Datensicherheits-Policy zuweisen** die Datensicherheits-Policy aus.
4. Klicken Sie auf **Anwenden**.

Zuweisen einer Datensicherheits-Policy zu mehreren Storage-Objekten

Info über diese Aufgabe

Weisen Sie mehreren Storage-Objekten desselben Typs (Volumes, Volume-Gruppen, Dateisysteme oder NAS-Server) eine Datensicherheits-Policy zu.

Schritte

1. Wählen Sie **Datensicherheit** > **Datensicherheits-Policies** aus.
2. Aktivieren Sie das Kontrollkästchen einer Policy aus der Liste und wählen Sie dann **Weitere Aktionen** > **Datensicherheits-Policy zuweisen** aus.

   Das Slide-out-Fenster **Datensicherheits-Policy zuweisen** enthält eine Zusammenfassung aller Storage-Ressourcen, denen bereits eine Datensicherheits-Policy zugewiesen ist.
3. Wählen Sie im Slide-out-Fenster **Datensicherheits-Policy zuweisen** den Ressourcentyp und anschließend die relevanten Objekte aus der Ressourcenliste aus.
4. Wiederholen Sie Schritt 3, wenn Sie die ausgewählte Policy zusätzlichen Ressourcentypen zuweisen möchten.
5. Klicken Sie auf **Zuweisen**.

Ändern der einem Storage-Objekt zugewiesenen Datensicherheits-Policy

Info über diese Aufgabe

Beachten Sie die folgenden Richtlinien für Replikationsregeln:

- Durch das Ersetzen einer Schutz-Policy, die eine Replikationsregel enthält, durch eine Policy ohne Replikationsregel wird die Replikation von allen Ressourcen entfernt, die dieser Policy zugewiesen sind.
- Durch das Ersetzen einer Schutz-Policy, die eine Replikationsregel enthält, durch eine Policy mit derselben Replikationsregel können Sie den lokalen Schutz neu konfigurieren, ohne die Replikation zu unterbrechen.
- Das Ersetzen einer Schutz-Policy, die eine Replikationsregel enthält, durch eine Policy mit einer anderen Replikationsregel ist nur möglich, wenn für beide Policies dasselbe Remotesystem konfiguriert ist.

  ANMERKUNG: Um die Zuweisung einer Datensicherheits-Policy mit einer Replikationsregel mithilfe eines anderen Remotesystems zu ändern, entfernen Sie die alte Policy, bevor Sie eine neue zuweisen.

Beachten Sie die folgenden Richtlinien für Remotebackupregeln:

- Durch das Ersetzen einer Schutz-Policy, die eine Remotebackupregel enthält, durch eine Policy ohne Remotebackupregel wird der Remoteschutz für das DD-Remotesystem entfernt.

- Das Ersetzen einer Schutz-Policy, die eine Remotebackupregel enthält, durch eine Policy mit derselben Remotebackupregel führt dazu, dass das nächste Backup ein komplettes Backup (und kein inkrementelles Backup) ist.
- Das Ersetzen einer Schutz-Policy, die eine Remotebackupregel enthält, durch eine Policy mit einer anderen Remotebackupregel und demselben Remotesystem führt dazu, dass das nächste Backup ein komplettes Backup (und kein inkrementelles Backup) ist.

Schritte

1. Wählen Sie die relevante Storage-Ressource aus, um das Fenster **Overview** zu öffnen.
2. Klicken Sie auf die Registerkarte **Protection**.
3. Klicken Sie neben dem Namen der zugewiesenen Datensicherheits-Policy auf **Ändern**.
4. Wählen Sie im Slide-Out-Fenster **Datensicherheits-Policy ändern** eine andere Datensicherheits-Policy aus.
5. Klicken Sie auf **Anwenden**.

Aufheben der Zuweisung einer Datensicherheits-Policy

Voraussetzungen

Das Entfernen der Datensicherheits-Policy aus einer Speicherressource führt zu Folgendem:

- Geplante Snapshots und Replikationen gemäß in der Policy definierten Regeln werden gestoppt.
- Vorhandene Snapshots verbleiben und werden gemäß den bei der Erstellung festgelegten Snapshot-Regeln im System aufbewahrt.
- Die Zielspeicherressource wechselt in den schreibgeschützten Modus. Sie können die Zielspeicherressource klonen, um eine Lese-/Schreib Kopie zu erhalten oder das Attribut **Replikationsziel** auf der Seite **Eigenschaften** der Storage-Ressource zu ändern.

ANMERKUNG: Sie können die Zuweisung einer Datensicherheits-Policy nicht aufheben, während der Import durchgeführt wird.

Schritte

1. Aktivieren Sie das Kontrollkästchen der Storage-Ressource, der Sie eine Datensicherheits-Policy zuweisen möchten.
2. Wählen Sie für Volumes, Volume-Gruppen und Dateisysteme **Protect** > **Unassign Protection Policy** aus. Wählen Sie für NAS-Server **More Actions** > **Unassign Protection Policy** aus.
3. Klicken Sie zum Bestätigen auf **Zuweisung aufheben**.

5

Replikation

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Synchronisation

Mit PowerStore können Sie die Zielressource asynchron mit Änderungen (z. B. Änderungen an Inhalt, Größe und Mitgliedschaft) aktualisieren, die seit dem letzten Synchronisationszyklus auf der Quellressource aufgetreten sind.

Die Synchronisation kann automatisch – nach einem festgelegten Zeitplan – oder manuell erfolgen. Snapshots werden vom Quellsystem zum Zielsystem synchronisiert und die Effizienz der Blockfreigabe wird beibehalten.

ANMERKUNG: Die Synchronisation von Virtual Volumes wird nur für schreibgeschützte Snapshots unterstützt.

Wenn ein Volume auf dem Zielsystem einem Host zugeordnet ist, legt das System die Node-Affinität für dieses Volume fest. Infolgedessen werden alle I/O-Vorgänge automatisch an den ausgewählten Node weitergeleitet. Es ist nicht erforderlich, die Replikationssitzung anzuhalten und fortzusetzen, damit die I/O-Umleitung wirksam wird. Das Festlegen der Node-Affinität für Volumes auf dem Zielsystem bietet Lastenausgleich und verhindert latenzbasierte Replikationen. Sie können die Node-Affinität manuell mithilfe der REST API festlegen.

ANMERKUNG: Wenn die Spalte für Node-Affinität in der Tabelle „Volumes“ nicht angezeigt wird, fügen Sie sie mithilfe der Option **Show/Hide Table Columns** hinzu.

ANMERKUNG: Wenn Sie einer Volume-Gruppe Volumes hinzufügen oder die Größe der Volume-Gruppe während einer asynchronen Replikationssitzung ändern, werden die Änderungen nicht sofort auf dem Ziel angezeigt. Sie können entweder eine manuelle Synchronisation durchführen oder warten, bis die Synchronisation basierend auf der RPO erfolgt.

Bei NAS-Servern werden alle Dateisysteme auf einem geschützten NAS-Server vom Quell- zum Zielsystem synchronisiert.
Wenn Dateisysteme während einer asynchronen Replikationssitzung geändert werden, werden die Änderungen beim nächsten Synchronisationszyklus auf dem Zielsystem übernommen.

Sie können eine Replikationssitzung synchronisieren, wenn sie einen der beiden Status aufweist:

- normal laufen
- System angehalten

Während eine Replikationssitzung synchronisiert wird, können Sie die folgenden Aktionen ausführen:

- Ein geplantes Failover vom Quellsystem durchführen
- Ein Failover vom Zielsystem durchführen
- Replikationssitzungen im Quell- oder Zielsystem anhalten
- Eine Replikationssitzung durch Entfernen einer Schutz-Policy löschen

Wenn die Synchronisation fehlschlägt, wird die Replikationssitzung in den Status „System paused“ versetzt. Wenn das System wiederhergestellt wird, fährt die Replikationssitzung an dem Punkt fort, an dem sie angehalten wurde.

Failover

Das Failover einer Replikationssitzung umfasst das Wechseln der Rollen zwischen den Quell- und Zielsystemen und das Umkehren der Richtung der Replikationssitzung.

Es gibt zwei Arten von Failovern:

- Geplantes Failover – Vom Nutzer initiiert: umfasst die Synchronisation zwischen Quelle und Ziel, um Datenverlust zu vermeiden.
- Ungeplantes Failover – Vom Zielsystem als Reaktion auf den Ausfall des Quellsystems initiiert.

Während eines Failovers der Replikationssitzung führt das System die folgenden Aktionen aus:

- Beenden der I/O-Vorgänge auf dem Quellobjekt
- Synchronisieren der Quell- und Zielspeicherobjekte (tritt nur bei einem geplanten Failover auf)
- Beenden der Replikationssitzung
- Umkehren der Rollen zwischen Quell- und Zielsystemen
- Heraufstufen der neuesten Objektversion auf der neuen Quelle
- Fortsetzen von I/O-Vorgänge auf der neuen Quelle (initiiert vom Benutzer)

Nach einem Failover können Sie auf Anwendungen auf dem neuen Quellsystem zugreifen, um Daten wiederherzustellen.

Durchführen eines Failover-Tests

Nachdem Sie eine Replikationssitzung eingerichtet haben, können Sie die Verbindung testen, um sicherzustellen, dass ihre Standorte ordnungsgemäß konfiguriert und für die Disaster Recovery vorbereitet sind.

Während eines Failover-Tests führt das System ein Failover durch und der Produktionszugriff wird mit replizierten Daten oder einem Point-in-Time-Snapshot zum Zielstandort bereitgestellt. Die Zielspeicherressource ist im Lese-/Schreibzugriff verfügbar und Produktionszugriff ist für Hosts und Anwendungen aktiviert. Sie können Ihre Disaster-Recovery-Konfiguration überprüfen, während die Replikation weiterhin im Hintergrund ausgeführt wird.

Wenn Sie den Failover-Test beenden möchten, wählen Sie eine der folgenden Aktionen aus:

- Failover auf die aktuellen Testdaten – Wenn Sie während des Failover-Tests Änderungen an den Daten vorgenommen haben, können Sie die aktualisierten Testdaten verwenden. Dadurch wird der Test beendet und die Testdaten werden beibehalten. Alle Daten, die während des Tests von der Quelle repliziert werden, werden verworfen und das Zielsystem wird die Quelle.

  ANMERKUNG: Sie müssen diese Änderungen lediglich bestätigen, bevor Sie ein Failover auf die Testdaten durchführen.
- Failover-Test beenden – Wenn Sie den Test beenden, wird der Produktionszugriff auf das Ziel für Hosts und Anwendungen deaktiviert und die Zielspeicherressource wird mit den neuesten Daten aktualisiert, die vom Quellsystem synchronisiert wurden. Sie können einen Backup-Snapshot der Testdaten erstellen, bevor Sie den Failover-Test beenden.

Beschränkungen

Ein Failover-Test kann nur unter den folgenden Bedingungen durchgeführt werden:

- Die Version von PowerStore auf dem Quell- und dem Zielsystem ist 2.x oder höher.
- Der Status der Replikationssitzung lautet nicht „Initialisierung läuft“, „Failover läuft“, „Failover durchgeführt“, „Für NDU/Migration angehalten“ oder „Failover-Test läuft“.

Während des Failover-Tests können Sie auf dem Zielsystem keine der folgenden Aktionen ausführen:

- Volume-Gruppenmitgliedschaft ändern
- Volume-Gruppengröße erhöhen
- Volume-Gruppennamen ändern
- Migration starten
- Entfernen einer Datensicherheits-Policy

ANMERKUNG: Sie können diese Aktionen weiterhin über das Quellsystem durchführen.

Sie können während eines Failover-Tests kein geplantes Failover durchführen. Beenden Sie den Failover-Test, um ein geplantes Failover durchzuführen. Ungeplante Failover werden jedoch möglicherweise in Reaktion auf eine Katastrophe weiterhin ununterbrochen durchgeführt. Wenn möglich, wird empfohlen, den Failover-Test vor einem ungeplanten Failover zu beenden, da alle Daten verloren gehen, die nach dem Start des Failover-Tests an das Ziel repliziert wurden.

Sie können Replikationssitzungen auch während eines Failover-Tests anhalten und wiederaufnehmen. Wenn Sie während eines Failover-Tests eine Replikationssitzung löschen, wird der Test abgebrochen.

Starten eines Failover-Tests

Sie können einen Failover-Test über die aktuellen Zieldaten oder einen beliebigen Snapshot starten.

Es gibt zwei Möglichkeiten, einen Failover-Test zu starten:

- Wählen Sie unter **Datensicherheit** > **Replikation** die Replikationssitzung aus, die Sie testen möchten, und wählen Sie dann **Failover-Test starten** aus.
- Wählen Sie auf der Registerkarte **Datensicherheit** der Ressource die Option **Replikation** und dann **Failover-Test starten** aus.

Nach dem Start des Failover-Tests wird in der Replikationssitzung eine Warnmeldung ausgegeben. Die Warnmeldung wird gelöscht, nachdem der Test beendet wurde.

Stoppen eines Failover-Tests

Bevor Sie den Failover-Test beenden, wird empfohlen, Dateisysteme zu unmounten und alle laufenden Anwendungen auf der Zielressource zu beenden, um eine Datenbeschädigung zu vermeiden.

Es gibt zwei Möglichkeiten, einen Failover-Test zu beenden:

- Wählen Sie unter **Datensicherheit** > **Replikation** die Replikationssitzung aus, in der ein Test durchgeführt wird, und wählen Sie dann **Failover-Test stoppen** aus.
- Wählen Sie auf der Registerkarte **Datensicherheit** der Ressource, auf der ein Test durchgeführt wird, die Option **Replikation** und dann **Failover-Test stoppen** aus.

Sie können auch einen Snapshot erstellen, um die Testdaten zu speichern, die während des Failover-Tests erstellt wurden.

Geplantes Failover

Wenn Sie ein geplantes Failover durchführen, erfolgt ein manuelles Failover der Replikationssitzung vom Quellsystem zum Zielsystem. Vor dem Failover wird das Zielsystem mit dem Quellsystem synchronisiert, um Datenverlust zu vermeiden.

Bevor Sie ein geplantes Failover durchführen, müssen Sie sicherstellen, dass alle I/O-Vorgänge für Anwendungen und Hosts beendet sind. Sie können keine Replikationssitzung anhalten, bei der gerade ein geplantes Failover durchgeführt wird.

Während eines geplanten Failover können Sie die folgenden Aktionen ausführen:

- Führen Sie ein ungeplantes Failover durch.
- Löschen Sie die Replikationssitzung durch Entfernen der Datensicherheits-Policy auf der Storage-Ressource.

