Dell PowerStore

Schutz Ihrer Daten

Version 4.4

HINWEIS: Dieser Inhalt wurde möglicherweise mit KI übersetzt. Weitere Informationen finden Sie hier.

März 2026
Rev. A10

DELL Technologies

Hinweise, 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 zu Produkten und Funktionen finden Sie im PowerStore-Infohub.
- **Troubleshooting**: Informationen zu Produkten, Softwareupdates, Lizenzierung und Service finden Sie auf Dell Support auf der entsprechenden Produktsupportseite.
- **Technischer Support**: Für technischen Support und Service-Requests gehen Sie zu Dell Support und rufen die Seite **Service-Requests** auf. Um eine Serviceanfrage stellen zu können, müssen Sie über einen gültigen Supportvertrag verfügen. Wenden Sie sich an Ihren Vertriebsmitarbeiter, wenn Sie einen gültigen Supportvertrag benötigen oder Fragen zu Ihrem Konto haben.

Kundenfeedback

Eine Feedback-Schaltfläche befindet sich auf der rechten Seite des PowerStore Managers. Wenn Sie **Feedback** auswählen, wird ein Browserfenster geöffnet, in dem Sie eine Feedbackumfrage ausfüllen und senden können.

1

Einleitung

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Datensicherheit

PowerStore bietet verschiedene Möglichkeiten zum Schutz Ihrer Daten:

- Lokaler Schutz: Erstellen Sie Snapshots (Point-in-Time-Kopien) von Volumes, Volume-Gruppenvirtuellen Maschinen 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 PowerStore OS 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 Aktivieren des NDMP-Backups.

Snapshots

Snapshots sind schreibgeschützte Point-in-Time-Kopien von Daten eines Volumes,Volume-Gruppe, virtuelle Maschine oder Dateisystem. 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 Storage-Ressourcen zuzuweisen. Das System erstellt automatisch Snapshots der relevanten Ressource gemäß dem in der Schutz-Policy festgelegten Zeitplan.

VonPowerStore3.5 können Sie sichere Snapshots erstellen, die von einem Administrator nicht manuell gelöscht werden können und automatisch gelöscht werden, wenn ihre Ablaufzeit erreicht ist. Sichere Snapshots bieten zusätzlichen Schutz vor Ransomware-Angriffen.

Wenn Daten beschädigt oder versehentlich gelöscht werden, können Sie die Daten aus den Snapshots wiederherstellen oder das Volume oderVolume-GruppeBis zum Zeitpunkt der Erstellung des Snapshots.

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 –PowerStoreHält alle Schreibvorgänge auf demVolume-Gruppe-Mitglieder, um eine einheitliche Point-in-Time-Kopie bereitzustellen und einen konsistenten Schutz auf allen Mitglieds-Volumes zu gewährleisten. Sie können Snapshots mit konsistenter Schreibreihenfolge erzeugen überPowerStore Manager.
- Anwendungskonsistente Snapshots: Sie können anwendungskonsistente Snapshots eines Volumes oder einerVolume-Gruppemit AppSync. 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 ein Snapshot in der Schreibreihenfolge konsistent oder anwendungskonsistent ist, sehen Sie sich die Spalten **Schreibreihenfolge konsistent** und **Anwendungskonsistent** in den Snapshot-Tabellen für ein Volume oderVolume-GruppeinPowerStore Manager.

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

Das Zuordnen von Snapshots zu Hosts wird nicht unterstützt inPowerStore. 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.

Details zu den möglichen Snapshot-bezogenen Vorgängen, die Sie durchführen können, finden Sie unterPowerStore Manager, siehe Kapitel "Snapshots ".

ANMERKUNG: Weitere Informationen zu Snapshot-Limits fürPowerStore*siehe Dell Technologies PowerStore Simple Support Matrix.*

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 und synchrone Remotereplikation für Volumes und Volume-Gruppen, NAS-Server und Virtual Volumes.

ANMERKUNG: Wenn der Replikationscluster über mehrere Appliances verfügt, wird empfohlen, dass die Kapazität der entfernten Appliances so ähnlich wie möglich ist. Erhebliche Schwankungen in der Kapazität von Remote-Appliances können zu einer unausgewogenen Zuweisung von Replikationssitzungen zwischen den Appliances führen, was sich auf die Cluster-Performance auswirken kann. Um eine unausgeglichene Zuweisung von Replikationssitzungen über Remote-Appliances hinweg auszugleichen, wird empfohlen, die Ziel-Volume-Migration durchzuführen.

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.

So konfigurieren Sie die Replikation für NAS-Server:

1. Konfigurieren Sie das Dateimobilitätsnetzwerk und ordnen Sie es zu.
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.

Für die Volume- und Dateireplikation ermöglicht Ihnen die PowerStore Failover-Kontrolle auf das Remotesystem und die Umkehrung der Richtung einer Remoteschutzsitzung. 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.

Detaillierte Informationen zu den Grenzwerten für synchronisierte und nicht synchronisierte Replikation finden Sie in der *Dell Technologies PowerStore Simple Support Matrix* auf der Seite „PowerStore-Dokumentation“.

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 bietet bidirektionale synchrone Replikation (aktiv-aktiv) über zweiPowerStoreSysteme. 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.

Der Metro-Schutz ermöglicht eine höhere Verfügbarkeit und Vermeidung von Notfällen, einen rechenzentrumsübergreifenden Ressourcenausgleich und eine Storage-Migration zwischen zweiPowerStoreSysteme.

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 erfordert zweiPowerStoreund optional einen Witness-Service, der auf einem eigenständigen Host oder einer VM ausgeführt wird.

Wenn Sie eine Metro-Ressource konfigurieren, wird das System, von dem die Metro-Ressource konfiguriert wird, automatisch als bevorzugt und das andere System als nicht bevorzugt konfiguriert. Wenn kein Witness-Service konfiguriert ist oder wenn der Witness-Service nicht verfügbar ist, helfen diese Rollen, das Systemverhalten in Fehlersituationen zu steuern. 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, während das bevorzugte System Hostzugriff gewährt.

Der Witness-Service ist ein passiver Drittanbieter, der auf einem eigenständigen Host installiert ist.

ANMERKUNG: Der Witness-Service muss auf einer dritten Fehlerdomäne bereitgestellt werden, die von den beiden getrennt istPowerStoreSysteme, die Teil der Metro-Sitzung sind. Die Installation des Witness-Service auf einem separaten System stellt seine Verfügbarkeit sicher, wenn auf den Metro-Systemen ein Stromausfall auftritt.

Der Witness beobachtet den Status der beiden Systeme. Wenn ein Fehler auftritt, bestimmt der Witness, welches System für Hosts zugänglich bleibt, und bedient weiterhin I/Os. Ein Witness, der an einem dritten Standort installiert ist, bietet Schutz vor einzelnen Ausfallszenarien.

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).

Eine Zusammenfassung der Metro-Attribute und einen Vergleich mit der synchronen und asynchronen Replikation finden Sie unter Replikationszusammenfassung.

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

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.
- Überwachen Sie den Status der Management- und Datenverbindung zu Troubleshooting-Zwecken.
- Wählen Sie ein Remotesystem und dann **Modify** aus, um seine Attribute zu bearbeiten. Sie können die Management-IP-Adresse und die Beschreibung ändern. Für den TCP-Verbindungstyp können Sie auch die Netzwerklatenz einer Remotesystemverbindung ändern.
- Wählen Sie ein Remotesystem und dann **Löschen** aus, 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-Sitzungen vorhanden sind.
- Wählen Sie ein Remotesystem aus und klicken Sie auf. **Weitere Aktionen** > **Überprüfen 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.
- Wählen Sie für Systeme mit TCP-Verbindungstyp ein Remotesystem aus und klicken Sie auf **Weitere Aktionen** > **Netzwerkgruppe managen** Zum Hinzufügen, Ändern oder Löschen von Netzwerkgruppen.
- 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, wählen Sie **Weitere Aktionen** > **Überprüfen und aktualisieren** Nachdem die Konnektivität wiederhergestellt wurde, ändern Sie den Status des Remotesystems in OK.
  - Wählen Sie ein Remotesystem aus und wählen Sie dann **Weitere Aktionen** > **Kapazitätsdetails anzeigen** Zum Anzeigen der Nutzungs- und historischen Kennzahlen für dieses System über einen ausgewählten Zeitraum.
  - Wenn das Zertifikat eines Remotesystems erneuert wurde, wählen Sie das Remotesystem und dann **Weitere Aktionen** > **Zertifikat aktualisieren** Zum Anzeigen und Bestätigen der Aktualisierung des Zertifikats des Remotesystems.
  - Sie können in den Spalten "Management/File State" und "Data Connection" der Tabelle **Remote Systems** nach Konnektivitätsproblemen suchen.

Überlegungen zu Replikation und Metro

Konfigurieren Sie Remotesystemverbindungen für die Replikation und den Metro-Schutz zwischen zwei Systemen, um sicherzustellen, dass Versionen und Verbindungstypen kompatibel sind.

Replikations- und Metro-Schutz erfordert eine Remotesystemverbindung zwischen zweiPowerStoreSysteme. Sie müssen eine Remotesystemverbindung erstellen, bevor Sie den Remoteschutz konfigurieren. Für die Replikation ist die Remotesystemverbindung

mit der Replikationsregel verknüpft. Wenn SiePowerStoreManager können Sie eine Remotesystemverbindung erstellen, während Sie eine Replikationsregel erstellen. Es ist auch möglich, ein Remotesystem zu erstellen, wenn Sie Metro auf einem Volume oder einer Volume-Gruppe konfigurieren.

Es ist möglich, eine Remoteverbindung zwischen Systemen zu erstellen, auf denen verschiedene Versionen (3.x, 4.x) ausgeführt werden. Die Systemversionen bestimmen die unterstützten Funktionen (Replikationstypen und Remoteschutzfunktionen). Auf beiden Systemen müssen die erforderlichenPowerStoreVersion, damit eine Funktion in dieser Version unterstützt wird. Die folgenden Bedingungen sollten für die Replikation von Storage-Objekten erfüllt sein:

Tabelle 1. Storage-Replikation – Anforderungen

Replication Type	Zulässige Versionen	Connection Type	Netzwerklatenz	Zweck des Storage-Netzwerks (für TCP-Verbindungstyp)
Asynchron – Volume	1.x oder höher	• TCP • FC – Unterstützt für Version 4.2 und höher	-	Replikation
Asynchron – Datei	3.x oder höher	• TCP • FC – Unterstützt für Version 4.3 und höher	-	Replikation
Asynchron – virtuelles Volume	3.x oder höher	TCP	-	Replikation
Metro	3.x oder höher für Volume-Unterstützung, 4.x oder höher für Volume-Gruppenunterstützung	• TCP (siehe Voraussetzungen und Einschränkungen für Metro) • FC – Unterstützt für Version 4.4 und höher	Niedrig (unter 5 ms)	Replikation
Synchron – Volume	4.x oder höher	• TCP • FC – Unterstützt für Version 4.3 und höher	Niedrig (unter 5 ms)	Replikation
Synchron – Datei	4.x oder höher	• TCP • Die synchrone Dateireplikation mit Metro-Replikation (mit automatischem Ausfall, wenn Witness konfiguriert ist) wird für Version 4.3 und höher unterstützt. • FC – Unterstützt für Version 4.4 und höher.	Niedrig (unter 5 ms)	Replikation

- Stellen Sie für den Verbindungstyp TCP sicher, dass die folgenden Bedingungen erfüllt sind:
  - Die Storage-Netzwerke müssen mit dem Replikationszweck konfiguriert werden.
  - Das Netzwerk muss mindestens einem Port zugeordnet sein.
  - Jeder Port muss mit mindestens zwei IP-Adressen bereitgestellt werden.
- Für die Replikation über eine FC-Verbindung (einschließlich Metro) müssen alle FC-Verbindungen FC-Switches verwenden (direkte Verbindungen oder Punkt-zu-Punkt-Verbindungen werden nicht unterstützt).
- Das Ändern des Datenverbindungstyps auf einem Remotesystem wird nicht unterstützt. Um den Datenverbindungstyp zu ändern, löschen Sie das Remotesystem und erstellen Sie ein neues Remotesystem mit dem neuen Datenverbindungstyp.

ANMERKUNG: Nach dem Löschen und erneuten Generieren des Remotesystems werden alle NAS-Daten, die auf das Remotesystem repliziert wurden, ungültig. Infolgedessen werden alle vorhandenen NAS-Daten auf den Remotestandort kopiert. Bei der Blockreplikation werden Daten am Remotestandort wiederverwendet und nur inkrementelle Daten auf das Remotesystem kopiert.

- TCP- und FC-Verbindungstypen können nicht gleichzeitig verwendet werden, um Daten zwischen zwei zu replizierenPowerStoreSysteme. Es ist möglich, Daten mithilfe des TCP-Verbindungstyps von System A auf System B und mithilfe des FC-Verbindungstyps von System A auf System C zu replizieren.

ANMERKUNG: Stellen Sie bei Remotesystemen mit TCP-Verbindungstyp sicher, dass Sie das Storage-Netzwerk mit Replikation als Zweck konfiguriert haben (siehe Remotesystemzweck festlegen) und es mindestens einem Port zugeordnet haben.

Überlegungen zum Remotebackup

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:

- Die Storage-Netzwerke müssen mit dem Replikationszweck konfiguriert werden.
- Das Netzwerk muss mindestens einem Port zugeordnet sein.
- Auf dem PowerStore-System muss Version 3.x oder höher ausgeführt werden.
- Für Informationen zu unterstützten PowerProtect DDOS-Versionen siehe *Dell Technologies PowerStore – einfache Suppportmatrix*.
- Das PowerStore Storage-Netzwerk muss in der Lage sein, mit dem PowerProtect DD-Datenübertragungsnetzwerk zu kommunizieren.
- Der Zweck des Storage-Netzwerks muss auf „Replikation“ festgelegt werden.

Wenn mehrere Storage-Netzwerke mit Replikationszweck vorhanden sind, wählt das System in den folgenden Szenarien ein Storage-Netzwerk mit maximaler Konnektivität zum PowerProtect DD-Remotesystem aus:

- Ein Remotesystem wird hinzugefügt.
- Verifizieren und Aktualisieren des Remotesystems.
- Das Storage-Netzwerk wird auf eine Weise neu konfiguriert, die sich auf das PowerProtect DD-Remotesystem auswirkt.

ANMERKUNG: Für Remotebackups wird empfohlen, ein symmetrisches Storage-Netzwerk zu konfigurieren, das auf allen Appliances des Clusters skaliert ist.

Hinzufügen einer Remotesystemverbindung für die Replikation und Metro

Konfigurieren einer Remotesystemverbindung zwischen Quelle und ZielPowerStoreSysteme zum Aktivieren der synchronen und asynchronen Replikation und des Metro-Schutzes.

Voraussetzungen

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

- System-IP-Adresse
- Benutzerauthentifizierungsinformationen oder vorübergehende Zugangsdaten zum Herstellen einer Verbindung zum System

Schritte

1. Auswählen **Schutz** > **Remotesysteme**.
2. Klicken Sie im Fenster **Remotesysteme** auf **Add**.
3. Konfigurieren Sie im Slide-Out-Fenster **Remotesystem hinzufügen** die folgenden Felder:
   - Remotesystemtyp: Wählen Sie **PowerStore**.
   - Management-IP-Adresse
   - Beschreibung (optional)
   - Dateiverbindungstyp
     - TCP – Wählen Sie die Netzwerklatenz aus.

       ANMERKUNG: Wenn das Remotesystem für die Metro- oder synchrone Replikation verwendet wird, muss die Netzwerklatenz auf „Niedrig“ festgelegt werden.

     - Fibre Channel (SCSI)

ANMERKUNG: Um die Replikation über FC zu konfigurieren, stellen Sie Folgendes sicher:

- Ports für die Replikation werden auf beiden konfiguriertPowerStoreSysteme (Bestimmen Sie, welche Ports für die Replikation verfügbar sind, und legen Sie Zonen für das FC-Netzwerk fest.
- Die Netzwerkverbindung wird hergestellt zwischen demPowerStoreSysteme auf den Managementschnittstellen.

- Nutzername oder temporäre ID

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

Ergebnisse

Das neue Remotesystem wird der Tabelle **Remotesysteme** hinzugefügt. Sie können den Mauszeiger über die Spalte **Capability** bewegen, um die Remoteschutzfunktionen für die neue Verbindung anzuzeigen.

ANMERKUNG: Die angezeigten Funktionen werden aus den Netzwerkkonfigurationen und den Softwareversionen abgeleitet, die auf den lokalen und Remotesystemen ausgeführt werden.

Temporäre Zugangsdaten für die Authentifizierung erzeugen

Info über diese Aufgabe

Wenn CAC/PIV auf PowerStore aktiviert ist, wird die Authentifizierung, die auf einem Nutzernamen und einem Kennwort basiert, deaktiviert. Wenn Sie einen Nutzernamen und ein Kennwort für die Authentifizierung angeben müssen (z. B. beim Erstellen einer Remotesystemverbindung), können Sie eine temporäre ID und einen geheimen Schlüssel mithilfe von PowerStore Manager oder einer REST API erstellen.

ANMERKUNG: Die temporären Zugangsdaten laufen nach 10 Minuten ab.

ANMERKUNG: Um die temporären Zugangsdaten mithilfe der REST API zu erstellen, führen Sie den Befehl „generate_temp_credentials“ aus.

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

Schritte

1. Wählen Sie unter PowerStore Manager die Option **Einstellungen** aus.
2. Wählen Sie unter „Sicherheit“ die Option **Authentifizierung** aus.
3. Wählen Sie die Registerkarte **Temporäre Zugangsdaten** aus.
4. Wählen Sie **Temporäre ID und geheimen Schlüssel erzeugen** aus.
   Eine temporäre ID und ein geheimer Schlüssel werden angezeigt.

Festlegen des Zwecks des Storage-Netzwerks

PowerStoreUnterstützt die Konfiguration dedizierter oder gemeinsam genutzter Ports für Hostkonnektivität und Replikation.

Wenn Sie ein Storage-Netzwerk erstellen, können Sie den Netzwerkzweck im Schritt **Network Details** des Assistenten **Create Storage Network** festlegen (**Einstellungen** > **Netzwerke** > **Netzwerk-IP-Adressen** > **Storage** > **Erstellen**).

ANMERKUNG: Sie können einen oder alle der verfügbaren Zwecke auswählen:

- Speicher (iSCSI)
- Storage (NVMe/TCP)
- Replikation

So aktivieren Sie die Replikation oder den Metro-Schutz zwischen zweiPowerStore-Systemen die Option **Replikation** aus.

Um das Backup auf PowerProtect über TCP zu aktivieren, wählen Sie die **Option Replication** aus.

ANMERKUNG: Wenn mehrere Storage-Netzwerke mit mehreren IPs mit dem Replikationszweck konfiguriert sind, kann der Remoteschutz mehr Systemressourcen verbrauchen. Bei komplexen Netzwerkkonfigurationen wird empfohlen, die Anforderungen des Remoteschutznetzwerks zu überprüfen, bevor ein Replikationszweck zugewiesen wird.

Um einem Netzwerk einen Zweck hinzuzufügen, wählen Sie das Netzwerk und dann **Weitere Aktionen** > **Neu konfigurieren**. Sie können den hinzugefügten Zweck dann bestimmten Ports zuweisen, die dem Netzwerk zugeordnet sind.

Wenn ein Zweck für einen oder mehrere Ports aktiviert ist, die einem Netzwerk zugeordnet sind, können Sie den Zweck nicht aus diesem Netzwerk entfernen. Wenn Sie einen Zweck aus einem Netzwerk entfernen möchten, deaktivieren Sie diesen Zweck zunächst auf allen Ports, die dem Netzwerk zugeordnet sind.

Um einen Zweck für einen Port zu ändern, wählen Sie **Hardware** > **Anschlüsse** > **[Anschluss]** > **Weitere Aktionen** > **Zugewiesene Zwecke ändern**. Wählen Sie das entsprechende Netzwerk aus und aktivieren oder deaktivieren Sie dann Zwecke, um sie dem Port hinzuzufügen oder daraus zu entfernen.

ANMERKUNG: Sie können den Zweck Replikation nicht von einem Port entfernen, der einem Storage-Netzwerk zugeordnet ist, wenn ein TCP-Remotesystem dieses Netzwerk verwendet.

Wenn das Storage-Netzwerk für eine Portzuordnung ausgewählt ist (im Schritt **Zuordnung für Appliance** des Assistenten **Storage-Netzwerk erstellen**), wird der Zweck in der Spalte „Dem Port zugewiesene Zwecke“ angezeigt.

Wenn die Konfiguration abgeschlossen ist, wird das Storage-Netzwerk der Tabelle „Verfügbare Netzwerke“ hinzugefügt und der Zweck wird in der Spalte „Zwecke“ angezeigt.

Um die zugeordneten Storage-Netzwerke eines Ports und deren Zwecke anzuzeigen, wählen Sie **Hardware** > **Anschlüsse**. Das zugeordnete Storage-Netzwerk für jeden Port wird in der Spalte „Zugeordnetes Netzwerk“ aufgeführt. Wenn mehrere zugeordnete Netzwerke vorhanden sind, wird die Anzahl der zugeordneten Netzwerke aufgeführt. Wählen Sie den Netzwerknamen oder die Nummer aus, die in der Spalte „Zugeordnetes Netzwerk“ angezeigt wird, um die Liste der Netzwerke anzuzeigen, die dem Port zugeordnet sind.

Replikationsnetzwerkgruppen

Jedes Remotesystem kann verschiedene Replikationsnetzwerke und -ports verwenden, die in einer Replikationsnetzwerkgruppe definiert sind. Ein Remotesystempaar kann eine oder mehrere Replikationsnetzwerkgruppen für den Replikationsdatenverkehr verwenden. Wenn Sie eine Remoteverbindung erstellen, wird automatisch eine Standardreplikations-Netzwerkgruppe für das Remotesystempaar erstellt. Die Standardgruppe umfasst alle Netzwerke, die über einen Replikationszweck verfügen. Sie können Replikationsnetzwerkgruppen nach Bedarf hinzufügen, ändern und löschen.

Um Replikationsnetzwerkgruppen hinzuzufügen, zu ändern und zu löschen, wählen Sie **Schutz** > **Remotesysteme** aus. Wählen Sie ein Remotesystem aus der Liste und dann **Weitere Aktionen** > **Netzwerkgruppen verwalten** aus.

Um die Details der Netzwerkgruppen anzuzeigen, die für ein Remotesystempaar konfiguriert sind, wählen Sie den Namen des Remotesystems aus der Liste **Remotesysteme** (**Schutz** > **Remotesysteme**) aus, um das Fenster **Eigenschaften** des Remotesystems zu öffnen. Auf der Registerkarte „Konnektivität“ werden detaillierte Informationen zum Netzwerk für Replikationsdaten angezeigt, das auf der Konfiguration der Replikationsnetzwerkgruppe basiert.

Hinzufügen einer Replikationsnetzwerkgruppe

Info über diese Aufgabe

Wenn Sie eine Replikationsnetzwerkgruppe erstellen, wird dieselbe Netzwerkgruppenkonfiguration auf beiden Mitgliedern des Remotesystempaars erstellt.

ANMERKUNG: Es kann einige Minuten dauern, bis die Netzwerkgruppe auf den beiden PowerStore-Systemen konfiguriert ist.