Sie können während eines Failover-Tests kein geplantes Failover durchführen.

Sie können einen geplanten Failover-Test über die aktuellen Zieldaten oder einen beliebigen Snapshot starten.

Es gibt zwei Möglichkeiten, um ein geplantes Failover zu initiieren:

- Wählen Sie unter **Datensicherheit** > **Replikation** die relevante Replikationssitzung und dann **Geplantes Failover** auswählen.
- Wählen Sie auf der Registerkarte **Datensicherheit** der Ressource die Option **Replikation** und dann **Geplantes Failover** aus.

Nach einem geplanten Failover ist die Replikationssitzung inaktiv. Verwenden Sie die Aktion **Neu schützen**, um die Zielspeicherressource zu synchronisieren und die Replikationssitzung fortzusetzen. Sie können auch die Option zum automatischen Schutz auswählen, bevor Sie das Failover durchführen. Dadurch wird die Synchronisation nach Abschluss des Failovers automatisch in die entgegengesetzte Richtung (bei der nächsten RPO) initiiert und die Quelle und das Zielsystem werden in einen normalen Status zurückversetzt.

Netzwerktrennung während eines DRT

Bei der Durchführung eines DRT wird nicht empfohlen, einen Netzwerkfehler zwischen dem lokalen und dem Remote-System zu simulieren und dann ein ungeplantes Failover auf das Zielsystem durchzuführen, um den Zugriff auf den DR-NAS-Server zu ermöglichen. Da keine Kommunikation zwischen den Systemen besteht, kann PowerStore nicht sicherstellen, dass sich beide NAS-Server in einem kompatiblen Zustand befinden. Nachdem die Verbindung wiederhergestellt wurde, befinden sich beide NAS-Server im Produktionsmodus (Split Brain). Demzufolge wechseln beide Systeme in den Wartungsmodus, um zu verhindern, dass Daten auf beide Speicherorte geschrieben werden.

Um diesen Status zu beheben, ist ein Eingreifen des technischen Supports erforderlich.

Weitere Informationen finden Sie im Dell Wissensdatenbank-Artikel 000215482 (Cutting the network connection between sites...).

Ungeplantes Failover

Ein ungeplantes Failover erfolgt nach Ereignissen auf Quellsystemen wie einem Quellsystemausfall oder Ereignissen, die zu Ausfallzeiten beim Produktionszugriff führen. Ein ungeplantes Failover wird vom Zielsystem initiiert und ermöglicht Produktionszugriff auf die ursprüngliche Zielressource von einem zeitpunktspezifischen Snapshot.

Wenn Sie ein ungeplantes Failover initiieren, können Sie auswählen, ob Sie die neueste Datenkopie oder einen Snapshot der Daten (falls verfügbar) als Datenquelle verwenden möchten.

Wenn die Verbindung zum Quellsystem wiederhergestellt ist, wird die ursprüngliche Quellressource in den Zielmodus versetzt. Verwenden Sie die Option **Erneut schützen**, um die Ziel-Storage-Ressource zu synchronisieren und dann die Replikationssitzung fortzusetzen.

ANMERKUNG: Bei der Durchführung einer Dateireplikation wird nicht empfohlen, das Dateimobilitätsnetzwerk nach einem ungeplanten Failover zu ändern. Nachdem die Verbindung zwischen den Quell- und Zielsystemen wiederhergestellt wurde, kann es sein, dass sich beide NAS-Server im Produktionsmodus befinden.

Zusätzliche Überlegungen zur Replikation

Wenn während der Blockreplikation das Quellsystem für NDU angehalten wird und das Zielsystem aktiv ist, wird der Status des Zielsystems in *System_Paused* geändert. Wenn das Zielsystem während des unterbrechungsfreien Upgrades des Quellsystems inaktiv ist und das Zielsystem wieder aktiv ist, verbleibt es im Status *OK*.

Wenn das Quellsystem während der Dateireplikation für ein unterbrechungsfreies Upgrade angehalten wird, verbleibt das Zielsystem unabhängig vom Verbindungsstatus im Status *OK*.

Testen der Disaster Recovery für NAS-Server, die sich in der Replikation befinden

Ein Disaster-Recovery-Test führt einen Disaster-Recovery-Plan durch, mit dem Sie überprüfen können, ob das System die Daten und den Betrieb im Notfall wiederherstellen kann.

PowerStore bietet mehrere Optionen, um die Fähigkeit des Systems zur Wiederherstellung nach einem Ausfall und zur Wiederherstellung der Funktionen zu testen:

- Klonen eines NAS-Servers für Disaster-Recovery-Tests mithilfe eindeutiger IP-Adressen.
- Klonen eines NAS-Servers für Disaster Recovery-Tests mithilfe eines isolierten Netzwerks mit doppelten IP-Adressen.
- Geplantes Failover (siehe Abschnitt oben).

Klonen eines NAS-Servers für Disaster-Recovery-Tests mithilfe eindeutiger IP-Adressen

Info über diese Aufgabe

Das Klonen eines NAS-Servers ist die empfohlene Option zum Testen von DR. Sie können den NAS-Server mit PowerStore Manager klonen und testen, ohne die Produktion zu beeinträchtigen. Um den Zugriff auf den neu geklonten NAS-Server zu aktivieren, muss eine neue und eindeutige Netzwerkschnittstelle konfiguriert werden. Die konfigurierte IP-Adresse kann weder auf dem Quell- noch auf dem Ziel-NAS-Server verwendet werden. Eindeutige Einstellungen sind auch erforderlich, um den Server einer AD-Domain hinzuzufügen.

Änderungen, die auf den geklonten Dateisystemen und auf Produktionsdateisystemen vorgenommen werden, beeinflussen sich nicht gegenseitig. Wenn der DR-Test abgeschlossen ist, kann der geklonte Server gelöscht werden.

Sie können eine der folgenden Optionen verwenden:

- Klonen Sie den NAS-Server auf dem Quellsystem, replizieren Sie ihn auf das Ziel und führen Sie ein geplantes Failover auf das Zielsystem durch.
- Klonen Sie den NAS-Server auf dem Zielsystem und greifen Sie auf die Daten zu (Failover ist nicht erforderlich, da die geklonten Ressourcen bereits auf dem Zielsystem zugänglich sind).

Schritte

1. Wählen Sie in PowerStore Manager **Storage** > **NAS-Server** aus.
2. Wählen Sie den NAS-Server, den Sie klonen möchten, und dann **Neue Verwendung** > **NAS-Server klonen** aus.
3. Geben Sie im Fenster **Clone erstellen** einen Namen für den Clone an und wählen Sie die Dateisysteme aus, die Sie klonen möchten.
4. Wählen Sie **Erstellen** aus.
   Der geklonte NAS-Server wird der Serverliste hinzugefügt.
5. Wählen Sie den Namen des geklonten NAS-Servers aus, um das Fenster mit den Serverdetails zu öffnen.
6. So fügen Sie eine Netzwerkschnittstelle hinzu:
   a. Wählen Sie die Registerkarte **Netzwerk** aus.
   b. Wählen Sie unter **Dateischnittstelle** die Option **Hinzufügen** aus.
   c. Geben Sie die Schnittstelleninformationen an und wählen Sie **Hinzufügen** aus.
7. So legen Sie das Freigabeprotokoll fest:
   a. Wählen Sie die Registerkarte **Protokollfreigaben**.
   b. Wählen Sie das entsprechende Protokoll (SMB, NFS oder FTP) aus.
   c. Ändern Sie die erforderlichen Felder und wählen Sie **Anwenden** aus.
8. Führen Sie die folgenden Schritte aus, wenn Sie den Quell-NAS-Server geklont haben:
   a. Replizieren Sie den NAS-Server auf das Zielsystem. Weitere Informationen finden Sie unter Replikation.
   b. Führen Sie ein geplantes Failover zum Ziel durch. Weitere Informationen finden Sie unter Geplantes Failover.
   c. Überprüfen Sie, ob der Host auf die Daten zugreifen kann.
9. Wenn Sie den replizierten Produktionsserver auf dem Zielsystem geklont haben, ist kein Failover erforderlich. Überprüfen Sie den Hostzugriff.

Klonen eines NAS-Servers für Disaster Recovery-Tests mithilfe eines isolierten Netzwerks mit doppelten IP-Adressen

Die Disaster Recovery kann mit derselben Konfiguration wie die Produktion getestet werden. Durch die Verwendung identischer Einstellungen kann das Risiko reduziert und die Reproduzierbarkeit in einem Ausfallszenario erhöht werden. Die Verwendung doppelter IP-Adressen führt jedoch zu Konflikten. Durch die Ausführung des DR-Tests in einer Umgebung, die von der Produktionsumgebung isoliert ist, können diese Konflikte vermieden werden.

Ab PowerStore Version 3.6 können Sie eine isolierte Disaster Recovery-Testumgebung (DRT) erstellen, um für den Notfall gerüstet zu sein.

Durch das Erstellen einer isolierten Umgebung können Sie dieselbe IP-Adresse und denselben Hostnamen wie das Produktionssystem verwenden und eines DRT für einen NAS-Server unter Replikation ohne Auswirkungen auf die Produktion durchführen.

Um eine DRT-Umgebung zu erstellen, müssen Sie ein isoliertes Netzwerk mit einem separaten DRT-Router einrichten und Link Aggregations mit den Netzwerk-I/O-Ports erstellen.

Erstellen Sie mithilfe von PSTCLI oder REST API eine dedizierte Netzwerkumgebung auf dem Zielserver, indem Sie den NAS-Server unter Replikation auf dem Ziel-PowerStore-System klonen. Der Clone ist eine vollständige Kopie der Produktionsumgebung und einer dedizierten Testumgebung, die von der Produktion isoliert ist. Sie können eine isolierte Netzwerkumgebung erstellen und die Testumgebung mit derselben IP-Adresse und demselben Hostnamen wie das Produktionssystem konfigurieren. Der DRT-NAS-Server hat keine Auswirkungen auf die Produktionsumgebung und kann ohne IP-Adressenkonflikte ausgeführt werden, wenn Failover und Failback auf dem Replikations-NAS-Server erfolgen.

So testen Sie DR mithilfe einer isolierten Testumgebung:

1. Erstellen Sie den NAS-Server-Clone auf dem Ziel. Verwenden Sie die `is_dr_test`-Markierung.
2. Erstellen Sie eine Nutzer-Bond-Schnittstelle für NAS mit derselben IP-Adresse wie der Quell-NAS-Server.
3. Fügen Sie den Clone dem AD hinzu (falls erforderlich).
4. Überprüfen Sie, ob Hosts auf die Daten zugreifen können.

ANMERKUNG: Sie können DRT auch auf eigenständigen NAS-Servern verwenden.

Voraussetzungen und Einschränkungen

Wenn Sie eine DRT-Umgebung erstellen möchten, müssen Sie sicherstellen, dass die folgenden Anforderungen erfüllt sind:

- Abrufen der Informationen zum privaten Netzwerk:
  - Gateway
  - Netzmaske
  - VLAN-ID (optional)
- Identifizieren Sie die Netzwerkports des isolierten Netzwerks und der Netzwerkports des Produktionsnetzwerks.

Beachten Sie die folgenden Einschränkungen beim Erstellen einer DRT-Umgebung:

- Die für DRT dedizierte Bond-Schnittstelle kann nicht verwendet werden, um andere Produktions-NAS-Server zu erstellen.
- Ein NAS-Server, der als Produktion konfiguriert ist, kann nicht als Teil des DRT neu konfiguriert werden.
- Ein NAS-Server, der als Teil des DRT konfiguriert ist, kann nicht als Produktion neu konfiguriert werden.
- Ein NAS-Server, der nicht mehr Teil eines DRT ist, kann nicht neu konfiguriert und muss gelöscht werden.
- Nachdem ein NAS-Server aktiv und mit Netzwerkinformationen konfiguriert wurde, sollte die zusätzliche Konfiguration (z. B. DNS, CAVA und Kerberos) manuell durchgeführt werden.
- Der DRT-fähige NAS-Server kann nicht repliziert werden.
- Das Ändern und Löschen des NAS-Servers kann mithilfe von PowerStore Manager durchgeführt werden.

Konfigurieren der Disaster Recovery-Testumgebung mithilfe von PSTCLI

Schritte

1. Rufen Sie den Namen des (zu klonenden) NAS-Servers am Zielstandort ab:

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> nas_server show
# | id | name | operational_status |  current_node_id  | file_interfaces.ip_addre~
--+-------------+--------+--------------------+-------------------
1 |647f545a-4b11-5cdd-4d4c-eeeba81eb143 | File80| Started | R2C4-appliance-1-node~|
127.1.1.1
```

2. Klonen Sie den NAS-Server, indem Sie einen neuen Namen für den Clone angeben und den Switch `-is_dr_test true` verwenden:

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> nas_server -name File80
clone -name File80_c -is_dr_test true
Success
```

3. Suchen Sie die IP-Port-ID für die NAS-Dateibündelung, die mit dem isolierten Netzwerk verbunden ist:

   ANMERKUNG: Wenn die NAS-Dateibündelung nicht erstellt wurde, können Sie sie mithilfe von PSTCLI oder PowerStore Manager erstellen.