So fügen Sie eine Netzwerkgruppe hinzu:

Schritte

1. Wählen Sie **Schutz** > **Remotesysteme** > **[Remotesystem]** aus.
2. Wählen Sie im Menü **Weitere Aktionen** die Option **Netzwerkgruppen verwalten** > **Erstellen** aus.
3. Geben Sie im Fenster **Netzwerkgruppen erstellen** den Gruppennamen an und wählen Sie das lokale Netzwerk und das Remotenetzwerk aus der jeweiligen Liste aus.
4. Wählen Sie **Übernehmen** aus, um die Gruppe zu erstellen.

Ändern einer Replikationsnetzwerkgruppe

Info über diese Aufgabe

Sie können ein oder mehrere Netzwerk(e) aus der Standardgruppe verschieben und je nach Bedarf eine separate Replikationsnetzwerkgruppe erstellen.

So ändern Sie eine Replikationsnetzwerkgruppe:

Schritte

1. Wählen Sie **Schutz** > **Remotesysteme** > **[Remotesystem]** aus.
2. Wählen Sie im Menü **Weitere Aktionen** die Option **Netzwerkgruppen verwalten** aus. Im Fenster **Netzwerkgruppen verwalten** werden die Netzwerkgruppen angezeigt, die für das Remotesystempaar erstellt wurden.
3. Wählen Sie die zu ändernde Gruppe aus und klicken Sie anschließend auf **Ändern**.
4. Im Fenster **Netzwerkgruppe ändern** können Sie den Gruppennamen ändern und der Gruppe lokale und Remotenetzwerke hinzufügen oder daraus löschen.
5. Wenn Sie fertig sind, wählen Sie **Ändern** aus, um die Änderungen zu übernehmen.

Löschen einer Replikationsnetzwerkgruppe

Info über diese Aufgabe

So löschen Sie eine Replikationsnetzwerkgruppe:

Schritte

1. Wählen Sie **Schutz** > **Remotesysteme** > **[Remotesystem]** aus.
2. Wählen Sie im Menü **Weitere Aktionen** die Option **Netzwerkgruppen verwalten** aus. Im Fenster **Netzwerkgruppen verwalten** werden die Netzwerkgruppen angezeigt, die für das Remotesystempaar erstellt wurden.
3. Wählen Sie die Gruppe aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
4. Wählen Sie **Löschen** aus, um den Vorgang zu bestätigen.

Verwenden von Jumbo Frames mit Remotesystemen

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.

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 (Wenn das Kennwort des PowerProtect DD-Nutzerkontos geändert wird...).

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 (Wenn eine Storage-Einheit aus DD entfernt wird...).

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 **Nutzerautorisierung** das Remotesystem-Zertifikat und klicken Sie auf **Bestätigen**, 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

Erstellen Sie einen Snapshot, um den Status einer Speicherressource zu einem bestimmten Zeitpunkt zu speichern und so die Wiederherstellung auf einen vorherigen Zustand zu ermöglichen.

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 eines Volumes, Volume-Gruppeeines Dateisystems 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 platzsparend sind, verbrauchen sie insgesamt Storage-Kapazität des Systems. Stellen Sie sicher, dass das System genug Kapazität für Snapshots hat.
- Überprüfen Sie bei der Konfiguration von Snapshots die Snapshot-Aufbewahrungs-Policy, die der Storage-Ressource zugeordnet ist. Sie können die Aufbewahrungs-Policy in den zugehörigen Regeln ändern oder je nach Zweck des Snapshot manuell eine andere Aufbewahrungs-Policy festlegen.
- Manuelle Snapshots, die mit PowerStore Manager erstellt werden, werden nach der Erstellung eine Woche lang aufbewahrt (sofern nicht anders konfiguriert).
- Wenn die maximale Anzahl von Snapshots erreicht ist, können keine weiteren erstellt werden. In diesem Fall müssen Sie vorhandene Snapshots löschen, um die Erstellung neuer Snapshots zu ermöglichen.

  ANMERKUNG: Weitere Informationen zu Snapshot-Limits finden Sie in der *Dell Technologies PowerStore Simple Support Matrix* auf der Seite PowerStore-Dokumentation.

- Um sichere Snapshots zu konfigurieren (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 erst am Ende des Aufbewahrungszeitraums gelöscht werden. Es 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 festgelegt. 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, Volumes,Volume-Gruppeoder Dateisystem, auf das ein Host zugreifen kann. Im Gegensatz zu einem vollständigen Clone 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.

ANMERKUNG: Wenn ein übergeordnetes Volume von einer Appliance zu einer anderen migriert wird, werden auch Thin Clones des Volumes migriert.

Erstellen eines Thin Clone eines Volume oderVolume-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. Auswählen **Storage** > **Volumes** oder **Storage** > **Volume-Gruppen** , um das entsprechende Ressourcenfenster zu öffnen.
2. Aktivieren Sie das Kontrollkästchen neben dem entsprechenden Volume oderVolume-Gruppeund wählen Sie dann **Neue Verwendung** > **Erstellen eines Thin Clone**.
3. Führen Sie im Slide-Out-Fenster **Erstellen Thin Clone** die folgenden Schritte aus:
   - Geben Sie einen Thin Clone-Namen ein.
   - Geben Sie eine Beschreibung ein.
   - Legen Sie eine QoS-Policy fest.
   - Legen Sie eine 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 eine Schutz-Policy fest.
4. Klicken Sie auf **Cloning**.

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**.

Aktualisieren eines NAS-Server-Clone

Aktualisieren Sie den geklonten NAS-Server mit den neuesten Daten aus der Quelle, ohne einen Clone erstellen zu müssen.

Voraussetzungen

Wenn ein Quell-NAS-Server erhebliche Konfigurations- und Datenänderungen durchläuft, muss der geklonte NAS-Server mit den Änderungen aktualisiert werden. Ab PowerStore 4.4 können Sie einen NAS-Server-Clone mit den Änderungen aktualisieren, die am Quellserver vorgenommen wurden.

Ein NAS-Server-Clone kann nicht aktualisiert werden, wenn:

- Der Clone verfügt über keine gültige Quelle (Sie finden die Clone-Quelle mithilfe der**NAS-Serverquelle**in der Tabelle **NAS Servers** .
- Der Clone enthält ein oder mehrere Dateisysteme, die nicht auf dem Host vorhanden sind (verwaiste Dateisysteme).
- Die Quelle oder der Clone enthält FLR-fähige Dateisysteme.
- Der NAS-Server ist Teil des aktiven NAS-Verschiebeprozesses.

Wenn ein neues Dateisystem auf der Quelle erstellt wurde, wird es während der Aktualisierung auf dem Ziel dupliziert.

Wenn ein Dateisystem vom Quell-NAS-Server gelöscht oder ein neues Dateisystem auf dem Clone-NAS-Server erstellt wird, schlägt die Aktualisierung des Clone fehl. Um den Clone zu aktualisieren, müssen die verwaisten Dateisysteme gelöscht und der Aktualisierungsvorgang erneut initiiert werden. Sie können die verwaisten Dateisysteme ausfindig machen, indem Sie den geklonten NAS-Server in der Tabelle **NAS-Server** auswählen und dann**Neue Verwendung** > **Anzeigen verwaister Dateisysteme**.

ANMERKUNG: Andere Konfigurationsänderungen als SMB- und NFS-Namen und -IPs werden im Rahmen des Aktualisierungsvorgangs nicht überschrieben.

ANMERKUNG: QoS-Policies werden nicht von Quelle auf Clone aktualisiert.

Info über diese Aufgabe

So aktualisieren Sie einen NAS-Server-Clone:

Schritte

1. Öffnen Sie das Fenster **NAS-Server** .
2. Wählen Sie einen NAS-Server-Clone aus und wählen Sie dann**Neue Verwendung** > **Clone aktualisieren**.

Ergebnisse

Der Clone-NAS-Server wird mit Daten vom Quell-NAS-Server aktualisiert und die Aktualisierungszeit und das Aktualisierungsdatum werden im**Letzte Aktualisierung**in der Tabelle **NAS Servers** .

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 für Block-Snapshots unterstützt, die für Volume- oder Volume-Gruppen und für Dateisystem-Snapshots erstellt werden (sowohl Protokoll als auch .snapshot).

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, eine Volume-Gruppe oder ein Dateisystem zu erzeugen, wählen Sie die Option **Sicherer Snapshot** im Bereich **Snapshot erstellen** 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. Fügen Sie der Tabelle **Snapshot-Regeln** die Spalte **Sichere Snapshots aktiviert** hinzu, um anzuzeigen, welche Regeln sichere Snapshots erzeugen.

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. Storage-Objekte 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 OS 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 PowerStore OS unter Version 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 PowerStore OS unter Version 3.5 auftritt, werden keine sicheren Snapshots für die Storage-Ressource erstellt.
- Sie können einen sicheren Snapshot wiederherstellen.
- Sie können einen sicheren Snapshot nicht aktualisieren.

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, des Replikationstyps 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 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:
   - Erstellen Sie den Regelnamen.
   - Wählen Sie ein vorhandenes Replikationsziel aus, oder konfigurieren Sie ein neues Ziel.
   - Wählen Sie den Replikationstyp (asynchron oder synchron) aus.

     ANMERKUNG: Durch Auswahl des synchronen Replikationstyps werden die RPO- und Warnmeldungsschwellenwerte auf Null gesetzt. Diese Werte können nicht geändert werden.

   - Wenn Sie den asynchronen Replikationstyp ausgewählt haben:
     - Legen Sie die RPO fest.
     - Legen Sie den alert threshold fest.
6. Klicken Sie auf **Create**.

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 asynchrone 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 **Protection** > **Protection 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:
   - Regelname
   - 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.
   - Aufbewahrungsfrist: Wählen Sie die Zeiteinheit ("Stunden", "Tage", "Monate" oder "Jahre") aus und legen Sie den Zeitraum fest, in dem die erzeugten Backups aufbewahrt werden sollen.

     ANMERKUNG: Die maximale Aufbewahrung beträgt 70 Jahre.
5. Klicken Sie auf **Erstellen**.

Erstellen einer Datensicherheits-Policy

Info über diese Aufgabe

Erstellen Sie eine Schutz-Policy, um lokalen 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. Auswählen **Schutz** > **Schutz-Policys**.
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 den Policy- und Regelnamen auf dem Quellsystem und dem angehängten Namen des Remotesystems. 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 Schutz-Policies, die Metro-Volumes zugewiesen sind, wird eine identische schreibgeschützte Policy auf dem Remotesystem erstellt und kann im Fenster **Schutz-Policies** des Remotesystems angezeigt werdenPowerStoreManager.

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.

Sie können eine asynchrone Replikationssitzung in eine synchrone Replikation (für Blockressourcen) oder eine synchrone Replikationssitzung in eine asynchrone Replikation (Block- und Dateiressourcen) ändern, indem Sie die in der Schutz-Policy verwendete Replikationsregel ändern.

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 Schutz-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:

- Zuweisen von Schutz-Policies mit Snapshot-, Replikations- und Remotebackupregeln zu Volumes undVolume-Gruppen.
- 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. Nachdem die Schutz-Policy dem Metro-Volume oder der Volume-Gruppe zugewiesen wurde, werden die Policy- und Snapshot-Regeln auf das Remotesystem kopiert und in den Tabellen "Protection Policies" und "Snapshot Rules" mit einem Schlosssymbol angezeigt, das anzeigt, dass sie schreibgeschützt sind.

Zum Schutz von Datei-Storage:

- PowerStoreUnterstützt 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.
- Sie können einem NAS-Server und den darin enthaltenen Dateisystemen verschiedene Schutz-Policies zuweisen.

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.

- Wenn Sie eine Schutz-Policy, die eine asynchrone Replikationsregel enthält, durch eine Policy ersetzen, die eine synchrone Replikationsregel enthält, kann dies Auswirkungen auf die Performance der Volume- und Volume-Gruppenreplikationssitzungen haben.

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

Info über diese Aufgabe

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.