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> ip_port_show -output nvp
8:  id =IP_PORT23
    current_usages =
    ip_pool_addresses =
    bond:
    name=BaseEnclosure-NodeA-bond1
```

4. Erstellen Sie die Schnittstelle für den geklonten NAS-Server:

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> file_interface create
-nas_server_name File80_c -ip_address "10.10.10.10" -prefix_length 24 -gateway
"10.10.10.1" -vlan_id 5
-ip_port_id IP_PORT23
Created
# |     id
--+------------------------------------
1 |64830ae5-2760-59ce-4c90-82772509648e
```

5. Zeigen Sie die Dateischnittstelle an:

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> file_interface_show
# |id | nas_server_id | ip_address | prefix_length | gateway | is_disabled
--+-------------+--------+--------------------+-------------------
  1 |647f5509-11f4-a52d-ee1f-82772509648e | 647f545a-4b11-5cdd-4d4c-eeeba81eb143 |
10.10.10.10 |24 | 10.10.10.1 | no
```

```
  2 |64830ae5-2760-59ce-4c90-82772509648e | 6483092f-3e71-8a92-0a0b-82772509648e |
10.10.10.10 |24 | 10.10.10.1 | no
```

Konfigurieren eines NAS-Servers in einer DRT-Umgebung mithilfe der REST API

Info über diese Aufgabe

ANMERKUNG: Überspringen Sie diesen Abschnitt, wenn Sie keine REST API verwenden.

Schritte

1. Um den NAS-Server im angegebenen Namespace zu klonen, führen Sie `/nas_server/{id}/clone` aus und geben Sie `is_dr_test` als „true“ an.
2. Führen Sie zum Erstellen einer Netzwerkschnittstelle `/file_interface` aus und geben Sie die Parameter für das private Netzwerk an.

   ANMERKUNG: In diesem Schritt wird die Dateischnittstelle für den geklonten NAS-Server mit derselben IP-Adresse, derselben Netzmaske und demselben Gateway wie der NAS-Produktionsserver erstellt. Verwenden Sie die/den Bond-Schnittstelle/IP_Port, die/der dem privaten Netzwerk zugeordnet ist.

Ergebnisse

Der NAS-Server ist aktiv und kann für DRT im isolierten Netzwerk verwendet werden.

Replikation von Virtuellen Volumes

PowerStore lässt sich in VMware Site Recovery Manager (SRM) integrieren, um die asynchrone Replikation von Virtuellen Volumes zu unterstützen.

Der Remoteschutz virtueller Maschinen wird mithilfe von vSphere Storage Policy-Based Management (SPBM) konfiguriert. Für die Recovery nach einem Ausfall wird das Failover virtueller Maschinen mithilfe von VMware SRM konfiguriert.

VMware SRM ist eine Disaster-Recovery-Lösung von VMware, die die Recovery oder Migration virtueller Maschinen zwischen einem geschützten Standort und einem Recovery-Standort automatisiert.

Snapshot- und Replikationsregeln, die in PowerStore erstellt werden, sind für vSphere verfügbar und können Datensicherheits-Policies hinzugefügt werden. vSphere stellt eine Storage-Policy für PowerStore während der vVol-Erstellung bereit.

Eine Replikationsgruppe mit Virtual Volumes, die zusammen repliziert werden sollen, ist die Replikations- und Failover-Einheit, die in vSphere konfiguriert ist.

Sowohl schreibgeschützte Snapshots als auch Snapshots mit Lese-/Schreibzugriff können für vVols erzeugt werden. Die manuelle oder gemäß dem festgelegten Zeitplan durchgeführte Synchronisation wird nur auf schreibgeschützte Snapshots angewendet.

So zeigen Sie die Details einer Replikationssitzung für Virtuelle Volumes an:

1. Wählen Sie **Schutz** > **Replikation** aus.
2. Klicken Sie auf den Status der Replikationssitzung, um Details anzuzeigen.

Die Grafik im Detailfenster der Replikationssitzung zeigt an, dass vSphere die Replikationssitzung verwaltet.

Im Detailfenster der Replikationssitzung können Sie Folgendes tun:

- Die Details der Replikationssitzung anzeigen.
- Die Replikationsgruppe umbenennen.
- Halten Sie die Replikationssitzung an und nehmen Sie sie wieder auf.
- Die Replikationssitzung synchronisieren.

Voraussetzungen

Stellen Sie vor dem Konfigurieren der Replikation von Virtual Volumes sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Sowohl das lokale als auch das Remotesystem müssen verbunden sein und über vVol-Funktionen verfügen (siehe Remotesysteme).

- Storage-Container müssen auf beiden Systemen definiert werden (**Storage** > **Storage-Containers** > **Erstellen**), damit sie gekoppelt werden können. Wenn auf jedem System ein einziger Storage-Container vorhanden ist, werden die Storage-Container automatisch gekoppelt. Andernfalls ist es erforderlich, das Ziel des Storage-Containers manuell anzugeben (**Storage** > **Storage-Container** > **[Storage-Container]** > **Schutz** > **Erstellen**).

Erstellen einer Replikationssitzung für Virtual Volumes

Info über diese Aufgabe

Weitere Informationen zur erforderlichen Konfiguration auf vSphere finden Sie in der VMware SRM-Nutzerdokumentation.

Schritte

1. Erstellen Sie in PowerStore eine Replikationsregel.

   Die Replikationsregel wird vCenter als Replikationsfunktion zur Verfügung gestellt.
2. Erstellen Sie auf vSphere eine Policy mithilfe der verfügbar gemachten Regel.

   Eine schreibgeschützte Kopie der Schutz-Policy mit einem identischen Namen wird PowerStore hinzugefügt (sichtbar in der Tabelle **„Schutz-Policies“**) und mit einem Sperrsymbol markiert.

   ANMERKUNG: Sie können auch Snapshot-Regeln hinzufügen, um den lokalen Schutz zu aktivieren.

   ANMERKUNG: Es ist nicht möglich, eine schreibgeschützte Schutz-Policy zu erstellen, zu ändern oder zu löschen und die Policy virtuellen Maschinen mithilfe von PowerStore zuzuweisen oder die Zuweisung aufzuheben. Um diese Aktionen durchzuführen, verwenden Sie die Storage-Policy-Aktualisierung in vSphere.
3. Erstellen Sie auf vSphere eine virtuelle Maschine, weisen Sie eine Storage-Policy mit einer Replikationsregel zu und verknüpfen Sie sie mit einer Replikationsgruppe.

Ergebnisse

Die Replikationsgruppe und die Replikationssitzung werden automatisch in PowerStore erstellt (sichtbar unter **Schutz** > **Replikation** > **[Replikationsgruppensitzung]**).

Überwachen der Replikationsgruppen-Performance

Wenn eine Storage-Policy mit einer PowerStore-Replikationsregel auf VMware erstellt und einer vVol-basierten VM zugewiesen wird, wird eine Replikationssitzung auf PowerStore für die vVol-Ressourcen in derselben Ressourcengruppe erstellt. VMware SRM verwendet diese VMware-Ressourcengruppen, um die geschützten VMs in Replikationsgruppen zu managen.

Sie können die Performance einer Replikationsgruppe über PowerStore überwachen. Wählen Sie **Protection** > **Replication** aus und klicken Sie auf den Sitzungsstatus einer vVol-Replikationssitzung, um die Sitzungsdetails anzuzeigen (der **Ressourcentyp** sollte *Replication Group* sein). Klicken Sie auf die Registerkarte **Replication Group Performance**, um die Performancedaten für die Replikationsgruppe anzuzeigen. Sie können auswählen, Diagramme der folgenden Daten anzuzeigen:

- Replication Remaining Data (Verbleibende Replikationsdaten)
- Replication Bandwidth (Normalized) (Replikationsbandbreite (normalisiert))
- Replication Transfer Time (Replikationsübertragungsdauer)

Sie können auch die Zeitskala für die angezeigten Daten festlegen.

Recovery virtueller Maschinen

Site Recovery Manager (SRM) ist eine Disaster-Recovery-Lösung von VMware, die die Recovery virtueller Maschinen während des Ausfallstatus automatisiert.

Um die Recovery virtueller Maschinen zu aktivieren, muss ein Recovery-Plan mithilfe von SRM konfiguriert werden. Ein Recovery-Plan führt vordefinierte Recovery-Schritte für ausgewählte Replikationsgruppen aus. Die Recovery-Schritte umfassen Failover-, Reprotect- und Failover-Tests.

Eine Schutzgruppe wird auf vSphere erstellt, die eine oder mehrere Replikationsgruppen und einen Recovery-Plan umfasst. Wenn ein Fehler auftritt, führt der SRM den Recovery-Plan auf den Virtual Volumes in den Replikationsgruppen aus.

In PowerStore können Sie den Status der Replikationssitzung während der Recovery überwachen.

Weitere Informationen finden Sie unter *VMware Site Recovery Manager*.

6

Metro-Schutz

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Voraussetzungen und Einschränkungen

Berücksichtigen Sie vor der Konfiguration von Metro die folgenden Einschränkungen:

- Metro-Unterstützung ist nur für PowerStore T-Modell-Appliances verfügbar. Metro wird von PowerStore X-Modell-Appliances nicht unterstützt.
- Metro-Schutz ist nur für Volumes aktiviert.
- Metro-Schutz unterstützt FC/SCSI- oder iSCSI-verbundene VMware ESXi-Hosts.
- Metro Witness wird bei HCI-Bereitstellungen von PowerStore nicht unterstützt.

Wenn eine Verbindung zu einem Remotesystem hergestellt wird, erkennt das System automatisch die Konfiguration und aktiviert die unterstützten Funktionen für das Remotesystem. Um die Block-Metro-Funktion zu aktivieren, überprüfen Sie, ob die folgenden Bedingungen auf beiden PowerStore-Systemen erfüllt sind:

- Auf den beiden Systemen wird PowerStore 3.x oder höher ausgeführt.
- Die Latenz auf dem Remotesystem ist niedrig.
- Der Datenverbindungstyp ist TCP: Wenn lokale und Remote-PowerStore-Systeme mit Version 3.x (oder höher) installiert sind, wird die TCP-Verbindung automatisch unterstützt. Wenn jedoch auf einem oder beiden PowerStore-Systemen Version 2.x ausgeführt wird, müssen Sie die Systeme auf 3.x aktualisieren, um Metro zu aktivieren. Nach dem Upgrade wird eine Warnmeldung angezeigt, in der Sie den Verbindungstyp des Remotesystems aktualisieren müssen. Klicken Sie auf den Link in der angezeigten Warnmeldung, um das Fenster **Remotesystemtransport aktualisieren** zu öffnen. Klicken Sie dann auf **Transport aktualisieren**.

  ANMERKUNG: Die Warnmeldung wird erst gelöscht, nachdem der Transport aktualisiert wurde.

Um einen Witness bereitzustellen, müssen Sie sicherstellen, dass die folgenden Voraussetzungen erfüllt sind:

- Der Witness muss auf einem Linux-Host (virtuell oder physisch) installiert sein.

  ANMERKUNG: Es wird dringend empfohlen, den Witness auf einer dritten Fehlerdomäne bereitzustellen, die von den beiden PowerStore-Systemen getrennt ist.
- Unterstützte Betriebssysteme:
  - Red Hat 8.8
  - SUSE Linux Enterprise Server (SLES) 15 SP5
- Abhängigkeiten (auf dem Linux-Host erforderlich):
  - Java 11
  - SQLite

ANMERKUNG: Bei Verwendung eines Paketmanagers (z. B. yum oder zypper) werden die aufgeführten Abhängigkeiten automatisch installiert.

- Hardware:
  - Das Betriebssystem muss auf einer x64-CPU-Architektur ausgeführt werden.
  - Mindestens 4 GB RAM
  - Mindestens 5 GB freier Speicherplatz
- Ports:
  - Port 443/tcp muss vor der Installation des Witness auf dem Witness-Host geöffnet sein.
  - Firewalls von Rechenzentren müssen Datenverkehr auf Port 443 zulassen, damit PowerStore Anforderungen an den Witness senden kann.
- Netzwerklatenz – Maximale Latenz von 100 Millisekunden im Managementnetzwerk zwischen PowerStore und dem Witness
- Zugriff auf das Nutzerkonto – Root- oder sudo-Zugriff ist erforderlich, um den Witness auf dem Host zu installieren.
- Stellen Sie die Konnektivität zum PowerStore-Managementnetzwerk sicher.
- Für einen virtuellen Witness wird empfohlen, eine statische IP-Adresse für die Witness-VM zu verwenden. Wenn Sie jedoch DHCP verwenden, fügen Sie PowerStore den Witness mithilfe des vollständig qualifizierten Domänennamens (FQDN) hinzu.

Konfigurieren der Hostkonnektivität

ANMERKUNG: Hostunterstützung wird für VMware vSphere Metro-Storage-Cluster bereitgestellt. Fibre Channel- und SCSI-Konnektivität werden unterstützt.

Die Host-Metro-Konnektivität ist auf lokalen und Remote-PowerStore-Systemen konfiguriert und ermöglicht es Hosts und Anwendungen, physische Volumes von den beiden Systemen als ein einziges Volume zu erkennen. Wenn Sie die Metro-Konnektivität für den Host konfigurieren, wählen Sie das bevorzugte Array aus, um zu bestimmen, welches System im Falle eines Ausfalls Zugriff auf den Storage behalten wird.

Um die Host-Metro-Konnektivität zu aktivieren, muss ein ESXi-Host sowohl auf dem lokalen als auch auf dem Remotesystem definiert und mit beiden Systemen verbunden sein.

Wenn Sie einen neuen ESXi-Host erstellen, können Sie mit dem Assistenten **Host hinzufügen** die Hostverbindung festlegen:

ANMERKUNG: Die Optionen für die Hostverbindung werden im Assistenten **Host hinzufügen** grafisch dargestellt.

- **Lokale Konnektivität** – Bietet Hostzugriff nur auf das lokale System.
  ANMERKUNG: Lokale Konnektivität kann auch mit Metro-Volumes verwendet werden.
- **Metro-Konnektivität** – Bietet Hostzugriff auf lokale und Remotesysteme. Wenn Sie diese Option auswählen, legen Sie den Systemzugriff fest:
  - **Host befindet sich am selben Standort wie dieses System** – Die Hostpfadlatenz ist für das lokale System niedriger und für das Remotesystem höher. Der Host versucht immer, I/O-Vorgänge an das lokale System zu senden (außer wenn das lokale System ausgefallen ist).
  - **Host befindet sich am selben Standort wie das Remotesystem** – Die Hostpfadlatenz ist für das Remotesystem niedriger. Der Host versucht immer, I/O-Vorgänge an das Remotesystem zu senden (außer wenn das Remotesystem ausgefallen ist).
  - **Befindet sich auf beiden Systemen** – Latenz und Performance des Hostpfads sind für lokale und Remotesysteme gleich. Der Host sendet I/O-Vorgänge basierend auf seinen Multipath-Überlegungen an die lokalen oder Remotesysteme.

ANMERKUNG: Unabhängig von der konfigurierten Konnektivität müssen alle Hosts auf demselben vCenter Cluster konfiguriert werden.

ANMERKUNG: Für einen ESXi-Host, der einem Metro-Volume zugeordnet ist, wird empfohlen, das Round-Robin-Pfadauswahl-Plug-in (PSP) mit aktiviertem Latenzmodus zu verwenden.

ANMERKUNG: Wenn eines der Systeme offline geht, gibt der ESXi-Host eine APD-Bedingung (All Paths Down) ein. Um diese Bedingung zu beheben, wird empfohlen, vSphere HA zu konfigurieren. Diese Konfiguration ermöglicht es virtuellen Maschinen auf verfügbaren ESXi-Hosts, neu zu starten und das APD-Problem zu beheben.

Metro Witness

Ab PowerStore Version 3.6 können Sie einen Witness-Server zum Metro-Schutz hinzufügen, um Schutz vor einzelnen Ausfallszenarien zu bieten.

Der Witness-Server ist ein passiver Drittanbieter, der auf einem eigenständigen Host installiert ist (vorzugsweise in einem anderen Rechenzentrum). Wenn ein Fehler auftritt, kontaktieren die lokalen und Remote-PowerStore-Systeme den Witness-Server und fordern die Unterteilung der Metro-Sitzung an. Der Witness bestimmt dann, welches System für Hosts zugänglich bleibt, und bedient weiterhin I/O-Vorgänge. Wenn möglich, hat der Witness Vorrang vor dem PowerStore-System, dem die bevorzugte Rolle zugewiesen wurde. Das Hinzufügen des Witness zu einer Metro-Sitzung bietet Schutz vor einzelnen Ausfallszenarien, einschließlich bevorzugter Systemausfälle, die nicht ohne Witness verarbeitet werden.

Der Witness-Service ist einfach und verwaltet keine kritischen Daten, die nicht neu erstellt werden können. Daher muss der Witness weder gesichert, gespeichert noch wiederhergestellt, sondern er kann entfernt und neu installiert werden, wenn eine Recovery erforderlich ist.

Bereitstellen des Metro Witness

Wenn die Voranforderungen erfüllt sind, können Sie den Witness direkt mit RPM installieren. Andernfalls können Sie die Abhängigkeiten automatisch mit einem Paketmanager (yum, zypper) installieren. Sie können das Installationspaket von der Dell Support-Seite herunterladen.

Führen Sie den folgenden Befehl aus, um den Witness-Service auf einem Linux-Host zu installieren:

```
sudo rpm -i <rpm_file>
```

ANMERKUNG: Sie können den Witness mit einem Paketmanager oder Mit RPM deinstallieren.

ANMERKUNG: Metro Witness wird bei HCI-Bereitstellungen von PowerStore nicht unterstützt.

Konfigurieren des Metro Witness

Info über diese Aufgabe

- Nur Administrator, Sicherheitsadministrator und Storage-Administrator sind berechtigt, den Witness zu konfigurieren.
- Sie können Witness vor oder nach der Konfiguration von Metro konfigurieren.
- Pro Metro-Cluster kann nur ein Witness konfiguriert werden.
- Das konfigurierte Metro wird für alle Metro-Sitzungen verwendet und kann für bestimmte Sitzungen nicht deaktiviert werden.
- Der Witness-Status ändert sich erst in „Aktiviert“, nachdem er für lokale und Remote-PowerStore-Systeme konfiguriert wurde.
- Auf die Witness-Server-Installationstools (sicherer Tokengenerator und Fingerabdruck) können Sie über den folgenden Pfad zuzugreifen:

```
sles15:~ # ls /opt/dell-witness-service/scripts
```

ANMERKUNG: Führen Sie die folgenden Schritte für lokale und Remote-PowerStore-Systeme aus.

Schritte

1. Wählen Sie im PowerStore Manager **Schutz** > **Witness** aus.
2. Wählen Sie im Fenster **Metro Witness die Option Hinzufügen** aus.
3. Füllen Sie im Fenster **Witness hinzufügen** die folgenden Felder aus:
   - Name
   - IP-Adresse/vollständig qualifizierter Domainname
   - Sicherheitstoken – Um ein Sicherheitstoken zu erzeugen, führen Sie das Skript „generate_token.sh“ aus. Weitere Informationen finden Sie im *PowerStore Sicherheitskonfigurationsleitfaden* auf der PowerStore-Dokumentationsseite.

     ANMERKUNG: Das Token läuft in zehn Minuten ab.
   - Beschreibung (optional)
4. Wählen Sie **Hinzufügen**.
5. Überprüfen Sie im Fenster **Nutzerautorisierung** den Fingerabdruck des Witness-Zertifikats und wählen Sie **Bestätigen** aus, um ihn zu akzeptieren.

   ANMERKUNG: Weitere Informationen finden Sie im *PowerStore Sicherheitskonfigurationsleitfaden* auf der PowerStore-Dokumentationsseite.

   Das Zertifikat wird im PowerStore-System gespeichert.

Ergebnisse

Der Witness wird erstellt und alle vorhandenen Metro-Volumes werden ihm automatisch zugewiesen. Neu erstellte Metro-Volumes werden automatisch dem Witness zugewiesen. Die Spalte **Metro-Ressourcen** im Fenster **Metro Witness** zeigt die Anzahl der Ressourcen an, die dem Witness zugewiesen sind. Wenn Sie auf die Zahl klicken, wird das Fenster **Metro-Ressourcen** geöffnet.

Witness-Änderung und -Recovery

Der Witness-Service ist einfach und verwaltet keine kritischen Daten, die nicht neu erstellt werden können. Daher muss der Witness weder gesichert, gespeichert noch wiederhergestellt, sondern er kann entfernt und neu installiert werden, wenn eine Recovery erforderlich ist.

Ändern der Lockbox-Parameter

Info über diese Aufgabe

Im Fenster **Witness-Eigenschaften** können Sie den Namen und die Beschreibung des Witness ändern.

ANMERKUNG: Wenn Sie die Witness-IP-Adresse oder den vollständig qualifizierten Domainnamen ändern möchten, müssen Sie den Witness entfernen und neu installieren.

Schritte

1. Wählen Sie **Schutz** > **Metro Witness** aus.
2. Aktivieren Sie das Kontrollkästchen neben dem Volume und wählen Sie **Ändern** aus.
3. Ändern Sie die erforderlichen Felder und wählen Sie **Anwenden** aus.

Ersetzen des Witness

Info über diese Aufgabe

Um den Witness zu ersetzen, entfernen Sie ihn aus den PowerStore-Systemen und fügen Sie ihn anschließend hinzu. Dieses Verfahren ist auch dann erforderlich, wenn sich der Hostname oder die IP-Adresse nicht geändert haben, da der neue Witness über ein anderes Zertifikat verfügt, das den PowerStore-Systemen hinzugefügt werden muss.

Schritte

1. Entfernen Sie den Witness aus jedem der PowerStore-Systeme. Weitere Informationen finden Sie unter Entfernen des Witness.
2. Fügen Sie den Witness jedem der PowerStore-Systeme hinzu. Weitere Informationen finden Sie unter Konfigurieren des Metro-Witness.

Ändern der Witness-Hostkonfiguration

Wenn der Host, auf dem der Witness installiert ist, geändert werden muss, können Sie einen der folgenden Schritte ausführen:

- Erstellen Sie einen Host mit der erforderlichen Konfiguration und installieren Sie den Witness. Entfernen Sie dann den vorhandenen Witness aus den PowerStore-Systemen und ersetzen Sie ihn durch den neuen Witness.
- Ändern Sie den vorhandenen Host:
  - Entfernen Sie den vorhandenen Witness aus den PowerStore-Systemen. Weitere Informationen finden Sie unter Entfernen des Witness.
  - Deinstallieren Sie den Witness vom vorhandenen Host.
  - Nehmen Sie die erforderlichen Konfigurationsänderungen auf dem Host vor.
  - Installieren Sie den Witness auf dem Host neu. Weitere Informationen finden Sie unter Bereitstellen des Metro Witness.
  - Fügen Sie den Witness zu den PowerStore-Systemen hinzu. Weitere Informationen finden Sie unter Konfigurieren des Metro-Witness.

Überwachen des Witness

Durch Auswahl von **Schutz** > **Metro Witness** > **[Witness]** werden die Witness-Eigenschaften angezeigt.

Der Witness hält die Kommunikation mit jedem Node auf jeder Appliance aufrecht.

Das Fenster **Eigenschaften** zeigt den Verbindungsstatus für jeden Node und den Gesamtverbindungsstatus des Witness an.

Die folgenden Verbindungsstatus sind verfügbar:

- Wird initialisiert – Alle Nodes initialisieren die Verbindung zum Witness.
- OK – Alle Nodes können mit dem Witness kommunizieren.
- Wird gelöscht – Der Witness wird aus dem Cluster gelöscht.
- Teilweise verbunden – Einige Nodes auf einigen Appliances können mit dem Witness kommunizieren oder derselbe Witness ist nicht auf dem Peer-System registriert.
- Nicht verbunden: Es können nicht alle Nodes mit dem Witness kommunizieren.

Nachdem der Witness konfiguriert wurde, versuchen alle Metro-Sitzungen unabhängig voneinander, mit ihm in Kontakt zu treten. Jede Metro-Sitzung weist einen Status auf, der angibt, ob die Metro-Sitzung den Witness verwenden kann, wenn ein Fehler auftritt. Mögliche Witness-Status für eine Metro-Sitzung:

- Wird initialisiert – Der Witness wird initialisiert, aber nicht eingebunden.
- Abgekoppelt – Die Metro-Sitzung wurde angehalten oder unterbrochen.
- Eingebunden – Alle Nodes auf allen Appliances sind mit dem Witness verbunden und können ihn verwenden, wenn ein Fehler auftritt.
- Abgekoppelt, ungültige Konfiguration oder nicht verfügbar: Die Witness-Konfiguration ist ungültig (der Witness ist beispielsweise nur auf einem PowerStore-System konfiguriert oder zwei verschiedene Witness-Komponenten sind auf dem lokalen und dem Remotesystem konfiguriert) oder der Witness ist nicht verfügbar.
- Abgekoppelt, konnte nicht initialisiert werden: Der Witness konnte nicht mit der Metro-Sitzung initialisiert werden.
- Dekonfiguration in Bearbeitung: Der Witness wird aus dem PowerStore-System entfernt.

Wenn das Cluster über mehrere Appliances verfügt, sind einige der Appliances möglicherweise mit dem Witness verbunden, andere nicht. Aus diesem Grund wird der Witness möglicherweise nicht für alle vorhandenen Metro-Sitzungen eingebunden.

Entfernen des Witness

Sie können den Witness jederzeit aus PowerStore entfernen, unabhängig davon, ob er Metro-Sitzungen zugewiesen ist.

Um den Witness zu entfernen, wählen Sie **Schutz** > **Metro Witness** aus, aktivieren Sie dann das Kontrollkästchen neben dem Witness und wählen Sie **Löschen** aus.

Wenn Sie den Witness löschen, wird er aus allen Metro-Sitzungen entfernt und die Sitzungen verwenden wieder Voreinstellungsregeln, um das Systemverhalten bei einem Ausfall zu bestimmen.

Wenn während des Löschens des Witness ein Fehler auftritt, verbleibt er im Status „Dekonfiguration in Bearbeitung“, bis der Fehler behoben ist, und setzt dann den Löschvorgang fort.

Witness – Fehlerszenarien

Wenn in einer Metro-Umgebung mit Witness ein Fehler auftritt, verhält sich das System wie folgt:

Wenn die Verbindung zwischen dem lokalen und dem Remotesystem unterbrochen wird, wird die Metro-Sitzung aufgeteilt. Beide Systeme fordern eine Aufteilung der Witness-Sitzung an. Der Witness antwortet mit „Erfolg“ auf die erste Anforderung und mit „Fehler“ auf die zweite Anforderung. Das System, das „Erfolg“ als Antwort erhalten hat, behält den Host-I/O-Zugriff auf das Metro-Volume bei, während das System, das den Fehler erhalten hat, sich selbst herabstuft.

Das nicht bevorzugte System sendet die Anforderung einige Sekunden nach dem bevorzugten System an den Witness. Wenn das bevorzugte System aktiv ist, erhält es die Antwort „Erfolg“ und wird ausgewählt, um den Host-I/O-Zugriff aufrechtzuerhalten.

Wenn das bevorzugte System ausgefallen ist, sendet es keine Anforderung an den Witness und das nicht bevorzugte erhält die Antwort „Erfolg“.

Wenn eines der Systeme die Verbindung zum Host verliert, hat dies keine Auswirkungen, da beide Systeme noch aktiv sind und der Host darauf zugreifen kann. Wenn ein Verbindungsverlust zwischen den Systemen auftritt, erhält das System, das noch mit dem Witness verbunden ist, die Antwort „Erfolg“ und behält den Host-I/O-Zugriff bei.

Konfigurieren eines Metro-Volumes

Info über diese Aufgabe

Durch die Aktivierung der Metro-Konfiguration für ein Volume wird es für Hosts von zwei PowerStore-Systemen mit einer Remotesystemverbindung sichtbar.

Die folgenden Volumes können nicht als Metro konfiguriert werden:

- Ein Volume-Clone
- Ein Volume, dem eine Datensicherheits-Policy zugewiesen ist, die eine Replikationsregel enthält
- Ein Volume, das zu einer Volume-Gruppe gehört
- Ein Volume mit einer schreibgeschützten Datensicherheits-Policy
- Ein Volume, das migriert oder importiert wird
- Ein Volume mit einem schreibgeschützten Replikationsziel, das nach dem Entfernen der Replikation bestehen bleibt

ANMERKUNG: Wenn ein Witness für dieses PowerStore-System konfiguriert wurde, wird das Metro-Volume automatisch dem Witness zugewiesen.

Schritte

1. Wählen Sie **Storage** > **Volume** aus und aktivieren Sie das Kontrollkästchen eines Volumes.
2. Wählen Sie **Schützen** > **Metro-Volume konfigurieren** aus.
   Das Slide-Out-Fenster **Metro-Volume konfigurieren** wird angezeigt.
3. Wählen Sie ein Remotesystem aus oder konfigurieren Sie ein neues Remotesystem.
4. Wählen Sie optional das Remotesystem zur Platzierung des Volumes aus.
5. Klicken Sie auf **Konfigurieren**.
6. Weisen Sie auf dem Remotesystem das konfigurierte Metro-Volume einem Host zu.

Festlegen der Metro-Rolle

Das System, von dem das Metro-Volume konfiguriert wird, wird bei der Konfiguration des Metro-Volumes automatisch als bevorzugt festgelegt. Wenn das Metro-Volume unterteilt oder angehalten wird und Metro Witness nicht konfiguriert ist, behält das bevorzugte System den Host- und Produktionszugriff sowie eine aktive Zuordnung zu einer Schutz-Policy bei.

Wenn der Metro-Volume-Status „Läuft normal“ (aktiv/aktiv) lautet, können Sie die Metro-Volume-Rolle mithilfe der folgenden Optionen von „Bevorzugt“ in „Nicht bevorzugt“ oder umgekehrt ändern:

- **Bevorzugte Rolle ändern**: Verwenden Sie diese Option, um die aktuelle Rolle eines ausgewählten Metro-Volumes zu ändern. Diese Option kann sowohl vom bevorzugten als auch vom nicht bevorzugten System verwendet werden.

  ANMERKUNG: Diese Option befindet sich im Detailfenster des Metro-Volumes.
- **Lokale Rolle auf „Bevorzugt“ festlegen**: Verwenden Sie diese Option, um die Rolle mehrerer ausgewählter nicht bevorzugter Metro-Volumes auf „Bevorzugt“ festzulegen. Diese Option sollte vor dem Herunterfahren des bevorzugten Systems für geplante Wartungsarbeiten verwendet werden. Wenn Sie die nicht bevorzugten Metro-Volumes auf „Bevorzugt“ festlegen, kann das Metro-Volume den Host- und Produktionszugriff während des Herunterfahrens fortsetzen.

Überwachen von Metro-Ressourcen

Info über diese Aufgabe

Sie können alle Metro-Objekte im System überwachen und Aktionen für ausgewählte Ressourcen durchführen oder den Status eines ausgewählten Metro-Volumes überwachen.

Schritte

1. Wählen Sie im Dashboard **Schutz** > **Metro** aus, um die Liste der Metro-Ressourcen und -Details zu öffnen.

   ANMERKUNG: Wenn Metro Witness konfiguriert ist, können Sie auch auf die Metro-Ressourcenliste zugreifen, indem Sie **Schutz** > **Metro Witness** > **Metro-Ressourcen** auswählen.

2. Aktivieren Sie das Kontrollkästchen einer Metro-Ressource, um die Aktionen anzuzeigen, die Sie auf diesem Volume durchführen können.