ANMERKUNG: Das Aufheben der Zuweisung einer Schutz-Policy, die eine synchrone Replikationsregel enthält, kann nur über das System erfolgen, das über die Lese-/Schreib-Policy verfügt (und nicht über die schreibgeschützte Kopie der Policy).

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:

Asynchrone Replikation

Die asynchrone Replikation ist ein Replikationsmodus, in dem Updates des Zielsystems (z. B. Änderungen an Inhalt, Größe und Mitgliedschaft) in einem festgelegten Intervall basierend auf der definierten RPO erfolgen. Während der Synchronisierung wird das Zielsystem mit allen Datenänderungen aktualisiert, die seit dem letzten Synchronisierungszyklus aufgetreten sind.

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

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

Um die asynchrone Replikation auf eine Storage-Ressource anzuwenden, weisen Sie die Ressource einer Schutz-Policy zu, die eine asynchrone Replikationsregel enthält. Durch das Zuweisen einer Schutz-Policy wird eine Replikationssitzung erstellt, die der Liste der Replikationssitzungen hinzugefügt wird (**Schutz** > **Replikation**), und die Spalte „Replikationstyp“ zeigt „Asynchron“ angezeigt.

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 Snapshot-Synchronisation wird für die Dateireplikation nicht unterstützt.

Sie können die Synchronisierung einer Replikationssitzung jederzeit manuell initiieren, indem Sie die Replikationssitzung und dann **Synchronisieren** auswählen. Die Replikationssitzung muss sich in einem folgenden Status befinden:

- Läuft normal
- 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

ANMERKUNG: Ein (geplantes oder ungeplantes) Failover ist erst möglich, nachdem eine Baseline-Datenkopie auf das Zielsystem geschrieben wurde. Dies wird durch den Status OK der Replikationssitzung angezeigt.

Eine Zusammenfassung der Attribute der asynchronen Replikation und einen Vergleich mit der synchronen Replikation und Metro finden Sie unter Replikationszusammenfassung.

Asynchrone Replikation für den Block

Für die asynchrone Blockreplikation gilt Folgendes:

- Wenn eine asynchrone Replikationssitzung erstellt wird, wird eine entsprechende schreibgeschützte Ressource auf dem Zielsystem erstellt. Eine schreibgeschützte Definition der Schutz-Policy wird auch auf dem Zielsystem erstellt. Diese Policy wird verwendet, wenn ein Failover der Replikationssitzung durchgeführt wird.
- 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.
- Sie können von asynchroner zu synchroner Replikation wechseln, indem Sie die Replikationsregel in der zugewiesenen Schutz-Policy ändern.

ANMERKUNG: Der Wechsel von asynchroner Replikation zu synchroner Replikation kann sich auf die Performance der Volume- und Volume-Gruppenreplikationssitzungen auswirken.

Asynchrone Replikation für die Datei

Für die asynchrone Dateireplikation gilt Folgendes:

- Die Schutz-Policy wird dem NAS-Server zugewiesen und standardmäßig werden alle Dateisysteme auf einem geschützten NAS-Server vom Quell- zum Zielsystem synchronisiert
- Sie können Dateisysteme hinzufügen oder Dateisysteme vom NAS-Server löschen, auch wenn er Teil einer Replikationssitzung ist.
- Wenn Dateisysteme während einer asynchronen Replikationssitzung geändert werden, werden die Änderungen beim nächsten Synchronisationszyklus auf dem Zielsystem übernommen.
- Der Wechsel von asynchroner zu synchroner Replikation wird nicht unterstützt.
- Die Snapshot-Replikation wird nicht unterstützt.

Synchrone Replikation

Die synchrone Replikation ist ein Replikationsmodus, in dem Aktualisierungen von Daten auf dem Quellsystem sofort auf das Zielsystem repliziert werden, sobald die Aktualisierung erfolgt (Replikation mit einer RPO von null). Durch die synchrone Replikation wird sichergestellt, dass beide Systeme zu jedem Zeitpunkt vollständig synchronisiert sind. Bei der synchronen Replikation wird kein Datenverlust garantiert, es kann jedoch je nach Entfernung zwischen den Quell- und Zielsystemen zu Latenzzeiten kommen.

ANMERKUNG: Keine Datenverluste sind garantiert, wenn die Replikation nicht ordnungsgemäß funktioniert, z. B. während der Pausen von Replikationssitzungen oder Netzwerkausfällen.

PowerStore Unterstützt synchrone Remotereplikation für Volumes, Volume-Gruppen, Thin Clones, Block-Snapshots und NAS-Server.

Um eine synchrone Replikation auf eine Storage-Ressource anzuwenden, weisen Sie die Ressource einer Schutz-Policy zu, die eine synchrone Replikationsregel enthält. Durch das Zuweisen einer Schutz-Policy wird eine Replikationssitzung erstellt, die der Liste der Replikationssitzungen (**Protection** > **Replication**) hinzugefügt wird. In der Spalte Replication Type wird Synchronous angezeigt.

Beim Erstellen einer Replikationssitzung wird die Storage-Ressource auf das Zielsystem repliziert. Beim Aktualisierungen der Ressource erfolgen, werden nur diese Aktualisierungen auf das Zielsystem repliziert.

Sie können das Failover einer synchronen Replikationssitzung mithilfe eines geplanten oder ungeplanten Failover durchführen. Weitere Informationen finden Sie im Abschnitt Failover.

Wenn Sie die Zuweisung der Schutz-Policy zur Storage-Ressource aufheben, wird die Replikationssitzung gelöscht. Wenn die Replikationssitzung normal ausgeführt wird, kann die Zuweisung der Policy nur auf dem Quellsystem aufgehoben werden.

Wenn Sie eine Schutz-Policy zuweisen, die eine synchrone Replikationsregel enthält, verfügt das Quellsystem über eine Lese-/Schreib-Policy, das Zielsystem hingegen über eine schreibgeschützte Kopie der Policy. Nur die Lese-/Schreib-Policy kann geändert oder entfernt werden. Wenn das System mit der Lese-/Schreib-Policy ausfällt, führt ein Failover zum Wechsel der Rollen der Systeme und Sie können die Lese-/Schreib-Policy über das Zielsystem verwalten.

Um die synchrone Replikation zu aktivieren, muss das Systempaar mit niedriger Netzwerklatenz (unter 5 Millisekunden) konfiguriert werden. Die konfigurierte Netzwerklatenz kann nicht geändert werden, während synchrone Replikationssitzungen für diese Systeme konfiguriert sind.

Eine Zusammenfassung der Attribute der synchronen Replikation und einen Vergleich mit der asynchronen Replikation und Metro finden Sie unter Replikationszusammenfassung.

Synchrone Replikation für den Block

- Beim Erstellen einer synchronen Replikationssitzung wird eine entsprechende schreibgeschützte Ressource auf dem Zielsystem erstellt. Eine schreibgeschützte Definition der Schutz-Policy wird auch auf dem Zielsystem erstellt. Diese Policy wird verwendet, wenn ein Failover der Replikationssitzung durchgeführt wird.
- Nutzer-Snapshots:
  - Snapshots der Ressource, die vor der Erstellung der Sitzung erstellt wurden, werden mit dem Zielsystem synchronisiert.
  - Nach der Erstellung der Replikationssitzung werden gleichzeitig Nutzer-Snapshots auf den Quell- und Zielsystemen mit nahezu identischem Inhalt erstellt.
  - Nutzer-Snapshots, die erstellt werden, wenn die Replikationssitzung angehalten wird, werden nach der Wiederaufnahme oder Recovery nicht auf das Zielsystem repliziert.
- Um die Parameter einer Ressource (z. B. Name, Größe und Performance-Policy) zu ändern, müssen Sie die Replikationssitzung anhalten.
- Sie können von einer synchronen zu einer asynchronen Replikation wechseln, indem Sie die Replikationsregel in der zugewiesenen Schutz-Policy ändern.

Während der synchronen Blockreplikation können Sie Folgendes ausführen:

- Intracluster-Migration: Während der Umstellung ändert sich der Status der Replikationssitzung in „Für Migration angehalten“. Die Replikationssitzung setzt ihren Status fort, wenn die Migration abgeschlossen ist. Sitzungen, die beim Start der Migration angehalten wurden, bleiben angehalten.
- Unterbrechungsfreies Upgrade (Non-disruptive Upgrade, NDU) – Replikationssitzungen, die beim Start des NDU den Status „Normalbetrieb“ aufweisen, bleiben während des unterbrechungsfreien Upgrades weiterhin aktiv. Der Status angehaltener Replikationssitzungen ändert sich in „Für unterbrechungsfreies Upgrade angehalten“.
- Clusterneukonfiguration – Sie können das Clusterreplikationsnetzwerk neu konfigurieren, den Cluster erweitern oder verkleinern oder verlagern. Die Replikation wird nach Abschluss der Neukonfiguration fortgesetzt.

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. Sie müssen die Replikationssitzung nicht anhalten 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.

Folgendes gilt für die synchrone Replikation von Volume-Gruppen:

- Alle Mitglieder müssen sich auf derselben Appliance befinden.
- Nur Volume-Gruppen mit einer konfigurierten Schreibreihenfolge können einer Schutz-Policy mit einer synchronen Replikationsregel zugewiesen werden.
- Eine Schutz-Policy, die einer Volume-Gruppe zugewiesen ist, gilt für alle Mitglieder der Gruppe. Einzelne Volumes in einer Volume-Gruppe können nicht durch eine Schutz-Policy geschützt werden.
- Um die Parameter einer Volume-Gruppe (z. B. Name, Performance-Policy und Konsistenz der Schreibreihenfolge) zu ändern, müssen Sie die ihr zugewiesene Replikationssitzung anhalten.

Synchrone Replikation für Dateien

Für die Dateireplikation gilt Folgendes:

- Die Schutz-Policy wird dem NAS-Server zugewiesen und standardmäßig werden alle Dateisysteme auf einem geschützten NAS-Server vom Quell- zum Zielsystem synchronisiert.
- Sie können Dateisysteme hinzufügen oder Dateisysteme vom NAS-Server löschen, auch wenn er Teil einer Replikationssitzung ist.
- Wenn eine synchrone Replikationssitzung erstellt wird, werden ein NAS-Server und leere Dateisysteme auf dem Zielsystem erstellt. Die Dateiserverkonfiguration und eine schreibgeschützte Schutz-Policy werden ebenfalls repliziert.
- Der NAS-Server auf dem Zielsystem ist ohne aktivierte IP-Konfiguration konfiguriert und alle Dateisysteme sind ohne aktivierte Freigaben verfügbar
- Wenn eine Replikationssitzung erstellt wird, werden die Dateisysteme auf das Ziel repliziert. Nachfolgende Änderungen werden auf das Ziel repliziert, wenn sie vorgenommen werden.
- Bei der synchronen Replikation erfordert die Vergrößerung eines in der Replikation befindlichen Dateisystems, dass die Replikationssitzung zunächst angehalten wird. Zum Verkleinern der Größe eines Dateisystems muss die Replikationssitzung nicht angehalten werden.
- Für die synchrone Replikation ist es nicht möglich, die Netzwerklatenz des Replikationssystempaars auf einen höheren Wert als fünf Millisekunden zu ändern, wenn synchrone Replikationssitzungen definiert sind.

- Der Wechsel zwischen synchroner und asynchroner Replikation wird für die Dateireplikation nicht unterstützt.
- PowerStore Ab 4.1 wurde das Polling-Intervall von Replikationsobjekten auf zwei Minuten erhöht. Die Erhöhung erfolgte, um die Leistung bei mehreren Abfrageanforderungen zu verbessern. Warten Sie zusätzliche Zeit, bis der Objektstatus in PowerStore Manager aktualisiert wird.
- Ab PowerStore Version 4.3 wird für die synchrone Dateireplikation die Metro-Technologie für das automatische Failover verwendet, sodass ein Witness-Service konfiguriert werden muss.