3. Um detaillierte Informationen zu einer bestimmten Metro-Ressource anzuzeigen, klicken Sie auf den Status des Volumes in der Spalte **Metro-Status**.

   Sie können auch detaillierte Informationen zu einer Metro-Ressource auf der Seite **Storage** > **Volumes** anzeigen.

   a. Klicken Sie auf der Seite **Storage** > **Volumes** auf den Namen eines Metro-Volumes, um die Seite mit den Informationen zu dem Volume anzuzeigen.
   b. Wählen Sie die Karte **Schutz** und dann die Registerkarte **Metro-Volume** aus, um die Informationen zum Metro-Volume anzuzeigen.

Anhalten eines Metro-Volumes

Info über diese Aufgabe

Das vorübergehende Anhalten eines Metro-Volumes ist in den folgenden Szenarien erforderlich:

- Wenn Konfigurationsänderungen erforderlich sind, die nicht durchgeführt werden können, wenn das Volume normal funktioniert, z. B. Ändern der Volume-Eigenschaften.
- Wenn die bevorzugten oder nicht bevorzugten Systeme gewartet werden müssen, z. B. der Austausch fehlerhafter Hardwarekomponenten oder Änderungen in der Netzwerkinfrastruktur.
- Wenn ein Fehler auf dem bevorzugten System vorliegt, für das das nicht bevorzugte System hochgestuft werden muss, um ein kontrolliertes Recovery zu ermöglichen.

Es kann entweder vom bevorzugten oder nicht bevorzugten System angehalten werden. Wenn ein Metro-Volume angehalten wird, wird die Synchronisation zwischen den Systemen vorübergehend gestoppt. Produktionszugriffs- und Datensicherheits-Policies bleiben auf dem bevorzugten System aktiv.

Wenn ein Metro-Volume aufgeteilt ist und keine Verbindung zwischen dem lokalen und dem Remotesystem besteht, wird es nur auf dem lokalen System angehalten (wo es implementiert wurde):

- Wenn es auf dem bevorzugten System angehalten wird
  - Der Host- und Produktionszugriff bleiben auf einem angehaltenen, bevorzugten Metro-Volume aktiviert.
  - Host- und Produktionszugriff bleiben auf dem nicht bevorzugten Metro-Volume unverändert.
- Wenn es auf dem bevorzugten System angehalten wird:
  - Der Host- und Produktionszugriff bleiben deaktiviert, sofern das Metro-Volume nicht hochgestuft wurde.
  - Da keine Netzwerkverbindung vorhanden ist, wird durch das angehaltene Metro-Volume nicht der bevorzugte Metro-Volume-Status geändert.
- Wenn die Verbindung aufgelöst wurde, sollte das Metro-Volume auch vom Remotesystem angehalten werden.

Schritte

1. Wählen Sie **Schutz** > **Metro** aus.
2. Aktivieren Sie das Kontrollkästchen des Metro-Volume, das Sie anhalten möchten, und klicken Sie auf **Anhalten**.
   Das Slide-Out-Fenster **Metro-Volume anhalten** wird angezeigt.
3. Klicken Sie zur Bestätigung auf **Anhalten**.

Fortsetzen eines Metro-Volumes

Info über diese Aufgabe

Die Fortsetzung kann entweder vom bevorzugten System oder vom nicht bevorzugten System gestartet werden.

Wenn Sie ein bevorzugtes, angehaltenes Metro-Volume fortsetzen, startet das bevorzugte System die Synchronisation von Daten mit dem nicht bevorzugten System. Nach Abschluss der Synchronisation kehrt der Metro-Volume-Status in den Aktiv-Aktiv-Zustand zurück.

Wenn Sie ein hochgestuftes (zuvor nicht bevorzugtes) angehaltenes Metro-Volume fortsetzen, startet das nicht bevorzugte System die Synchronisation mit dem bevorzugten System (Reprotecting-Status), um in den Aktiv-Aktiv-Zustand zurückzukehren.

ANMERKUNG: Wenn ein Metro-Volume für längere Zeit angehalten wurde, kann die Synchronisation aufgrund des angesammelten Datenvolumens auf dem bevorzugten System eine Weile dauern.

Wenn das nicht bevorzugte System hochgestuft wurde, werden durch die Wiederaufnahme des Metro-Volumes aus dem hochgestuften nicht bevorzugten System die Daten vom hochgestuften nicht bevorzugten System mit dem bevorzugten System synchronisiert.

Schritte

1. Wählen Sie **Schutz** > **Metro** aus.
2. Aktivieren Sie das Kontrollkästchen des fortzusetzenden Metro-Volumes und klicken Sie auf **Fortsetzen**.
   Das Dialogfeld **Metro-Volume fortsetzen** wird angezeigt.
3. Klicken Sie zur Bestätigung auf **Fortsetzen**.

Hochstufen eines Metro-Volumes

Voraussetzungen

Das Hochstufen eines Metro-Volumes ist im Zustand `Fractured` oder `Paused` zulässig.

Info über diese Aufgabe

Wenn die Verbindung zwischen den beiden Storage-Systemen ausfällt oder wenn das nicht bevorzugte System ausgefallen ist, wird die Synchronisation zwischen den Systemen angehalten und das Metro-Volume wird aufgeteilt. Das bevorzugte System bleibt aktiv und bedient weiterhin I/Os. Wenn sich der Nutzer auf dem bevorzugten System befindet, ist keine Aktion erforderlich. Die Systeme werden synchronisiert, wenn das Problem behoben ist.

Wenn auf dem bevorzugten System ein Fehler auftritt, wird die Synchronisation zwischen den Systemen gestoppt und das Metro-Volume wird aufgeteilt. Beide Systeme bedienen keine I/O mehr. Um auf das Metro-Volume zugreifen zu können, müssen NutzerInnen das Metro-Volume auf dem nicht bevorzugten System hochstufen, um den Host- und Produktionszugriff darauf zu aktivieren, bis das bevorzugte System wiederhergestellt wird. Wenn der/die NutzerIn feststellt, dass das bevorzugte System verfügbar ist, kann das Metro-Volume auf dem nicht bevorzugten System problemlos hochgestuft werden. Wenn sich der/die NutzerIn auf dem nicht bevorzugten System befindet, kann der Status des bevorzugten Systems nicht bestimmt werden (ob das System ausgefallen ist oder die Verbindung zum System getrennt wurde). In diesem Fall kann das Hochstufen des Metro-Volumes auf dem nicht bevorzugten System dazu führen, dass beide Systeme weiterhin I/O bedienen, aber nicht synchronisiert werden.

Schritte

1. Wählen Sie **Schutz** > **Metro** aus.

   Die Metro-Seite listet alle Metro-Ressourcen auf und ermöglicht die Bewertung aller betroffenen Volumes und die Priorisierung beim Hochstufen entsprechend Ihren Überlegungen.

   ANMERKUNG: Der Metro-Status des Volumes sollte `Fractured` lauten.

2. Klicken Sie auf den Status des Metro-Volumes, um die Seite „Metro-Volume“ anzuzeigen, und klicken Sie auf **Hochstufen**.
   Das Slide-Out-Fenster **Metro-Volume hochstufen** wird angezeigt.

   ANMERKUNG: Vor der Hochstufung wird ein Snapshot des Metro-Volumes erstellt.

3. Vergewissern Sie sich, das Sie die Auswirkungen des Hochstufens des Metro-Volumes verstehen, falls das Remotesystem I/Os verarbeitet, und überprüfen Sie nach Möglichkeit, ob das Remotesystem ausgefallen ist.
4. Aktivieren Sie das Bestätigungskontrollkästchen unten im Slide-Out-Fenster **Metro-Volume hochstufen** und wählen Sie **Hochstufen** aus.
   Der hochgestufte Status des Volumes wird im Abschnitt „Details des Metro-Volume“ auf der Seite **Metro-Volume** angezeigt.

Herunterstufen eines Metro-Volumes

Info über diese Aufgabe

Wenn der Speicherplatz auf dem bevorzugten System knapp wird, wird die Synchronisation zwischen den Systemen gestoppt und das Metro-Volume wird aufgeteilt. Beide Systeme bedienen keine I/O mehr. In diesem Fall muss das Metro-Volume auf dem nicht bevorzugten System hochgestuft werden, um Host- und Produktionszugriff darauf zu ermöglichen, bis das bevorzugte System das Problem behebt. Zur Aktivierung dieses Status muss zuerst das Metro-Volume auf dem bevorzugten System heruntergestuft werden.

Schritte

1. Wählen Sie **Schutz** > **Metro** aus.

   ANMERKUNG: Die Metro-Seite listet alle Metro-Ressourcen auf und ermöglicht die Bewertung aller betroffenen Volumes und die Priorisierung beim Hochstufen entsprechend Ihren Überlegungen.

2. Klicken Sie auf den Status eines Metro-Volumes, um die Seite „Metro-Volume“ anzuzeigen, und klicken Sie auf **Herunterstufen**.
   Das Slide-Out-Fenster **Metro-Volume herunterstufen** wird angezeigt.
3. Vergewissern Sie sich, das Sie die Auswirkungen des Herunterstufens des Metro-Volumes verstehen, falls das Remotesystem I/Os verarbeitet, und überprüfen Sie nach Möglichkeit, ob das Remotesystem ausgefallen ist.
4. Klicken Sie auf **Herunterstufen**.
   Der heruntergestufte Status des Volumes wird im Abschnitt „Details des Metro-Volume“ auf der Seite „Metro-Volume“ angezeigt.

Beenden eines Metro-Volumes

Info über diese Aufgabe

Wenn Sie ein Metro-Volume beenden, wird die Metro-Konfiguration entfernt, was zu zwei unabhängigen Volumes führt. Wenn das Remote-Volume nicht gelöscht wird, entfernt das System die ihm zugewiesene Datensicherheits-Policy, hebt die Zuordnung der Hosts auf und weist sie einem neuen, anderen SCSI-WWN zu. Sie können ein Metro-Volume entweder vom bevorzugten oder vom nicht bevorzugten System beenden.

Schritte

1. Wählen Sie **Storage** > **Volume** aus und aktivieren Sie das Kontrollkästchen eines Volumes.
2. Wählen Sie **Schützen** > **Metro-Volume beenden** aus.
   Das Slide-Out-Fenster **Metro-Volume beenden** wird angezeigt.
3. Wählen Sie eine der folgenden Optionen aus dem Slide-Out-Fenster aus:
   - Beenden Sie Metro und behalten Sie das Volume auf dem lokalen und dem Remotesystem.
     ANMERKUNG: Das Remotesystem hebt die Zuordnung der Hosts auf und weist dem Volume einen anderen SCSI-WWN zu.
   - Beenden Sie Metro und löschen Sie das Volume und alle zugehörigen Snapshots auf dem Remotesystem.
4. Klicken Sie auf **Beenden**.

Verwenden von Schutz-Policies mit Metro

Wenn ein vorhandenes Metro-Volume einer Schutz-Policy zugewiesen wird oder ein Volume mit einer Schutz-Policy für Metro konfiguriert ist, wird derselbe Schutz auf das Metro-Volume auf beiden Systemen angewendet. Die Schutz-Policy, die auf dem Remotesystem erstellt wird, ist schreibgeschützt. Änderungen an der Schutz-Policy und den Snapshot-Regeln können nur an der Policy vorgenommen werden, die vom Nutzer erstellt wurde (unabhängig vom Storage-System, auf dem sie erstellt wurde). Die schreibgeschützte Policy wird alle 15 Minuten mit den Änderungen synchronisiert.

Vom Nutzer initiierte Snapshots, die auf einem Storage-System erstellt werden, werden auch auf dem anderen System erzeugt.

ANMERKUNG: Die asynchrone Replikation wird bei Metro-Volumes nicht unterstützt. Eine Schutz-Policy, die eine Replikationsregel enthält, kann keinem Metro-Volume zugewiesen werden.

Die Zuweisung einer Schutz-Policy kann auf dem lokalen oder Remotesystem (entweder bevorzugt oder nicht bevorzugt) erfolgen.

Die Zuweisung der Schutz-Policy sollte auf dem Storage-System erfolgen, auf dem sie zugewiesen wurde. Nachdem die Zuweisung der Schutz-Policy zum Volume im lokalen System aufgehoben wurde, wird die Zuweisung zum Volume auf dem anderen System aufgehoben. Sobald die schreibgeschützte Schutz-Policy nicht mehr von Metro-Volumes verwendet wird, wird sie automatisch aus dem System gelöscht.

ANMERKUNG: Wenn die Zuweisung der Policy zum Storage-System, dem sie zugewiesen wurde, aufgrund eines Metro-Volume-Ausfalls nicht aufgehoben werden kann, ist Folgendes zulässig:

- Eine schreibgeschützte Policy kann nicht zugewiesen oder gegen eine Lese-/Schreib-Policy von einem bevorzugten Metro-Volume ausgetauscht werden, wenn sie aufgeteilt ist.
- Eine schreibgeschützte Policy kann für eine Lese-/Schreib-Policy von einem hochgestuften, nicht bevorzugten Metro-Volume aufgehoben oder ausgetauscht werden.

ANMERKUNG: Wenn das Metro-Volume aufgeteilt oder eine Metro-Sitzung angehalten wird, werden Snapshots nur auf dem aktiven System erzeugt. Wenn das Metro-Volume von allein behoben oder die Sitzung fortgesetzt wird, werden die Snapshots nicht auf das Remotesystem kopiert und bleiben auf dem lokalen System, bis sie ablaufen oder gelöscht werden.

7

Remotebackup

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Terminologie

Tabelle 2. Remotebackupterminologie

BEGRIFF	DESCRIPTION
PowerProtect DD	Eine Data Domain Appliance der neuen Generation, die in erster Linie für Datenbackups entwickelt wurde.
PowerProtect Data Manager	Eine zentrale Managementanwendung für das Management eines oder mehrerer physischer oder Cloud-interner PowerProtect DD-Systeme.
DD Storage Unit	Eine logische Einheit auf PowerProtect DD, die für Backupanwendungen über das DD Boost-Protokoll bereitgestellt wird.
PowerProtect DD-Remotesystem	Erstellen Sie eine Storage-Einheit auf dem PowerProtect DD-System.
Remotesitzung	Eine Remote-Snapshot-Sitzung, die den Status und Fortschritt eines Vorgangs auf einem PowerProtect DD-Remotesystem widerspiegelt. Der Sitzungstyp kann „Backup“, „Abruf“ oder „Instant Access“ lauten.
Remote-Snapshot	Eine Darstellung der Daten, die auf der PowerProtect DD gesichert werden und per Instant Access abgerufen oder durchsucht werden können.

Voraussetzungen und Einschränkungen

Berücksichtigen Sie bei der Verwendung von Remotebackups die folgenden Begrenzungen:

- Pro Ressource (Volume oder Volume-Gruppe) kann nur eine Remotebackupsitzung erstellt werden.
- Pro Remote-Snapshot kann nur eine Abruf- oder Instant-Access-Sitzung erstellt werden.
- Pro Node können bis zu zwei Instant-Access-Sitzungen erstellt werden.

- Remotebackup- und -Abrufsitzungen sowie Instant Access-Sitzungen schließen sich gegenseitig aus: Wenn eine Instant Access-Sitzung aktiv ist, können Remotebackup- und -Abrufsitzungen nicht ausgeführt werden, und wenn Remotebackup- und Abrufsitzungen aktiv sind, können Instant Access-Sitzungen nicht ausgeführt werden.
- Wenn ein unterbrechungsfreies Upgrade oder eine Neukonfiguration des Netzwerks durchgeführt wird, können keine Remotebackup-, Abruf- und Instant-Access-Sitzungen ausgeführt werden.
- Eine Instant-Access-Sitzung kann für eine Volume-Gruppe erstellt werden, die bis zu vier Volumes umfassen.
- Für eine optimale Systemleistung wird empfohlen, dass bis zu 125 Volumes auf PowerProtect DD pro Appliance gesichert werden.
- Für eine optimale Systemleistung wird empfohlen, bis zu 125 Remotebackupsitzungen pro Appliance zu erstellen.
- Die Unterstützung für DDVE in der Cloud ist nur bei AWS-Cloud-Anbietern verfügbar.
- Die Deduplizierung ist auf der Client-Seite deaktiviert, auf der PowerProtect Appliance-Seite jedoch aktiviert.
- HA wird für Instant Access nicht unterstützt. Instant Access schlägt fehl, wenn ein Cluster neu gestartet oder ein Failover durchgeführt wird. Weitere Informationen finden Sie im Dell Wissensdatenbank-Artikel 000208509 (Instant Access-Sitzungen zeigen nach dem Neustart des Node den Status „Failed“ an).

Dokumentationsressourcen

Weitere Informationen finden Sie in den folgenden Ressourcen:

Tabelle 3. Dokumentationsressourcen

Dokument	Beschreibung	Position
PowerProtect Data Manager – Administrator- und Benutzerhandbuch	Dieses Dokument stellt Konfigurationsinformationen für PowerProtect Data Manager bereit.	https://www.dell.com/support/home/en-us/product-support/product/enterprise-copy-data-management/docs
Dell PowerProtect Data Manager: Data Protection für Dell PowerStore Storage-Arrays	Dieses Dokument konzentriert sich auf das Backup und die Recovery von Block-Volume-Daten auf PowerStore Storage-Arrays mithilfe von PowerProtect Data Manager.	https://infohub.delltechnologies.com/t/dell-powerprotect-data-manager-data-protection-for-dell-powerstore-storage-arrays/
PowerStore-Onlinehilfe	Die Onlinehilfe enthält kontextsensitive Informationen für die in PowerStore Manager geöffnete Seite.	In PowerStore Manager integriert

Grundlegender Workflow für Remotebackups

Das Sichern von Ressourcen auf einer PowerProtect DD ist die grundlegende Aktion, die Sie durchführen können. Wenn Backups auf einer PowerProtect DD erstellt werden, können Sie sie durchsuchen und abrufen. Jede Remotebackupaktion ist mit einer Remotebackupsitzung verknüpft, mit der Sie den Fortschritt dieser Aktion nachverfolgen können.

Info über diese Aufgabe

Führen Sie die folgenden Schritte zum Erstellen einer Remotebackupsitzung aus:

Schritte

1. Hinzufügen einer Remotesystemverbindung für Remotebackups.
2. Erstellen einer Remotebackupregel.
3. Erstellen einer Datensicherheits-Policy– Einer Schutz-Policy kann nur eine Remotebackupregel hinzugefügt werden.
4. Zuweisen einer Datensicherheits-Policy– Weisen Sie einem Volume oder einer Volume-Gruppe eine Policy zu, die eine Remotebackupregel enthält.
   Eine Remotebackupsitzung wird erstellt und auf der Registerkarte **Backupsitzungen** der Seite **Remotebackup** angezeigt.

Sitzungsstatus

Remotebackup-, Abruf- und Instant-Access-Sitzungen durchlaufen verschiedene Status, die den Fortschritt der Sitzungen und mögliche Probleme anzeigen.

Die folgenden Status sind möglich:

- **Initialisieren** – Die Sitzung wird erstellt. Nach Abschluss der Erstellung ändert sich der Status in „Leerlauf“.
- **Leerlauf** – Es werden keine Daten an die Remote-Appliance übertragen. Die Sitzung verbleibt im Leerlauf-Status, bis die geplante Remotebackupregel ausgelöst wird oder wenn Sie ein manuelles Backup initiieren.
- **Vorbereiten** – Das PowerStore-System bereitet die Durchführung eines Backups vor. Wenn mehrere aktive Sitzungen vorhanden sind, verbleibt die Sitzung möglicherweise im Status „Vorbereiten“, bis sie den Anfang der Warteschlange erreicht.
- **IO-Weiterleitung** (gilt nur für Instant-Access-Sitzungen): Die Sitzung führt die Weiterleitung der Host-I/O-Daten durch.
- **In Bearbeitung** – Das System erstellt das Backup auf dem Remotesystem. Während dieses Status können Sie auf den Statuslink klicken, um den Backupfortschritt zu überwachen und weitere Details anzuzeigen.
- **Abgeschlossen** (gilt nur für für Abrufsitzungen): Die Sitzung wurde erfolgreich abgeschlossen.
- **System angehalten** – Die Sitzung wird durch ein unterbrechungsfreies Upgrade oder eine unterbrechungsfreie Migration angehalten.
- **Angehalten** – Die Sitzung wird angehalten.
- **Abbrechen** – Die Sitzung wird abgebrochen.
- **Abgebrochen** – Die Sitzung wurde explizit abgebrochen. Sitzungen in den Status „Vorbereiten“, „In Bearbeitung“ und „Angehalten“ können abgebrochen werden.
- **Löschen** – Die Sitzung wird gelöscht.
- **Fehlgeschlagen** – Die Sitzung konnte das Backup nicht erstellen.
- **Rollback in Bearbeitung**: Es ist ein Fehler aufgetreten, während die Sitzung aktiv war, und die Änderungen werden zurückgesetzt.
- **Fehlgeschlagen –Bereinigung erforderlich** – Ein Fehler ist aufgetreten, während Änderungen zurückgesetzt wurden (als Ergebnis eines vorherigen Fehlers). Der regelmäßig ausgeführte Bereinigungsservice löst das Problem automatisch und der Sitzungsstatus wird in „Fehlgeschlagen“ geändert. Bei Remotebackupsitzungen können geplante Backups nicht ausgeführt werden, während sich die Sitzung in diesem Status befindet.
- **Abgebrochen – Bereinigung erforderlich** – Während des Sitzungsabbruchvorgangs ist ein Fehler aufgetreten. Der Bereinigungsservice, der regelmäßig ausgeführt wird, löst das Problem automatisch und der Sitzungsstatus wird in „Abgebrochen“ geändert. Bei Remotebackupsitzungen können geplante Backups nicht ausgeführt werden, während sich die Sitzung in diesem Status befindet.
- **Bereinigung erforderlich** – Die Sitzung wurde erfolgreich abgeschlossen, aber während der lokalen Bereinigungsphase ist ein Fehler aufgetreten. Der Bereinigungsservice, der regelmäßig ausgeführt wird, löst das Problem automatisch und der Sitzungsstatus wird in „Leerlauf“ oder „Abgeschlossen“ geändert. Bei Remotebackupsitzungen können geplante Backups nicht ausgeführt werden, während sich die Sitzung in diesem Status befindet.
- **Bereinigung wird durchgeführt** – Es wird eine Bereinigung wird durchgeführt.

Managen von Remotebackupsitzungen

Wenn Sie einem Volume oder einer Volume-Gruppe eine Schutz-Policy zuweisen, die eine Remotebackupregel enthält, wird eine Remotebackupsitzung erstellt und auf der Registerkarte **Backupsitzungen** der Seite **Remotebackup** angezeigt.

Auf der Registerkarte **Backupsitzungen** können Sie die folgenden Aktionen für eine Remotebackupsitzung durchführen:

- **Backup**: Sie können ein manuelles On-Demand-Backup durchführen, wenn die Sitzung inaktiv ist, zum Beispiel wenn die Ressource über einen längeren Zeitraum nicht gesichert wurde.

  ANMERKUNG: Ein manuell erstelltes Backup unterliegt der Aufbewahrungs-Policy, die in der Remotebackupregel festgelegt ist.
- **Pause**: Das Anhalten einer Sitzung im inaktiven Status führt dazu, dass die Sitzung sofort angehalten wird. Wenn Sie eine Sitzung anhalten, die sich im Status „In Bearbeitung“ befindet, wird die Sitzung erst angehalten, nachdem das aktuell ausgeführte Backup abgeschlossen ist. Nachfolgende Backups werden nicht durchgeführt, während die Sitzung angehalten ist.
- **Resume**: Verwenden Sie diese Option, um eine angehaltene Backupsitzung fortzusetzen. Das nächste Backup erfolgt gemäß dem festgelegten Zeitplan.
- **Delete**: Sie können diese Option nur verwenden, um eine Sitzung für eine Ressource zu löschen, die durch eine externe Policy geschützt ist. Für Ressourcen, die durch die PowerStore-Policy geschützt sind, können Sie die zugehörige Remotebackupsitzung löschen, indem Sie die Zuweisung der Policy zur Ressource aufheben oder die Remotebackupregel aus der zugewiesenen Policy entfernen.
- **Cancel**: Sie können diese Option nur zum Abbrechen einer Backupsitzung im Status „In Bearbeitung“ verwenden. Das Abbrechen einer Sitzung führt dazu, dass das aktuelle Backup abgebrochen und kopierte Daten verworfen werden.

  ANMERKUNG: Wenn sich die Sitzung im Status „Prepare“ befindet, werden möglicherweise andere Sitzungen in die Warteschlange eingereiht. Wenn Sie auf **Cancel** klicken, ändert sich der Sitzungsstatus in **Canceling**, aber die Sitzung wird nur abgebrochen, wenn sie den Anfang der Warteschlange erreicht und aktiv wird (Status „In Bearbeitung“).

Ressourcen

Auf der Registerkarte „Ressourcen“ werden alle Volumes und Volume-Gruppen angezeigt, denen Remote-Snapshots zugeordnet sind.

Eine Ressource wird der Tabelle **Ressourcen** hinzugefügt, nachdem eine für die Ressource erstellte Remotebackupsitzung die Erstellung eines Remote-Snapshot ausgelöst hat.

Wenn ein Volume oder eine Volume-Gruppe mit zugehörigen Remote-Snapshots aus PowerStore gelöscht wird, sind die Remote-Snapshots nicht betroffen. Die gelöschte Ressource bleibt in der Tabelle „Ressourcen“ aufgeführt, bis alle zugehörigen Remote-Snapshots abgelaufen sind. Um zu sehen, ob eine Ressource gelöscht ist, fügen Sie mit der Option **Show/Hide Table Columns** die Spalte **Quelle gelöscht** zur Tabelle „Ressourcen“ hinzu.

Auf der Registerkarte **Ressourcen** können Sie folgende Aktionen ausführen:

- Snapshots managen: Wenn Sie eine Ressource aus der Liste auswählen und auf **Snapshots managen** klicken, werden alle Remote-Snapshots angezeigt, die für diese Ressource erstellt wurden:
  - Die Ablaufzeit von automatisch und manuell erstellten Snapshots basiert auf der Aufbewahrungszeit, die in der Remotebackupregel konfiguriert wurde.
  - Die Ablaufzeit eines Remote-Snapshot kann nicht geändert werden. Das Ändern der Aufbewahrungsfrist in einer Remotebackupregel hat keine Auswirkungen auf vorhandene Snapshots.
  - Für automatisch generierte Snapshots enthält ein Remote-Snapshot-Name den Namen der Remotebackupregel, die sie erstellt hat.
  - Wenn Sie einen Snapshot aus der Liste auswählen und auf **Retrieve** klicken, wird eine Abrufsitzung für diesen Snapshot erstellt. Einzelheiten hierzu finden Sie unter Abrufen eines Remote-Snapshots im selben PowerStore-Cluster.
  - Wenn Sie einen oder mehrere Snapshots auswählen und auf **Löschen** klicken, werden die Snapshots gelöscht.

  ANMERKUNG: Sie können auch die Remote-Snapshots für eine Ressource anzeigen und zugehörige Aktionen durchführen, indem Sie auf die Ressource klicken und dann die Registerkarte **Remote-Snapshots** auswählen.
- Instant Access: Wenn Sie eine Ressource aus der Liste auswählen und auf **Instant Access** klicken, wird der Prozess für die Aktivierung des sofortigen Zugriffs für den ausgewählten Remote-Snapshot initiiert. Details finden Sie unter Erstellen einer Instant-Access-Sitzung.
- Remote-Snapshots erkennen: Verwenden Sie diese Option, wenn Sie einen Remote-Snapshot einer Ressource auf einem anderen PowerStore-Cluster abrufen möchten. Details finden Sie unter Abrufen eines Remote-Snapshots in einem anderen Cluster.

Abrufsitzungen

Snapshots von Volumes und Volume-Gruppen, die auf einer PowerProtect DD gesichert werden, können auf demselben oder auf anderen PowerStore-Clustern abgerufen werden.

Möglicherweise möchten Sie einen Remote-Snapshot abrufen, um die Quellressource wiederherzustellen oder einen Thin Clone zu erstellen.

Abrufen eines Remote-Snapshots im selben PowerStore-Cluster:

- Wenn das Quell-Volume oder die Volume-Gruppe des abgerufenen Backups noch im System vorhanden ist, wird ein lokaler Snapshot auf dem PowerStore-Cluster erstellt. Wenn möglich, erfolgt der Abruf inkrementell.