Anhalten einer Replikationssitzung

Wenn Sie eine Replikationssitzung anhalten, werden Änderungen, die an der Ressource auf dem Quellsystem vorgenommen wurden, nicht auf das Zielsystem repliziert.

Sie können eine Replikationssitzung vom Quell- oder Zielsystem anhalten. Um ein Zielsystem anzuhalten, wählen Sie **Protection** > **Replication** > **[Replikationssitzung]** und dann **Pause** aus.

Wenn Sie eine synchrone Replikationssitzung anhalten, wird ein Recovery-Snapshot erstellt, der als letzte gemeinsame Basis dient, wenn die Sitzung fortgesetzt wird.

PowerStore Ab 4.3 verwendet die synchrone Dateireplikation Metro für das automatische Failover. Durch das Anhalten einer Replikationssitzung wird die Witness-Interaktion getrennt und das automatische Failover deaktiviert.

Während eine Replikationssitzung angehalten ist, können Sie Folgendes tun:

- Nehmen Sie die Replikationssitzung wieder auf.
- Löschen der Replikationssitzung durch Entfernen der Schutz-Policy von der Storage-Ressource
- Ändern der Größe oder Umbenennen der Storage-Ressource
- Ändern der Mitgliedschaft einer Volume-Gruppe.
- Initiieren der Migration zu einer anderen Appliance im Cluster

Fortsetzen einer Replikationssitzung

Wenn Sie eine Replikationssitzung fortsetzen, werden Änderungen, die während der Pause an der Ressource auf dem Quellsystem vorgenommen wurden, mit dem Zielsystem synchronisiert.

Sie können eine Replikationssitzung vom Quell- oder Zielsystem fortsetzen. Um ein Zielsystem fortzusetzen, wählen Sie **Schutz** > **Replikation** > **[angehaltene Replikationssitzung]** und dann **Fortsetzen** aus.

Wenn Sie eine synchrone Replikationssitzung fortsetzen, werden Änderungen an der Storage-Ressource auf dem Quellsystem basierend auf dem Recovery-Snapshot, der erstellt wurde, als die Sitzung angehalten wurde, mit der Ressource auf dem Zielsystem synchronisiert. Hostdaten, die während der Pause auf die Ressource geschrieben wurden, werden mit dem Ziel synchronisiert. Die laufende Replikation wird fortgesetzt, um die Synchronisierung zwischen Quelle und Ziel aufrechtzuerhalten.

ANMERKUNG: Snapshots, die erstellt wurden, während die Replikationssitzung angehalten wurde, werden nicht mit dem Ziel synchronisiert.

PowerStore Ab 4.3 verwendet die synchrone Dateireplikation Metro für das automatische Failover. Nach der Wiederaufnahme einer Replikationssitzung dauert es etwa fünf Minuten, bis der Status des Witness-Service in "Engagiert" wechselt.

Wenn Sie eine asynchrone Replikationssitzung fortsetzen, wird die Synchronisierung bei der nächsten RPO durchgeführt. Sie können Ressourcen manuell synchronisieren, indem Sie die Replikationssitzung und dann **Synchronisieren** auswählen.

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 Synchronisierung zwischen Quelle und Ziel, um Datenverlust zu vermeiden.
- Ungeplantes Failover – Eingeleitet vom Zielsystem als Reaktion auf einen Ausfall des Quellsystems.

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)
- Wenn der Nutzer ein geplantes Failover durchgeführt hat, führen Sie die Aktion „Neu schützen“ aus.

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.

ANMERKUNG: Ein Failover-Test kann nur auf dem Zielsystem durchgeführt werden.

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.

Um den Failover-Test zu beenden, 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 zur 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 TastenPowerStoreDie Version auf dem Quell- und Zielsystem ist 2.x oder höher.
- Der Status der Replikationssitzung ist OK.

  ANMERKUNG: Ein Failover-Test kann auch durchgeführt werden, wenn der Status der Replikationssitzung "System Paated" oder "Paused" nach Abschluss der Erstsynchronisation lautet.

Während des Failover-Tests können Sie die folgenden Aktionen auf dem Zielsystem nicht durchführen:

- 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, um den Verlust von Daten zu vermeiden, die nach dem Start des Failover-Tests auf das Ziel repliziert werden.

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:

- Von **Schutz** > **Replikation**, wählen Sie 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:

- Von **Schutz** > **Replikation**, wählen Sie die Replikationssitzung aus, in der ein Test ausgeführt 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 Start des Failovers wird das Zielsystem mit dem Quellsystem synchronisiert, um Datenverlust zu vermeiden.

Bevor Sie ein geplantes Failover durchführen, müssen Sie alle I/O-Vorgänge für Anwendungen und Hosts beenden. 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 Löschen 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.

Für die synchrone Replikation kann ein geplantes Failover vom Quellsystem initiiert werden, wenn sich die Replikationssitzung im Normalbetrieb befindet. Da die Daten vollständig zwischen den Systemen synchronisiert werden, wird kein Datenverlust durch das Failover verursacht. Es wird jedoch empfohlen, I/O-Vorgänge für Anwendungen und Hosts zu beenden, bevor Sie ein Failover initiieren.

Nach einem geplanten Failover ist die Replikationssitzung inaktiv. Verwenden Sie die Aktion **Neu schützen**, um die Ziel-Storage-Ressource 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.

ANMERKUNG: Wenn Daten im Rahmen der Aktion „Neu schützen“ synchronisiert werden, wird im Performancediagramm für das Quellsystem ein einzelner Punkt angezeigt. Da der nächste Zeitpunkt im Diagramm registriert wird, wenn die nächste Synchronisierung erfolgt, wird das Diagramm leer angezeigt. Um die Performancewerte anzuzeigen, zeigen Sie mit der Maus auf das Diagramm.

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, PowerStore kann nicht sichergestellt werden, dass sich beide NAS-Server in einem kompatiblen Zustand befinden. Nachdem die Verbindung wiederhergestellt wurde, befinden sich beide NAS-Server im Produktionsmodus (Split Brain). Infolgedessen wechseln beide Systeme in den Zielmodus, um zu verhindern, dass Daten an 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.

ANMERKUNG: VonPowerStore4.3 verwendet die synchrone Dateireplikation Metro für automatisches Failover. Wenn ein Witness-Service konfiguriert ist, ist automatisches Failover für alle synchronen Dateireplikationssitzungen verfügbar. Weitere Informationen zur Witness-Konfiguration finden Sie unter Metro Witness .

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: Bevor Sie ein ungeplantes Failover durchführen, fahren Sie den NAS-Server am Produktionsstandort herunter. Es wird nicht empfohlen, den Replikationslink herunterzufahren, um die Funktion für ungeplante Failover zu testen, da dies zur Nichtverfügbarkeit von Daten führen kann. VonPowerStore4.3 ist es erforderlich, den Cluster vor einem ungeplanten Failover herunterzufahren.

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.

ANMERKUNG: Um einen unterbrechungsfreien Zugriff auf Daten in der SMB-Umgebung zu ermöglichen, wird empfohlen, Continuous Availability für SMB-Freigaben zu konfigurieren und die Freigaben nach der Wiederherstellung der Verbindung erneut zu mounten.

Automatisches Failover für synchrone Dateireplikation

Bei der synchronen Dateireplikation wird die Metro-Technologie für das automatische Failover verwendet, sodass eine Witness-Servicetechnologie erforderlich ist, um automatisch ein Failover auf das Zielsystem durchzuführen, wenn das Quellsystem ausgefallen ist.

PowerStore Ab 4.3 wird für die synchrone Dateireplikation die Metro-Technologie für das automatische Failover verwendet. Ein Witness-Service muss konfiguriert werden, um das automatische Failover zu aktivieren.

Das System erkennt, wenn das Quellsystem ausgefallen ist, und führt automatisch ein Failover der Replikationssitzung auf das Zielsystem durch.

In der Replikationssitzungstabelle (**Protection** > **Replication**) zeigt **Auto Failover State** an, ob die Replikationssitzung für Auto-Failover aktiviert ist. Mögliche Zustände lauten:

- Nicht zutreffend: Die Replikationssitzung ist keine synchrone Dateireplikationssitzung.
- Upgrade erforderlich: Die Softwareversion des Remotesystems für die Replikationssitzung unterstützt den File Witness Service (FWS) nicht. Es ist erforderlich, das System auf eine Version zu aktualisieren, die FWS unterstützt, um das automatische Failover zu aktivieren.
- Manuelle Aktivierung erforderlich – Sowohl lokale als auch Remotesysteme unterstützen Witness-basiertes automatisches Failover. Um das automatische Failover für die Legacy-Replikationssitzung manuell zu aktivieren, aktivieren Sie das Kontrollkästchen neben der Sitzung und wählen Sie **dann Enable Auto Failover** aus.

- Enabled for Witness Interaction: Die Replikationssitzung ist für Witness-basiertes automatisches Failover aktiviert.

ANMERKUNG: **Der Auto-Failover-Status** wird auch im Detailfenster der Replikationssitzung angezeigt.

Die Replikation erfolgt auf NAS-Serverebene, aber synchronisierte File Metro-Replikationsvorgänge werden auf Dateisystemgruppenebene durchgeführt, die alle synchronisierten Dateisystempaare umfasst.

Wenn sich während einer synchronen File Metro-Replikationssitzung eines der Dateisystempaare nicht im synchronisierten Status befindet (z. B. nach dem Anhalten und Wiederaufnehmen der Replikationssitzung) und ein Verbindungsverlust ein automatisches Failover auslöst, wird für nicht synchronisierte Dateisysteme kein Failover auf das Zielsystem durchgeführt, während für alle Dateisysteme, die sich im synchronisierten Zustand befinden, ein Failover durchgeführt wird und I/O-Vorgänge vom neuen Quellsystem ausgeführt werden. Infolgedessen wird der Status der Replikationssitzung in **"Partielles Failover"** geändert.

Durch Klicken auf den Pfeil neben dem Namen des NAS-Servers in der **Replikationstabelle** wird die Liste der Dateisysteme mit dem Status der einzelnen Dateisysteme erweitert.

Sie können eine der folgenden Optionen auswählen:

- Warten Sie, bis das Quellsystem wiederhergestellt und die Replikationssitzung vollständig synchronisiert ist, und wiederholen Sie dann das Failover.

  ANMERKUNG: Um sicherzustellen, dass alle Dateisysteme synchronisiert sind, überprüfen Sie, ob sich der Status der Replikationssitzung (Spalte **Replikationssitzungsstatus** >) in **Failover** geändert hat. PowerStore Ab 4.3 können Sie auch die REST API verwenden, um den Synchronisationsstatus einer Replikationssitzung zu überprüfen. Überprüfen Sie für synchrone File Metro-Replikationssitzungen den Status auf dem Zielsystem. Überprüfen Sie bei Legacy-Replikationssitzungen den Status auf dem Quellsystem.

- Retry the failover using the force option: Wählen Sie die Replikationssitzung und dann **Failover** aus. Wählen Sie im angezeigten Hinweis zur **Failover-Replikation** die Option **Force failover from the destination resource** aus.

  ANMERKUNG: Das erzwungene Failover kann mithilfe der PowerStore Manager ODER REST API initiiert werden.

  ANMERKUNG: Die Verwendung von erzwungenem Failover kann zu Datenverlust führen.

Wiederherstellen eines NAS-Servers

Sie können Szenarien mit mehreren Ausfällen in Systemen durch Failover- oder Recovery-Maßnahmen beheben, um die Zugänglichkeit und Funktionalität des NAS-Servers aufrechtzuerhalten.

Es können Szenarien mit mehreren Fehlern auftreten, in denen die Quell- und Zielsysteme nicht miteinander kommunizieren können und eines der Systeme oder beide nicht mit dem Witness-Service kommunizieren können. Wenn diese Szenarien eintreten, sind die NAS-Server auf den lokalen und Remotesystemen offline und der Witness-Service kann nicht bestimmen, welches System für den Host zugänglich bleiben soll.