- Wenn das Quell-Volume oder die Volume-Gruppe des abgerufenen Backups nicht mehr im System vorhanden ist, werden sowohl ein neues Volume als auch ein lokaler Snapshot erstellt und das neue Volume wird mit den Snapshot-Daten wiederhergestellt.

Abrufen eines Remote-Snapshots in einem anderen PowerStore-Cluster:

- Da das Quell-Volume nie in diesem Cluster vorhanden war, werden sowohl ein neues Volume als auch ein lokaler Snapshot erstellt. Das neue Volume wird mit den Snapshot-Daten wiederhergestellt.

Für jeden Abrufvorgang wird eine Abrufsitzung erstellt. Der anfängliche Status der Sitzung lautet „Prepare“. Sobald die Sitzung mit dem Kopieren des Snapshots beginnt, ändert sich der Status in „In-Progress“. Nachdem der Snapshot kopiert wurde, ändert sich der Status in „Completed“.

Sie können den Fortschritt der abgerufenen Sitzungen auf der Registerkarte **Sitzungen abrufen** (**Protection** > **Remotebackup**) anzeigen und überwachen. Sie können auch die folgenden Aktionen ausführen:

- Delete: Verwenden Sie diese Option, um eine Abrufsitzung mit dem Status **Completed** zu löschen.
- Cancel: Verwenden Sie diese Option, um eine Abrufsitzung mit dem Status **In Bearbeitung** abzubrechen.

  ANMERKUNG: Wenn der Sitzungsstatus **In Bearbeitung** ist, werden möglicherweise andere Sitzungen in die Warteschlange eingereiht. Wenn Sie auf **Cancel** klicken, ändert sich der Sitzungsstatus in **Canceling**, aber die Sitzung wird nur abgebrochen, wenn sie den Anfang der Warteschlange erreicht und aktiv wird.

Nachdem ein Backup abgerufen wurde, funktioniert es als lokaler Snapshot. Sie können ein abgerufenes Backup verwenden, um ein primäres Volume wiederherzustellen oder einen Clone zu erstellen. Der abgerufene Snapshot ist auf „No Automatic Deletion“ gesetzt. Sie können diese Einstellung ändern, indem Sie eine Aufbewahrungsfrist konfigurieren. Sie können ihn auch in einen sicheren Snapshot ändern.

Abrufen eines Remote-Snapshots im selben PowerStore-Cluster

Info über diese Aufgabe

Möglicherweise möchten Sie einen Remote-Snapshot auf demselben PowerStore-Cluster abrufen, auf dem sich die Quellressource befindet, wenn Sie die übergeordnete Ressource wiederherstellen oder einen Thin Clone erstellen müssen. Sie können einen Remote-Snapshot einer Ressource abrufen, unabhängig davon, ob sie noch vorhanden ist oder gelöscht wurde.

Schritte

1. Klicken Sie auf **Protection** > **Remote Backup** und wählen Sie die Registerkarte **Ressourcen** aus.

   Auf der Registerkarte **Ressourcen** werden alle Ressourcen (Volumes und Volume-Gruppen) angezeigt, denen Remote-Snapshots zugeordnet sind.
2. Klicken Sie in der Liste „Ressourcen“ auf das Kontrollkästchen neben der Ressource und wählen Sie **Snapshots managen** aus, um alle für diese Ressource erstellten Backups anzuzeigen.
3. Wählen Sie im Bereich **Snapshots managen** den Snapshot aus, den Sie abrufen möchten, und klicken Sie auf **Retrieve**.
4. Klicken Sie in der Bestätigungsmeldung auf **Retrieve**.
   Eine Abrufsitzung wird für den Snapshot erstellt und der Tabelle „Sitzungen abrufen“ hinzugefügt. Wenn die Quellressource auf dem Cluster vorhanden ist, wird ein lokaler Snapshot unter der Quellressource erstellt und das abgerufene Backup wird darauf kopiert. Der Abruf kann eine vollständige Kopie sein oder nur die Unterschiede zwischen dem Backup und der Ressource enthalten (inkrementelle Kopie), je nach letztem Backup. Wenn die Quellressource nicht mehr auf dem Cluster vorhanden ist, wird ein neues Volume oder eine neue Volume-Gruppe auf dem PowerStore-Cluster sowie ein lokaler Snapshot erstellt, in den der Remote-Snapshot kopiert wird.

   Sie können den Fortschritt der Abrufsitzung in **Protection** > **Remotebackup** > **Sitzungen abrufen** überwachen.

Abrufen eines Remote-Snapshots in einem anderen Cluster

Info über diese Aufgabe

Wenn Sie einen Remote-Snapshot in einem anderen PowerStore-Cluster als dem Cluster mit der Quellressource abrufen, werden ein neues Volume oder eine neue Volume-Gruppe auf dem PowerStore-Cluster und ein lokaler Snapshot erstellt, auf den der Remote-Snapshot kopiert wird.

Schritte

1. Klicken Sie auf **Protection** > **Remotebackup** und wählen Sie die Registerkarte **Ressourcen** aus.
2. Klicken Sie auf **Remote-Snapshots erkennen**.
3. Legen Sie im Bereich **Remote-Snapshots erkennen** Folgendes fest:
   - PowerProtect DD-Remotesystem: Wählen Sie die PowerProtect DD aus, von der Sie das Backup abrufen möchten.
   - PowerStore Global ID: Geben Sie die globale eindeutige Kennung für das PowerStore-Cluster an, von dem das Backup initiiert wurde. Sie können die globale ID des Clusters unter **Settings** > **Cluster** > **Properties** anzeigen.
   - From: Geben Sie das Startdatum und die Startzeit für die Suche nach Remote-Snapshots an.
   - To: Geben Sie das Enddatum und die Endzeit für die Suche nach Remote-Snapshots an.
4. Klicken Sie auf **Next**.
5. Wählen Sie aus der Liste der ermittelten Snapshots den Snapshot aus, den Sie abrufen möchten, und klicken Sie auf **Next**.

   ANMERKUNG: Sie können nur Snapshots auswählen, die von einem PowerStore-Cluster erstellt wurden.
6. Überprüfen Sie die zusammengefassten Informationen und klicken Sie auf **Retrieve**.

Ergebnisse

PowerStore erstellt eine Abrufsitzung, die auf der Registerkarte **Sitzungen abrufen** angezeigt werden kann. Wenn die Sitzung abgeschlossen ist, werden der abgerufene Snapshot und ein neues Volume auf dem lokalen Cluster erstellt.

Abrufen – zusätzliche Überlegungen

- Wenn die ursprüngliche Quelle eines Backup-Snapshots, der aus der DD abgerufen wird, nicht mehr vorhanden ist (verwaister Snapshot), werden Blöcke auf dem neu erstellten Volume, das bei der Sicherung des ursprünglichen Volumes nicht beschrieben wurden, zugewiesen und mit Nullen geschrieben. Daher sind die physischen und logischen Kapazitäten identisch (wenn sie die abgerufenen Backupkapazitätsdaten betrachten). Wenn das neue Volume einem Host zugeordnet ist, werden der verwendete und der freie Speicherplatz richtig angezeigt. Weitere Informationen finden Sie im Dell Wissensdatenbank-Artikel 000208504 (Nachdem PowerStore aus Data Domain abgerufen wurde...).
- Wenn ein Quell-Volume oder eine Volume-Gruppe nicht mehr auf dem PowerStore-Cluster vorhanden ist, führt das Abrufen des entsprechenden Backups immer dazu, dass eine neue Quelle zusammen mit dem abgerufenen Snapshot erstellt wird.
- Wenn die Größe des abgerufenen Snapshots nicht mit der Größe des Quell-Volumes übereinstimmt, ist der Abruf vollständig (der gesamte Snapshot wird von PowerProtect nach PowerStorekopiert.
- Der inkrementelle Abruf (nur das Abrufen der Änderungen, die seit dem Backup aufgetreten sind) erfolgt, wenn die folgenden Bedingungen erfüllt sind:
  - Die Größe des Quell-Volumes hat sich seit dem Backup nicht geändert.
  - Sowohl das Quell-Volume als auch das neueste Remotebackup sind auf dem PowerStore-Cluster vorhanden.
- Die durchschnittliche Übertragungsrate für einen inkrementellen Abruf ist möglicherweise nicht immer genau, obwohl der Prozentsatz des Abruffortschritts die Menge der abgerufenen Daten genau widerspiegelt.

Instant-Access-Sitzungen

Mit Instant Access können Sie auf Remote-Snapshots auf einer PowerProtect DD zugreifen, ohne sie auf dem PowerStore-Cluster abrufen zu müssen.

- Verwenden Sie die Instant-Access-Option, um einen Remote-Snapshot zu durchsuchen, bevor Sie entscheiden, ob Sie ihn abrufen, oder um auf einen Snapshot einer gelöschten, beschädigten oder geänderten Ressource zuzugreifen und in den Host zu kopieren.
- Pro Remote-Snapshot ist nur eine Instant-Access-Sitzung zulässig.
- Eine Instant-Access-Sitzung kann für Volume-Gruppen erstellt werden, die bis zu vier Mitglieder umfassen.
- Wenn eine Instant-Access-Sitzung ausgeführt wird, führt das PowerStore-Cluster keine Backup- und Abrufvorgänge durch und lokale Ressourcen werden nicht geschützt.
- Der sofortige Zugriff schlägt fehl, wenn ein Cluster neu gestartet wird oder ein Failover durchgeführt wird. Um den sofortigen Zugriff in diesem Fall erneut zu starten, heben Sie die Zuweisung des Volumes mit direktem Zugriff zum Host auf, löschen Sie die Sitzung und erstellen Sie die Sitzung erneut.
- Das System legt die Node-Affinität zu Instant-Access-Sitzungen bei der Erstellung fest. Wenn der Host nicht auf den Node zugreifen kann, zu dem die Instant-Access-Sitzung eine Affinität hat, führt die Instant-Access-Sitzung kein Failover auf den anderen Node durch und der Host hat Probleme beim Zugriff auf die Instant-Access-Ressourcendaten.

Die folgenden Informationen werden auf der Registerkarte **Instant-Access-Sitzungen** bereitgestellt:

- Status: Der Sitzungsstatus lautet I/O-Weiterleitung.
- Lokale Ressource: Zeigt das neue Volume oder die neue Volume-Gruppe an, die im Rahmen der Sitzung erstellt wird. Durch Klicken auf den Hyperlink „Lokale Ressource“ wird die Seite „Details“ für diese Ressource geöffnet, auf der Sie die Volume-Details oder Mitglieder der Volume-Gruppe anzeigen können. Sie können auch Performancedaten anzeigen, ausgegebene Warnmeldungen überprüfen und Hosts der Ressource zuordnen oder deren Zuordnung aufheben.

Auf der Registerkarte „Instant-Access-Sitzungen“ können Sie eine Instant-Access-Sitzung beenden. Um die Sitzung zu beenden, müssen Sie zunächst alle Hostzuordnungen zur lokalen Ressource entfernen.

Die Volumes und Volume-Gruppen, die bei Instant-Access-Sitzungen erstellt werden, werden auch unter **Storage** > **Volumes** > **Instant Access** und **Storage** > **Volume Groups** > **Instant Access** angezeigt.

Erstellen einer Instant-Access-Sitzung

Mit Instant Access können Sie Zugriff auf Remote-Snapshots auf der PowerProtect DD erhalten, ohne sie auf dem PowerStore-Cluster abrufen zu müssen.

Schritte

1. Wählen Sie **Protection** > **Remotebackup** > **Resources** aus.
2. Aktivieren Sie in der Ressourcenliste das Kontrollkästchen neben der Ressource und klicken Sie auf **Instant Access**.
   Im Bereich **Instant Access aktivieren** werden alle verfügbaren Remote-Snapshots für die ausgewählte Ressource angezeigt.

3. Wählen Sie den Snapshot aus, auf den Sie zugreifen möchten.

   ANMERKUNG: Sie können auch die Ressource auswählen und dann **Remote-Snapshots** > **remote snapshot** > **Enable Instant Acess** auswählen.

4. Optional können Sie Hosts dem Volume zuordnen, das erstellt wird, wenn die Instant-Access-Sitzung initiiert wird. Klicken Sie auf **Map Hosts**, wählen Sie die zuzuordnenden Hosts aus und klicken Sie auf **Apply**.
   Die zugeordneten Hosts werden im Abschnitt „Hostverbindung“ aufgeführt.

   ANMERKUNG: Diese Option ist nur für Volumes und nicht für Volume-Gruppen vorhanden. Das Zuordnen von Hosts zu Mitgliedern einer Volume-Gruppe ist erst möglich, nachdem Sie die Instant-Access-Sitzung erstellt haben (siehe Details unten).

5. Klicken Sie auf **Aktivieren**.
   Eine Instant-Access-Sitzung wird erstellt und der Registerkarte **Instant-Access-Sitzungen** hinzugefügt. Ein lokales zugeordnetes Volume oder eine Volume-Gruppe wird für die Sitzung erstellt und kann auf der Registerkarte **Instant Accesser Zugriff** im Fenster **Volumes** oder **Volume Groups** angezeigt werden.

   ANMERKUNG: Die Registerkarte **Instant Access** wird nur angezeigt, wenn PowerProtect DD als Remotesystem hinzugefügt wird.

   Die erstellte Ressource ist les- und beschreibbar. Daten werden vorübergehend auf die PowerProtect DD Appliance geschrieben, während der Remote-Snapshot unverändert bleibt. Wenn die Sitzung gelöscht wird, gehen alle Schreibvorgänge verloren.

Ergebnisse

Nachdem Sie einen sofortigen Zugriff für eine Volume-Gruppe erstellt haben, können Sie Hosts Mitgliedern der Volume-Gruppe zuordnen, die für die Sitzung erstellt wurde:

1. Wählen Sie **Protection** > **Remotebackup** > **Instant-Access-Sitzungen** aus.
2. Klicken Sie auf den Link für die Volume-Gruppe in der Spalte **Lokale Ressource**, um ihre Mitglieder anzuzeigen.
3. Wählen Sie die Mitglieder aus, die Sie zuordnen möchten, und klicken Sie auf **Map**, um den Bereich **Map Hosts** zu öffnen.

Instant Access – zusätzliche Hinweise