Um die folgenden Fehlerszenarien zu beheben, initiieren Sie ein Failover auf das Zielsystem:

- Die Verbindung zwischen dem Zielsystem und dem Witness-Service fällt aus, und dann fällt das Quellsystem aus.
- Der Witness-Service fällt aus und dann fällt das Quellsystem aus.

Um die folgenden Fehlerszenarien zu beheben, verwenden Sie die **Option Wiederherstellen** (**Storage** > **NAS-Server** > **[NAS-Server]** > **Weitere Aktionen** > **Wiederherstellen**):

- Die Verbindung zwischen dem Quellsystem und dem Witness-Service fällt aus, und dann fällt das Zielsystem aus.
- Der Witness-Service fällt aus und dann fällt das Zielsystem aus.
- Die Verbindung zwischen dem Zielsystem und dem Witness-Service, gefolgt von der Verbindung zwischen dem Quellsystem und dem Witness-System, fällt aus, und dann fällt die Verbindung zwischen dem Quell- und dem Zielsystem aus.
- Der Witness-Service fällt aus und dann fällt auch die Verbindung zwischen dem Quell- und dem Zielsystem aus.

Nachdem Sie **Recover** ausgewählt haben, wechselt der wiederhergestellte NAS-Server in den Produktionsmodus.

ANMERKUNG: Verwenden Sie die **Option Wiederherstellen** nicht für andere als die oben angegebenen Szenarien.

ANMERKUNG: Die Wiederherstellung des NAS-Servers kann auch mithilfe der REST API initiiert werden.

Weitere 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*.

PowerStore Ab 4.3 verwendet die synchrone Dateireplikation Metro für das automatische Failover. Es wird empfohlen, ein Failover der Replikationssitzung zum Remotestandort durchzuführen, bevor Sie das unterbrechungsfreie Upgrade initiieren, um ein automatisches Failover während Neustarts des Quellstandortclusters zu verhindern.

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.

In PowerStoreOS 3.6 und höher können Sie eine isolierte Disaster-Recovery-Testumgebung (DRT) erstellen, um auf einen Notfall vorbereitet 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 Integration in VMware Live Site Recovery zur Unterstützung der asynchronen Replikation von Virtual Volumes.

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

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

Snapshot- und Replikationsregeln, die in PowerStore werden vSphere zur Verfügung gestellt und können Schutz-Policies hinzugefügt werden. vSphere bietet eine Speicher-Policy für PowerStore während der Erstellung von vVols.

Eine Replikationsgruppe, die virtuelle Volumes enthält, 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 Aktion 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 Live Site Recovery verwendet diese VMware-Ressourcengruppen, um die geschützten VMs in Replikationsgruppen zu verwalten.

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.

Auf vSphere wird eine Schutzgruppe 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 PowerStorekönnen Sie den Status der Replikationssitzung während der Recovery überwachen.

Weitere Informationen finden Sie im *VMware Site Recovery Manager-Handbuch*.

6

Metro-Schutz

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Voraussetzungen und Einschränkungen

Berücksichtigen Sie vor der Konfiguration des Metro-Schutzes die folgenden Einschränkungen:

- Metro-Unterstützung ist nur verfügbar mitPowerStore T-ModellundPowerStoreQ-Modell-Appliances.
- Metro-Schutz wird für Volumes und Volume-Gruppen unterstützt.
- Metro-Schutz unterstützt FC/SCSI- oder iSCSI-verbundene Windows-, Linux- und VMware ESXi-Hosts.

ANMERKUNG: Windows- und Linux-Hosts werden abPowerStoreOS 4.x

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, stellen Sie sicher, dass die folgenden Bedingungen auf beidenPowerStoreSysteme:

- Die beiden Systeme werden ausgeführtPowerStoreOS 3.x oder höher
- Die Latenz auf dem Remotesystem ist niedrig.
- Datenverbindungstyp:
  - TCP – wenn lokal und remotePowerStoreSysteme mit Version 3.x (oder höher) installiert sind. Die TCP-Verbindung wird automatisch unterstützt. Wenn jedoch einer oder beide derPowerStoreSysteme, auf denen Version 2.x ausgeführt wird, müssen Sie ein Upgrade der Systeme auf 3.x durchführen, 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.

  - FC – StandPowerStoreVersion 4.4, FC-Verbindungstyp wird für Metro unterstützt.

Um einen Witness-Service bereitzustellen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Der Witness-Service muss auf einem eigenständigen Linux-Host (virtuell oder physisch) installiert sein.
- Der Witness-Service muss auf einer dritten Fehlerdomäne bereitgestellt werden, die von den beiden getrennt istPowerStoreSysteme, die Teil der Metro-Sitzung sind. Die Installation des Witness-Service auf einem separaten System stellt seine Verfügbarkeit sicher, wenn auf den Metro-Systemen ein Stromausfall auftritt.

- Unterstützte Betriebssysteme: Weitere Informationen finden Sie in der *Dell Technologies PowerStore Simple Support Matrix* auf der Seite „PowerStore-Dokumentation“.
- Abhängigkeiten (auf dem Linux-Host erforderlich):
  - Java 11 oder Java 17 (fürPowerStoreVersion 4.2 und höher)
  - SQLite

  ANMERKUNG: Die aufgelisteten Abhängigkeiten werden automatisch installiert, wenn Sie einen Paketmanager (z. B. Yum oder Zypper) verwenden.
- Hardware:
  - Das Betriebssystem muss auf einer x64-CPU-Architektur ausgeführt werden.
  - Mindestens 4 GB RAM
  - Mindestens 5 GB freier Festplattenspeicherplatz
- Ports:
  - Port 443/tcp muss vor der Installation des Witness auf dem Witness-Host geöffnet sein.
  - Rechenzentrumsfirewalls müssen Datenverkehr auf Port 443 zulassen, umPowerStoreZum Senden von Anforderungen an den Witness-Service.
- Netzwerklatenz – Maximale Latenz von 100 Millisekunden im Managementnetzwerk zwischenPowerStoreund der Witness-Service.
- Nutzerkontozugriff – Root- oder Sudo-Zugriff ist erforderlich, um den Witness-Service auf dem Host zu installieren.
- Stellen Sie die Konnektivität zumPowerStoreManagementnetzwerk.
- Für einen virtuellen Witness wird empfohlen, eine statische IP-Adresse für die Witness-VM zu verwenden. Wenn Sie jedoch DHCP verwenden, fügen Sie den Witness zuPowerStoreunter Verwendung des FQDN (Fully Qualified Domain Name).

ANMERKUNG: Weitere Informationen zu Metro-Limits finden Sie in der *Dell Technologies PowerStore Simple Support Matrix* auf der Seite „PowerStore-Dokumentation“.

Konfigurieren der Hostkonnektivität

ANMERKUNG: Hostunterstützung wird für VMware vSphere Metro-Storage-Cluster bereitgestellt. Sowohl Fibre Channel- als auch iSCSI-Verbindungen werden unterstützt.

ANMERKUNG: Ab PowerStore-Version 4.x wird Hostunterstützung für Windows- und Linux-Hosts bereitgestellt.

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.

Sowohl auf dem lokalen als auch auf dem Remotesystem muss ein Host (ESXi, Windows oder Linux) festgelegt werden, um die Host-Metro-Verbindung zu aktivieren.

Wenn Sie einen 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 Verbindung 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

In PowerStoreOS 3.6 und höher können Sie dem Metro-Schutz einen Witness-Service hinzufügen, um Schutz vor Szenarien mit einem einzelnen Ausfall zu bieten.

Der Witness-Service ist ein passiver Drittanbieter, der auf einem eigenständigen Host installiert wird.

ANMERKUNG: Der Witness-Service muss in einer dritten Fehlerdomäne bereitgestellt werden, die von den beiden PowerStore Systemen getrennt ist, die Teil der Metro-Sitzung sind. Durch die Installation des Witness-Service auf einem separaten System wird seine Verfügbarkeit bei einem Stromausfall auf den Metro-Systemen sichergestellt.

Wenn ein Fehler auftritt, kontaktieren die lokalen und Remotesysteme PowerStore den Witness-Service und fordern die Aufteilung 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-Service zu einer Metro-Sitzung bietet Schutz vor Szenarien mit einzelnen Ausfällen, einschließlich bevorzugter Systemausfälle, die ohne einen Witness nicht 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 Voraussetzungen erfüllt sind, können Sie RPM verwenden, um den Witness-Service direkt zu 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 einen Package Manager oder RPM verwenden, um den Witness-Service zu deinstallieren.

ANMERKUNG: Der Witness-Service ist nur verfügbar mitPowerStore T-ModellundPowerStoreQ-Modell-Appliances.

Konfigurieren des Metro Witness

Info über diese Aufgabe

- Nur Administratoren, Sicherheitsadministratoren und Speicheradministratoren sind berechtigt, den Witness-Service zu konfigurieren.
- Sie können den Witness-Service vor oder nach der Konfiguration von Metro konfigurieren.
- Pro Cluster kann nur ein Witness-Service konfiguriert werden.
- Der konfigurierte Witness-Service wird für alle Metro-Sitzungen verwendet und kann nicht für bestimmte Sitzungen deaktiviert werden.
- Der Status des Witness-Service ändert sich erst in "Engagiert", nachdem er sowohl für lokale als auch für Remotesysteme PowerStore konfiguriert wurde.
- Verwenden Sie den folgenden Pfad, um auf die Installationstools des Witness-Service (Generator für sichere Token und Fingerabdruck) 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 Manager **Protection** > PowerStore Metro 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. Überprüfen Sie die angezeigten Installationsanforderungen und aktivieren Sie das Kontrollkästchen zur Bestätigung.
5. Wählen Sie **Hinzufügen**.
6. 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 und Volume-Gruppen werden ihm automatisch zugewiesen. Neu erstellte Metro-Volumes und Volume-Gruppen werden automatisch dem Witness zugewiesen. Die Spalte **Metro-Ressourcen** im Fenster **Metro Witness** zeigt die Anzahl der Ressourcen an, die dem Witness zugewiesen sind.

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-Service zu ersetzen, entfernen Sie ihn aus den PowerStore Systemen und fügen Sie ihn dann hinzu. Das Entfernen und Hinzufügen des Witness ist auch dann erforderlich, wenn der Hostname oder die IP-Adresse nicht geändert wurden, da der neue Witness über ein anderes Zertifikat verfügt, das den PowerStore Systemen hinzugefügt werden muss.

Schritte

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

Ändern der Witness-Hostkonfiguration

Wenn der Host, auf dem der Witness-Service 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-Service unterhält die Kommunikation mit jedem Node auf jeder Appliance.

Im Fenster **Witness-Eigenschaften** werden der Verbindungsstatus für jeden Node und der allgemeine Verbindungsstatus des Witness-Service angezeigt.

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.
- Disengaged Invalid Configuration or Unavailable: Die Witness-Konfiguration ist ungültig (z. B. ist der Witness nur auf einem PowerStore-System konfiguriert oder auf dem lokalen und dem Remotesystem sind zwei verschiedene Witnesses konfiguriert) oder der Witness ist nicht verfügbar.
- Abgekoppelt, konnte nicht initialisiert werden: Der Witness konnte nicht mit der Metro-Sitzung initialisiert werden.
- Konfiguration wird aufgehoben – 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-Service 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 einem Witness-Service 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 ab zwei Volumes sichtbarPowerStoreSysteme mit Remotesystemverbindung

Metro kann für Volumes und für Clones von Volumes konfiguriert werden, die keine Mitglieder einer Volume-Gruppe sind.

Die folgenden Volumes können nicht als Metro konfiguriert werden:

- Ein Volume, dem eine Datensicherheits-Policy zugewiesen ist, die eine Replikationsregel enthält
- Ein Volume oder ein Volume-Clone, das/der bzw. der Mitglied einer Volume-Gruppe ist
- 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 hierfür konfiguriert wurdePowerStoreSystem wird das Metro-Volume automatisch dem Witness zugewiesen.

Schritte

1. Auswählen **Storage** > **-Volume** und aktivieren Sie das Kontrollkästchen eines Volumes.
2. Auswählen **Sichern** > **Konfigurieren eines Metro-Volumes**.
   Das Slide-Out-Fenster **Metro-Volume konfigurieren** wird angezeigt.
3. Wählen Sie ein Remotesystem aus oder konfigurieren Sie ein neues Remotesystem.
4. Wenn das Remotesystem über mehrere Appliances verfügt, können Sie die Platzierung des Volumes auf dem Remotesystem auswählen.
5. Klicken Sie auf **Configure**.
6. Weisen Sie auf dem Remotesystem das konfigurierte Metro-Volume einem Host zu.

Konfigurieren einer Metro-Volume-Gruppe

Info über diese Aufgabe

Durch Aktivieren der Metro-Konfiguration für eine Volume-Gruppe wird sie für Hosts ab zwei Volumes sichtbarPowerStoreSysteme mit Remotesystemverbindung

ANMERKUNG: Alle Volumes in einer Volume-Gruppe werden als eine einzige Instanz behandelt, und alle Aktionen, die die Volume-Gruppe betreffen, gelten für alle ihre Mitglieder.

Die folgenden Volume-Gruppen können nicht als Metro konfiguriert werden:

- Eine leere Volume-Gruppe
- Ein Volume-Gruppen-Clone
- Eine Volume-Gruppe mit einem Clone-Mitglied
- Eine Volume-Gruppe ohne Schreibreihenfolge-Konsistenz
- Eine Volume-Gruppe, die Volumes enthält, die nicht lokal sind
- Eine mit einer Schutz-Policy zugewiesene Volume-Gruppe, die eine Replikationsregel enthält.
- Eine Volume-Gruppe mit einer schreibgeschützten Schutz-Policy
- Eine Volume-Gruppe, die migriert oder importiert wird
- Eine Volume-Gruppe, die ein schreibgeschütztes Replikationsziel ist

ANMERKUNG: Wenn ein Witness hierfür konfiguriert wurdePowerStoreSystem wird die Metro-Volume-Gruppe dem Witness automatisch zugewiesen.

Schritte

1. Auswählen **Storage** > **Volume-Gruppe** Aktivieren Sie das Kontrollkästchen einer Volume-Gruppe.
2. Auswählen **Sichern** > **Metro-Volume-Gruppe konfigurieren**.
   Das Slide-Out-Fenster **Metro-Volume-Gruppe konfigurieren** wird angezeigt.
3. Wählen Sie ein Remotesystem aus oder konfigurieren Sie ein neues Remotesystem.
4. Klicken Sie auf **Configure**.
5. Weisen Sie auf dem Remotesystem die konfigurierte Metro-Volume-Gruppe einem Host zu.

Festlegen der Metro-Rolle

ANMERKUNG: Die Metro-Rolle kann für einzelne Volumes, Clones einzelner Volumes oder Volume-Gruppen festgelegt werden. Sie können keine Metro-Rolle für Volumes oder Clones festlegen, die Mitglieder einer Volume-Gruppe sind.

Nach der Konfiguration der Metro-Ressource wird das System, von dem aus die Metro-Ressource (Volume, Volume-Clone oder Volume-Gruppe) konfiguriert wurde, automatisch als bevorzugt festgelegt. Wenn die Metro-Ressource 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 Status der Metro-Ressource "Läuft normal" (aktiv/aktiv) lautet, können Sie die Rolle der Metro-Ressource mithilfe der folgenden Optionen von "Bevorzugt" in "Nicht bevorzugt" oder von "Nicht bevorzugt" in "Bevorzugt" ändern:

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

  ANMERKUNG: Sie können auf diese Option zugreifen, indem Sie **Schutz** > **Metro** Klicken Sie dann auf den Metro-Status der relevanten Ressource, um das Fenster Metro-Ressourcendetails zu öffnen.

- **Lokale Rolle auf "Bevorzugt" festlegen** : Verwenden Sie diese Option, um die Rolle mehrerer ausgewählter nicht bevorzugter Metro-Ressourcen auf "Bevorzugt" festzulegen. Diese Option sollte vor dem Herunterfahren des bevorzugten Systems für geplante Wartungsarbeiten verwendet werden. Wenn Sie die nicht bevorzugten Metro-Ressourcen auf „Bevorzugt“ festlegen, können der Host- und Produktionszugriff während des Herunterfahrens beibehalten werden.

Überwachen von Metro-Ressourcen

Info über diese Aufgabe

Sie können alle Metro-Ressourcen im System anzeigen, ihren Status überwachen und Aktionen für ein ausgewähltes Metro-Volume, einen Clone oder eine Volume-Gruppe durchführen.

Schritte

1. Auswählen**Schutz** > **Metro**, um die Liste der Metro-Ressourcen und Details zu öffnen.

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 der Ressource im**Metro-Status**-Spalte.

   Sie können auch detaillierte Informationen zu einer Metro-Ressource anzeigen über**Storage** > **Volumes**oder dem**Storage** > **Volume-Gruppen**Seite:

   a. Klicken Sie auf den Namen einer Metro-Ressource im**Storage** > **Volumes**oder dem**Storage** > **Volume-Gruppen**Seite, auf der die Seite "Ressourceninformationen" angezeigt wird.
   b. Wählen Sie das**Schutz**und wählen Sie dann die**Metro-Volume**oder dem**Metro-Volume-Gruppe**Registerkarte, auf der die Metro-Informationen für die ausgewählte Ressource angezeigt werden.

Anhalten einer Metro-Ressource

Info über diese Aufgabe

ANMERKUNG: Sie können einzelne Metro-Volumes, Clones oder Volume-Gruppen anhalten. Es ist nicht möglich, ein Metro-Volume oder einen Metro-Clone, die Mitglieder einer Volume-Gruppe sind, anzuhalten.

Das vorübergehende Anhalten einer Metro-Ressource ist in den folgenden Szenarien erforderlich:

- Wenn Konfigurationsänderungen erforderlich sind, die nicht durchgeführt werden können, wenn die Ressource normal funktioniert, z. B. Ändern der Ressourceneigenschaften.
- 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 eine Metro-Ressource angehalten wird, wird die Synchronisierung zwischen den Systemen vorübergehend gestoppt. Produktionszugriffs- und Datensicherheits-Policies bleiben auf dem bevorzugten System aktiv.

Wenn eine Metro-Ressource aufgeteilt ist und keine Verbindung zwischen dem lokalen und dem Remotesystem besteht, wird sie nur auf dem lokalen System angehalten (wo es initiiert wurde):

- Wenn ein Anhaltevorgang über das bevorzugte System initiiert wird:
  - Der Host- und Produktionszugriff bleiben auf einer angehaltenen, bevorzugten Metro-Ressource aktiviert.
  - Host- und Produktionszugriff bleiben auf der nicht bevorzugten Metro-Ressource unverändert.
- Wenn ein Anhaltevorgang über das nicht bevorzugte System initiiert wird:
  - Der Host- und Produktionszugriff bleiben deaktiviert, sofern die Metro-Ressource nicht hochgestuft wurde.
  - Da keine Netzwerkverbindung vorhanden ist, wird durch die Pause der bevorzugte Metro-Ressourcenstatus nicht geändert.
- Wenn die Verbindung aufgelöst wurde, sollte das Metro-Volume auch vom Remotesystem angehalten werden.

Schritte

1. Auswählen **Schutz** > **Metro**.
2. Aktivieren Sie das Kontrollkästchen der anzuhaltenden Metro-Ressource und klicken Sie auf **Pause**.
   Das Slide-Out-Fenster **Metro-Volume/Volume-Gruppe anhalten** wird angezeigt.
3. Klicken Sie zur Bestätigung auf **Anhalten**.

Fortsetzen einer Metro-Ressource

Info über diese Aufgabe

ANMERKUNG: Sie können einzelne Metro-Volumes, Clones oder Volume-Gruppen fortsetzen. Es ist nicht möglich, ein Metro-Volume oder einen Metro-Clone fortzusetzen, die Mitglieder einer Volume-Gruppe sind.

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

Wenn Sie eine bevorzugte, angehaltene Metro-Ressource fortsetzen, startet das bevorzugte System die Synchronisation von Daten mit dem nicht bevorzugten System. Nach Abschluss der Synchronisierung kehrt der Status der Metro-Ressource in den Aktiv-Aktiv-Zustand zurück.

Wenn Sie eine hochgestufte (zuvor nicht bevorzugte) angehaltene Metro-Ressource fortsetzen, startet das nicht bevorzugte System die Synchronisation mit dem bevorzugten System (Status „Neu schützen“), um in den Aktiv-Aktiv-Zustand zurückzukehren.

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

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

Schritte

1. Auswählen**Schutz** > **Metro**.
2. Aktivieren Sie das Kontrollkästchen der fortzusetzenden Metro-Ressource und klicken Sie auf**Wiederaufnehmen**.
   Das Dialogfeld **Metro-Volume/Volume-Gruppe fortsetzen** wird angezeigt.
3. Klicken Sie auf**Wiederaufnehmen**zur Bestätigung.

Hochstufen einer Metro-Ressource

Voraussetzungen

- Sie können einzelne Metro-Volumes, Clones oder Volume-Gruppen hochstufen. Es ist nicht möglich, ein Metro-Volume oder einen Metro-Clone, die Mitglieder einer Volume-Gruppe sind, hochzustufen.
- Das Hochstufen eines Metro-Volumes ist im Status `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 die Metro-Ressource 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 Synchronisierung zwischen den Systemen beendet und das Metro-Volume wird aufgeteilt. Beide Systeme bedienen keine I/O mehr. Um auf die Metro-Ressource zuzugreifen, müssen Nutzer die Metro-Ressource auf dem nicht bevorzugten System hochstufen, um den Host- und Produktionszugriff darauf zu aktivieren, bis das bevorzugte System wiederhergestellt wird.

Wenn der Nutzer feststellt, dass das bevorzugte System verfügbar ist, kann die Metro-Ressource auf dem nicht bevorzugten System problemlos hochgestuft werden. Wenn sich der/die Nutzerln 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. Auswählen**Schutz** > **Metro**.

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

   ANMERKUNG: Der Metro-Status der Ressource sollte `Fractured` lauten.

2. Wählen Sie den Status der Metro-Ressource aus, um die Detailseite der Metro-Ressource anzuzeigen, und wählen Sie dann**Übernehmen**.
   Das Slide-Out-Fenster **Metro-Volume/Volume-Gruppe hochstufen** wird angezeigt.

   ANMERKUNG: Vor der Hochstufung wird ein Snapshot der Metro-Ressource 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/Volume-Gruppe hochstufen** und wählen Sie**Übernehmen**.
   Der hochgestufte Status der Metro-Ressource wird auf der Seite mit den Metro-Ressourcendetails angezeigt.

Herunterstufen einer Metro-Ressource

Info über diese Aufgabe

ANMERKUNG: Sie können einzelne Metro-Volumes, Clones oder Volume-Gruppen herunterstufen. Es ist nicht möglich, ein Metro-Volume oder einen Metro-Clone, die Mitglieder einer Volume-Gruppe sind, herunterzustufen.

Wenn der Speicherplatz auf dem bevorzugten System knapp wird, wird die Synchronisierung zwischen den Systemen beendet und die Metro-Ressource wird aufgeteilt. Beide Systeme bedienen keine I/O mehr. In diesem Fall muss die Metro-Ressource 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 die Metro-Ressource auf dem bevorzugten System heruntergestuft werden.