- Instant Access wird für alle Blockressourcen mit Ausnahme von VMware vStorage VMFS-Datenspeichern unterstützt. Wenn Sie auf Daten in einem Remote-Snapshot zugreifen müssen, rufen Sie den Remote-Snapshot ab und erstellen und mounten Sie dann einen Thin Clone.
- HA wird für Instant Access nicht unterstützt. Weitere Informationen finden Sie unter Hochverfügbarkeit und im Dell Wissensdatenbank-Artikel 000208509 (Instant Access-Sitzungen zeigen nach dem Neustart des Nodes den Status „Fehlgeschlagen“ an).
- Instant Access wird für DDVE in der Cloud nicht unterstützt.

Hohe Verfügbarkeit

Hohe Verfügbarkeit wird für Remotebackupsitzungen und Abrufsitzungen unterstützt (aber nicht sichergestellt), für Instant-Access-Sitzungen hingegen nicht:

- Wenn ein Node ausgefallen ist oder ein Node neu gestartet wird:
  - Backup- und Abrufsitzungen führen ein Failover auf den Peer-Node aus und werden dort weiter fortgesetzt.
  - Instant-Access-Sitzungen sind Node-spezifisch. Wenn der Node, auf dem die Sitzung ausgeführt wird, nicht erreichbar oder inaktiv ist, wechselt die Sitzung in den Status „Fehlgeschlagen“. Heben Sie die Zuweisung des Volumes zum Host auf, löschen Sie die Sitzung und erstellen Sie die Sitzung dann erneut.
- Wenn eine Appliance ausgeschaltet oder neu gestartet wird:
  - Alle Backup- und Abrufsitzungen werden fortgesetzt, wenn die Appliance wieder aktiv ist.
  - Instant-Access-Sitzungen werden in den Status „Fehlgeschlagen“ verschoben. Heben Sie die Zuweisung des Volumes zum Host auf, löschen Sie die Sitzung und erstellen Sie die Sitzung dann erneut.

Remotebackupwarnungen

Auf der Registerkarte **Warnungen** (befindet sich unter **Überwachung**) werden allgemeine Warnmeldungen angezeigt, die für Remotebackupsitzungen erzeugt werden, z. B. Sitzungserstellung und -abschluss, Hinzufügen oder Entfernen eines Remotesystems usw. Sie können Remotebackupwarnungen filtern, indem Sie **Remotesitzung** und **Remotesystem** als Ressourcentyp auswählen.

Warnmeldungen werden auch ausgegeben, wenn Ausfälle auftreten. Die Anzahl der Warnmeldungen wird auf den Registerkarten **Backupsitzungen** und **Abrufsitzungen** angezeigt. Wenn Sie auf die Zahl klicken, wird das Fenster **Warnmeldungen** geöffnet.

A

Anwendungsbeispiele

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Anwendungsbeispiele für Snapshots und Thin Clones

Sie können Snapshots und Thin Clones verwenden, um beschädigte Volumes wiederherzustellen und Testumgebungen zu erstellen.

Snapshots sind schreibgeschützte Kopien, die verwendet werden können, um den aktuellen Status eines Objekts zu speichern. Sie können Snapshots verwenden, um Daten schnell wiederherzustellen, wenn sie durch Beschädigungen oder Nutzerfehler verloren gegangen sind. Auf Snapshots können Hosts nicht direkt zugreifen.

Thin Clones sind beschreibbare Kopien eines Snapshot, eines Volume oder einer Volume-Gruppe, auf die Hosts zugreifen können. Thin Clones können als Kopie des übergeordneten Objekts direkt oder mithilfe eines Snapshot erstellt werden. Snapshots und Thin Clones sind platzsparende Kopien, die gemeinsame Datenblöcke mit dem übergeordneten Objekt haben.

Verwenden von Snapshots und Thin Clones für die partielle Recovery eines Volume

Sie können Snapshots und Thin Clones verwenden, um einen Teil eines Volume, z. B. einzelne Dateien oder Datenbank-Datensätze, auf den Stand eines bestimmten Zeitpunkts zurücksetzen. Erstellen Sie zunächst einen Thin Clone aus dem Snapshot, der die wiederherzustellenden Daten enthält. Ermöglichen Sie dann den Hostzugriff auf den Clone und stellen Sie die Daten vom Host wieder her.

Verwenden von Snapshots zum Wiederherstellen eines Volume oder einer Volume-Gruppe

Sie können Snapshots verwenden, um ein Volume auf einen vorherigen Zeitpunkt zurückzusetzen, wenn eine Beschädigung vorliegt. Um ein Volume oder eine Volume-Gruppe auf einen vorherigen Zeitpunkt zurückzusetzen, können Sie den Volume-Wiederherstellungsvorgang nutzen und dabei einen Snapshot von einem Zeitpunkt vor der Beschädigung verwenden. Der Wiederherstellungsvorgang wird sofort ausgeführt. Sie können auch einen Backup-Snapshot erstellen, um den Zustand des Volume oder der Volume-Gruppe vor dem Wiederherstellungsvorgang zu speichern.

Verwenden von Thin Clones zum Testen eines Patch vor der Anwendung auf das Produktions-Volume

Bevor Sie einen Patch oder ein Softwareupdate einer kritischen Anwendung auf einem Volume installieren, können Sie einen Thin Clone des Volume erstellen und das Update zunächst auf diesen Thin Clone anwenden. Nachdem Sie das Update installiert haben und geprüft haben, dass es sich reibungslos in Ihrer Umgebung installieren lässt, können Sie es auf den anderen Volumes installieren.

Erstellen von Thin Clones für die Entwicklungsnutzung

Statt Volumes oder Volume-Gruppen für jeden Entwickler einzeln bereitzustellen, können Sie Thin Clones erstellen. Durch Erstellen von Thin Clones des Volume oder der Volume-Gruppe können Sie jedem Entwickler die gleichen Daten und die gleiche Konfiguration zur

Verfügung stellen. Die Thin Clones benötigen auch weniger Speicherplatz, als wenn Sie einen vollständigen Clone des Volume erstellen oder einzelne Volumes oder Volume-Gruppen bereitstellen. Sie können auch Snapshots von Thin Clones erstellen und diese replizieren.

Anwendungsbeispiele für die Replikation

Sie können eine Replikation bei geplanten Ausfallzeiten, z. B. während der Migration zwischen Clustern oder der Installation eines wichtigen Softwareupdates, und für die Disaster Recovery verwenden.

Migration zwischen Clustern

Wenn Sie ein Speicherobjekt zu einem anderen PowerStore-Cluster migrieren möchten, können Sie eine einmalige Replikation zwischen den beiden Clustern einrichten, gefolgt von einem geplanten Failover zum neuen Cluster. Nach der Migration entfernen Sie das Quellobjekt, um Speicherplatz im ursprünglichen Cluster zurückzugewinnen.

Verwenden der Replikation für geplante Ausfallzeiten

Geplante Ausfallzeiten sind Situationen, in denen Sie das Quellsystem für eine Wartung oder für Tests offline setzen, während Sie vom Zielsystem aus arbeiten. Vor der geplanten Ausfallzeit wird eine aktive Replikationssitzung für Quelle und Ziel ausgeführt. Es gibt keinen Datenverlust bei geplanten Ausfallzeiten.

In diesem Szenario wird das Quellsystem Boston für die Wartung offline genommen und das Zielsystem New York wird während des Wartungszeitraums als Produktionssystem verwendet. Kehren Sie nach der Wartung von der Produktion zum System Boston zurück.

Wählen Sie zum Starten geplanter Ausfallzeiten die Option **Planned Failover** auf dem Quellsystem Boston aus. Das Zielsystem New York ist vollständig mit der Quelle synchronisiert, um sicherzustellen, dass keine Daten verloren gehen. Die Sitzung bleibt angehalten, während das Quellsystem Boston schreibgeschützt wird und das Ziel Lese-/Schreibzugriff erhält. Die Zielspeicherressource New York kann Zugriff auf den Host bereitstellen. Wählen Sie auf der Zielspeicherressource New York die Option **Reprotect** aus, um die Replikation in umgekehrter Richtung wiederaufzunehmen.

Um die Vorgänge auf dem System Boston nach der Wartung wieder aufzunehmen, wählen Sie auf dem System New York **Planned Failover** aus. Wählen Sie nach Abschluss des Failover auf dem System Boston die Option **Reprotect** aus.

ANMERKUNG: Um mit „Reprotect“ Daten vom Ziel auf die Quelle zu replizieren, stellen Sie sicher, dass auf dem Zielsystem eine Replikations-Policy mit einer Replikationsregel vorhanden ist, die auf das Quellsystem verweist. Beispiel: Wenn die reguläre Replikationssitzung von einem Standort in Boston zu einem Standort in New York erfolgt, muss die Replikations-Policy auf der Zielspeicherressource in New York auf Boston verweisen.

Verwenden der Replikation zur Disaster-Recovery

In diesem Disaster-Recovery-Szenario ist das Quellsystem Boston aufgrund eines durch eine Naturkatastrophe oder einen menschlichen Fehler verursachten Notfalls nicht verfügbar. Das Zielsystem New York wurde erstellt und enthält eine vollständige Kopie oder ein Replikat der Produktionsdaten. Der Datenzugriff kann durch ein Failover auf New York wiederhergestellt werden, da eine Replikationssitzung zwischen den Systemen Boston und New York konfiguriert wurde.

Die Verwendung von Replikaten zur Disaster-Recovery minimiert den potenziellen Verlust von Daten. Das Replikat hat gemäß zugehöriger Replikationsregel den Stand der letzten Synchronisation des Ziels mit der Quelle. Der Grad des potenziellen Datenverlusts ist abhängig von der Recovery Point Objective (RPO)-Einstellung in der zugehörigen Replikationsregel. Für die Replikationssitzung kann ein Failover auf das Zielsystem „New York“ durchgeführt werden, indem die neuesten Daten verwendet werden, die von Boston repliziert wurden.

Nach dem Failover der Sitzung auf das System „New York“ wird der Lese-/Schreibzugriff zugewiesen. Bei der ursprünglichen Erstellung einer Replikationssitzung zwischen den Quell- und Zielsystemen erhielt die Storage-Ressource die korrekten Zugriffsberechtigungen für den Host und die Freigabe. Die frühzeitige Erstellung des richtigen Hostzugriffs auf dem Zielsystem verringert die Ausfallzeit in einem Notfall.

So kehren Sie zum System „Boston“ zurück, wenn es wieder verfügbar ist:

1. Wählen Sie im System „New York“ die Option **Reprotect** aus, wodurch die Replikationssitzung in umgekehrter Richtung fortgesetzt wird.
2. Nachdem die Systeme synchronisiert wurden, wählen Sie die Option **Planned Failover** auf dem System „New York“ aus.
3. Aktivieren Sie das Kontrollkästchen, um das System nach dem Failover automatisch zu schützen. Oder wählen Sie nach Abschluss des Failovers auf dem Quellsystem die Option **Reprotect** aus.

ANMERKUNG: Um mit „Reprotect“ Daten vom Ziel auf die Quelle zu replizieren, stellen Sie sicher, dass auf dem Zielsystem eine Replikations-Policy mit einer Replikationsregel vorhanden ist, die auf das Quellsystem verweist. Beispiel: Wenn die Replikationssitzung von einem Standort in Boston zu einem Standort in New York erfolgt, muss die Replikations-Policy auf der Zielspeicherressource in New York auf Boston verweisen.

Anwendungsbeispiele für Metro-Schutz

Verwenden Sie Metro-Schutz, um hohe Datenverfügbarkeit, Lastenausgleich und Migration sicherzustellen.

Verwenden von Metro für hohe Verfügbarkeit

Ein Metro-Volume wird mithilfe von zwei unterschiedlichen Storage-Arrays bereitgestellt, die zusammenarbeiten, um Anwendungshosts ein einzelnes Metro-Volume zur Verfügung zu stellen, indem dasselbe SCSI-Image und dieselben Daten bereitgestellt werden. Die Hosts und Anwendungen, die auf ihnen ausgeführt werden, nehmen zwei physische Volumes als ein einziges Volume mit mehreren Pfaden wahr. Infolgedessen können Hosts auf beide Seiten des Metro-Volumes zugreifen. Wenn ein Linkverlust oder -ausfall eines der Systeme vorliegt, kann der Hostzugriff weiterhin auf das aktive System aufrechterhalten werden.

Metro-Schutz bietet bidirektionale synchrone Replikation, bei der beide Seiten des Metro-Volumes für die Produktion verwendet werden können. Anstelle von Disaster Recovery (durch Failover einer Replikationssitzung auf ein Remotesystem) ermöglicht Metro die Vermeidung von Notfällen, indem eine automatische Synchronisierung zwischen den Systemen ohne Ausfallzeit bereitgestellt wird.

Verwenden von Metro für den Lastenausgleich

Mit PowerStore Metro Volume können die Rechenzentren für die vollständige Nutzung von PowerStore-Systemen über eine Aktiv-Aktiv-Umgebung optimiert werden, die eine Lastverteilung über PowerStore-Systeme hinweg ermöglicht. Das unterbrechungsfreie Verschieben von Anwendungen zwischen PowerStore-Systemen ist einfach und kann durchgeführt werden, wenn ein Kapazitäts- oder Performance-Ausgleich erforderlich ist.

Verwenden von Metro für die Migration

Sie können Metro-Volumes verwenden, wenn Workloads zwischen PowerStore-Systemen migriert werden müssen. Die Verwendung von Metro-Volumes für die Migration ist einfach und nutzerfreundlich und reduziert das Risiko von Datenverlusten. Mit der Metro-Volume-Option ist die Migration unterbrechungsfrei und wenn die Migration abgeschlossen ist, kann das Metro-Volume entweder entfernt oder aufbewahrt werden, um eine extrem schnelle Recovery im Falle eines Systemausfalls oder sogar eines vollständigen Systemausfalls am Standort zu ermöglichen.