Schritte

1. Auswählen**Schutz** > **Metro**.

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

2. Wählen Sie den Status einer Metro-Ressource aus, um die Detailseite der Metro-Ressource anzuzeigen, und wählen Sie dann**Herunterstufen**.
   Das Slide-Out-Fenster **Metro-Volume herunterstufen** wird angezeigt.
3. Vergewissern Sie sich, das Sie die Auswirkungen des Herunterstufens der Metro-Ressource verstehen, falls das Remotesystem I/Os verarbeitet, und überprüfen Sie nach Möglichkeit, ob das Remotesystem ausgefallen ist.
4. Auswählen**Herunterstufen**.
   Der heruntergestufte Status der Ressource wird auf der Detailseite der Metro-Ressource angezeigt.

Beenden einer Metro-Ressource

Info über diese Aufgabe

ANMERKUNG: Sie können einzelne Metro-Volumes, Clones oder Volume-Gruppen beenden. Es ist nicht möglich, ein Metro-Volume oder einen Metro-Clone zu beenden, die Mitglieder einer Volume-Gruppe sind.

Wenn Sie eine Metro-Ressource beenden, wird die Metro-Konfiguration entfernt, was zu zwei unabhängigen Volumes oder Volume-Gruppen führt. Wenn die Remote-Ressource nicht gelöscht wird, entfernt das System die ihm zugewiesene Schutz-Policy, hebt die Zuordnung der Hosts auf und weist sie einem neuen, anderen SCSI-WWN zu. Sie können eine Metro-Volume-Ressource über das bevorzugte oder das nicht bevorzugte System beenden.

Schritte

1. Auswählen**Schutz** > **Metro**.
2. Wählen Sie den Status einer Metro-Ressource aus, um die Detailseite der Metro-Ressource anzuzeigen, und wählen Sie dann**Metro beenden**.
   Das Slide-Out-Fenster **Metro-Volume/Volume-Gruppe beenden** wird angezeigt.
3. Wählen Sie eine der folgenden Optionen aus dem Slide-Out-Fenster aus:
   - Beenden Sie Metro und behalten Sie die Ressourcen auf dem lokalen und dem Remotesystem bei.

     ANMERKUNG: Das Remotesystem hebt die Zuordnung der Hosts auf und weist der Ressource einen anderen SCSI-WWN zu. Wenn Sie eine Metro-Volume-Gruppe beenden, wird jedem Mitglied der Volume-Gruppe ein anderer SCSI-WWN zugewiesen.

   - Beenden Sie Metro und löschen Sie die Ressource und alle zugehörigen Snapshots auf dem Remotesystem.

     ANMERKUNG: Remote-Volumes und Volume-Gruppen, die nicht abgelaufenen sicheren Snapshots zugeordnet sind, können nicht gelöscht werden.

4. Klicken Sie auf**Ende**.

Übersicht über die zulässigen Aktionen auf einer Metro-Ressource

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 ausführen können.

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

Tabelle 2. 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
	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

Verwenden von Schutz-Policies mit Metro

Wenn eine vorhandene Metro-Ressource mit einer Schutz-Policy zugewiesen wird oder ein Volume mit einer Schutz-Policy für Metro konfiguriert ist, wird derselbe Schutz auf die Metro-Ressource 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 Änderungen synchronisiert.

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

ANMERKUNG: Die synchrone und asynchrone Replikation wird mit Metro-Ressourcen nicht unterstützt. Eine Schutz-Policy, die eine Replikationsregel enthält, kann keiner Metro-Ressource 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 zur Ressource im lokalen System aufgehoben wurde, wird die Zuweisung zur Ressource auf dem anderen System aufgehoben. Sobald keine Metro-Ressourcen vorhanden sind, die die schreibgeschützte Schutz-Policy verwenden, wird sie automatisch aus dem System gelöscht.

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

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

ANMERKUNG: Wenn die Metro-Ressource aufgeteilt oder eine Metro-Sitzung angehalten wird, werden Snapshots nur auf dem aktiven System erzeugt. Wenn die Metro-Ressource 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.

Verwenden von QoS mit Metro

Wenn ein Metro-Volume oder eine Metro-Volume-Gruppe mit einer QoS-Policy konfiguriert ist, wird die Policy nicht auf das Remotesystem repliziert. Wenn Sie eine Metro-Konfiguration mit QoS verwenden, wird empfohlen, dieselbe QoS-Policy auf beiden Seiten der Metro-Ressource zu konfigurieren.

Wenn eine QoS-Policy nur auf einer Seite der Metro-Ressource konfiguriert ist, bevorzugt ein Host möglicherweise bestimmte Pfade zum Senden von I/O. Dies kann auch der Fall sein, wenn eine QoS-Policy auf beiden Seiten der Metro-Ressource konfiguriert ist, die QoS-Grenzwerte jedoch nicht übereinstimmen.

7

Remotebackup

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Terminologie

Tabelle 3. 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.
- Wenn die Größe der gespiegelten Volumes die maximale Speicherkapazität der Data Domain Storage Unit (SU) überschreitet, kann der Backup-Vorgang möglicherweise fehlschlagen. Es wird empfohlen, bei Verwendung von Remotebackup keine SU-Quoten festzulegen. Weitere Informationen finden Sie in der Dokumentation zu PowerProtect DD.
- 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.
- Remotebackup wird auf Metro-Volumes nicht unterstützt.
- 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).

Dokumentationsangebot

Weitere Informationen finden Sie in den folgenden Ressourcen:

Tabelle 4. Dokumentationsangebot

Dokument	Beschreibung	Position
PowerProtect Data Manager – Administrator- und Benutzerhandbuch	Dieses Dokument stellt Konfigurationsinformationen für PowerProtect Data Manager bereit.	Dell Support
Dell PowerProtect Data Manager: Data Protection für Dell PowerStore Handbuch zu Storage-Arrays	Dieses Dokument konzentriert sich auf das Backup und die Recovery von Block-Volume-Daten auf PowerStore Storage-Arrays mit PowerProtect Data Manager	Dell Infohub
PowerStore Onlinehilfe	Die Onlinehilfe enthält kontextsensitive Informationen für die in PowerStore Manager geöffnete Seite.	Eingebettet in PowerStore Manager

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 Schutz-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 wurde durch ein unterbrechungsfreies Upgrade oder eine 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** > **Remote Backup** 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 **Einstellungen** > **Cluster** > **Eigenschaften** anzeigen. Für weitere Informationen zum Abrufen der Cluster-Global-ID, siehe Dell Wissensdatenbank-Artikel 000226798 (Anleitung zum Abrufen der primären Cluster-Global-ID).
   - 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 **Weiter**.

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 für eine Storage-Ressource ausgeführt wird, kann der PowerStore Cluster keine Backup- und Abrufvorgänge für geschützte Ressourcen durchführen, die sich auf derselben Appliance wie diese Ressource befinden. Es wird empfohlen, die Instant-Access-Sitzung nach Möglichkeit zu beenden, um einen kontinuierlichen Schutz für Storage-Ressourcen bereitzustellen.
- 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-Ressource.

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 Access** im Fenster **Volumes** oder **Volume-Gruppen** 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 von PowerStore 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.

8

NDMP-Backup für NAS-Server

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Aktivieren des NDMP-Backups

Sie können Standardbackups für die NAS-Server mithilfe von NDMP konfigurieren. Das Network Data Management Protocol (NDMP) bietet einen Standard zur Sicherung von Dateiservern in einem Netzwerk. Wenn NDMP aktiviert ist, kann eine Datenmanagementanwendung (DMA) eines Drittanbieters, z. B. Dell NetWorker, denPowerStoreNDMP unter Verwendung der IP-Adresse des NAS-Servers.

Info über diese Aufgabe

Die Aktivierung von NDMP erfolgt nach der Erstellung des NAS-Servers.

PowerStoreunterstützt:

- Drei-Wege-NDMP – Die Daten werden durch die DMA über ein lokales Netzwerk (LAN) oder ein Wide Area Network (WAN) übertragen.
- Komplette und inkrementelle Backups

Schritte

1. Auswählen **Storage** > **NAS-Server** > **[NAS-Server]** > **Schutz**.
2. Wenn unter **NDMP Backup** die Option **Disabled** aktiviert ist, schieben Sie die Schaltfläche, um zu **Enabled** zu wechseln.
3. Geben Sie ein Kennwort für **New Password** ein.
   Der Nutzername lautet immer `ndmp`.
4. Geben Sie im Feld **Kennwort überprüfen** dasselbe Kennwort erneut als neues Kennwort ein.
5. Klicken Sie auf **Anwenden**.

Nächste Schritte

Verlassen Sie die NDMP-Seite und navigieren Sie zurück zur NDMP-Seite, um zu überprüfen, ob NDMP aktiviert ist.

A

Replikationszusammenfassung

Dieser Anhang enthält folgende Informationen:

Themen:

Replikationszusammenfassung

In der folgenden Tabelle sind die verschiedenen Attribute der Replikation (synchron und asynchron) und Metro zusammengefasst.

Tabelle 5. Replikation und Metro – Zusammenfassung

Attribut	Asynchrone Replikation	Synchrone Replikation	Metro
Unterstützter Typ	Block und Datei	Block und Datei	Block
Speicherressourcen	Volumes, Volume-Gruppen, Thin Clones, NAS-Server, vVols	Volumes, Volume-Gruppen, Thin Clones, NAS-Server	Volumes, Volume-Gruppen
Replikationstyp	Asynchronous	Synchronous	Synchronous
Ziel-RPO	Festwert 5 min – 24 h	0	0.
Hostzugriff	Aktiv/Passiv. Erfordert ein Failover	Aktiv/Passiv. Erfordert ein Failover oder RTO>0. Bei Dateien ist automatisches Failover erforderlich.	Aktiv/Aktiv-ALUA-Pfadwechsel
Hostprotokolle	SCSI, NVMe	SCSI, NVMe	SCSI
Block-WWN/NQN	Verschieden	Verschieden	Gleicher WWN an beiden Enden
Witness	Nein	Datei - Ja Block – Nein	Ja
RTT/Distanz	Nicht zutreffend	5 Millisekunden	5 Millisekunden*
Performance-Auswirkungen auf den Hostzugriff	Minimale Auswirkungen je nach Dimensionierung und Workload	Fügt zusätzliche Latenz hinzu (Round-Trip-Zeit für die Spiegelung)	Fügt zusätzliche Latenz hinzu (Round-Trip-Zeit für die Spiegelung)
Snapshot-Replikation	Replikation von Block-Snapshots auf der Quelle. Die Snapshot-Replikation für Datei wird nicht unterstützt.	Nahezu identische Block-Snapshots. Die Snapshot-Replikation für Datei wird nicht unterstützt.	Nahezu identische Snapshots
Failover-Test	Ja (z. B. Datei, Verwendung eines Clone)	Ja (z. B. Datei, Verwendung eines Clone)	Nicht zutreffend
Konvertierung asynchron <-> synchron	Zulässig für Blockressourcen. Wird für Datei nicht unterstützt.	Zulässig für Blockressourcen. Wird für Datei nicht unterstützt.	Nicht unterstützt
Recovery-Snapshot	Gemeinsame Basis bei jedem Replikationszyklus	Unterstützt bei Pause	Nicht unterstützt
NDU	Replikation wird während NDU angehalten.	Aktive Sitzungen werden fortgesetzt	Aktive Sitzungen werden fortgesetzt

1

1 Einige geschützte Anwendungen erfordern möglicherweise eine niedrigere RTT/Distanz für Metro-Konfigurationen.

B

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 Datenmigration 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 Rechenzentren für die vollständige Nutzung von PowerStore-Systemen über eine Aktiv/Aktiv-Umgebung optimiert werden, die einen Workload-Ausgleich 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 reduziert das Risiko für Datenverluste. Mit der Metro-Volume-Option ist die Migration unterbrechungsfrei. Wenn die Migration abgeschlossen ist, kann das Metro-Volume entweder entfernt oder beibehalten werden, um eine schnelle Recovery bei einem Systemausfall oder sogar einem vollständigen Standortausfall zu ermöglichen.