Dell PowerStore

Konfigurieren von SMB

4.1

Februar 2025
Rev. A07

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

Vorwort

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.

ANMERKUNG: Kunden mit PowerStore X-Modell: Die aktuellen technischen Handbücher und Leitfäden für Ihr Modell finden Sie in der *PowerStore 3.2.x-Dokumentation*, die Sie von der PowerStore-Dokumentationsseite dell.com/powerstoredocs herunterladen können.

Hier erhalten Sie Hilfe

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

- **Produktinformationen**: Dokumentation oder Versionshinweise zum Produkt und den Funktionen finden Sie auf der PowerStore-Dokumentationsseite dell.com/powerstoredocs.
- **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 einen Service-Request stellen zu können, müssen Sie über eine gültige Supportvereinbarung verfügen. Wenden Sie sich an Ihren Vertriebsmitarbeiter, wenn Sie einen gültigen Supportvertrag benötigen oder Fragen zu Ihrem Konto haben.

1

Übersicht

Dieses Kapitel enthält die folgenden Informationen:

Themen:

SMB-Unterstützung

PowerStore T-Modell und PowerStore Q-Modell unterstützen SMB 1 bis SMB 3.1.1. Wenn die SMB-Unterstützung auf dem NAS-Server aktiviert ist, können Sie SMB-fähige Dateisysteme erstellen. Der NAS-Server mit SMB-Unterstützung kann entweder eigenständig sein oder über die Active Directory-Domain verbunden werden. Die über die Domain verbundenen NAS-Server werden standardmäßig in der Organisationseinheit „OU=Computers, OU=EMC NAS Servers“ platziert.

ANMERKUNG: Der Client-Zugriff über das SMB1-Protokoll ist aufgrund potenzieller Sicherheitslücken standardmäßig deaktiviert. Wenn Client-Zugriff über SMB1 erforderlich ist, kann dies durch Ändern des Parameters `cifs.smb1.disabled` aktiviert werden. Es wird empfohlen, mindestens SMB2 zu verwenden, um die Sicherheit und Effizienz zu erhöhen.

SMB-Dateisysteme und -Freigaben verfügen über die folgenden erweiterten Protokolloptionen:

ANMERKUNG: Diese Optionen, mit Ausnahme von „Oplocks Enabled“, sind standardmäßig deaktiviert.

Tabelle 1. Erweiterte SMB-Protokolloptionen

Protokolloptionen	Level
Synchrone Schreibvorgänge aktiviert	Dateisystem
Oplocks aktiviert	Dateisystem
Benachrichtigung bei Schreibvorgang aktiviert	Dateisystem
Benachrichtigung bei Zugriff aktiviert	Dateisystem
Kontinuierliche Verfügbarkeit	Share
Protokollverschlüsselung	Share
Access Based Enumeration	Share
Branch Cache aktiviert	Share
Offlineverfügbarkeit	Share

Überlegungen zur Planung

Überprüfen Sie die folgenden Informationen, bevor Sie NAS-Server und Dateisysteme konfigurieren:

Unterstützung für Datei-Storage ist nur auf den PowerStore T-Modell- und PowerStore Q-Modell-Appliances verfügbar.

NAS-Servernetzwerke

Konfigurieren Sie Folgendes, bevor Sie NAS-Server mit dem SMB-Protokoll konfigurieren:

1. Konfigurieren Sie einen oder mehrere DNS-Server.

2. Wenn Sie den NAS-Server zu Active Directory (AD) hinzufügen, konfigurieren Sie mindestens einen NTP-Server auf dem Speichersystem, um das Datum und die Uhrzeit zu synchronisieren. Es wird empfohlen, mindestens zwei NTP-Server pro Domain einzurichten, um einen Single-Point-of-Failure zu vermeiden.

   ANMERKUNG: Während der AD-Erstellung wird NTP konfiguriert.

3. Erstellen Sie ein Domain-Konto in Active Directory.

Das Erstellen von Netzwerk-VLANs und IP-Adressen ist für NAS-Server optional. Wenn Sie beabsichtigen, ein VLAN für NAS-Server zu erstellen, kann das VLAN weder für das PowerStore T-Modell und das PowerStore Q-Modell-Management noch für die Storage-Netzwerke freigegeben werden. Stellen Sie außerdem sicher, dass Sie mit Ihrem Netzwerkadministrator zusammenarbeiten, um die Netzwerkressourcen zu reservieren und das Netzwerk auf dem Switch zu konfigurieren. Weitere Informationen finden Sie unter *PowerStore T und Q – Netzwerkleitfaden für Storage-Services*.

Skalierbarkeit

Ab PowerStore OS 3.5 gibt es ein gemeinsames Limit für Dateisystem-Volumes und vVols. Die Gesamtzahl der Objekte wird gemäß des höchsten Grenzwerts der drei Objekttypen bestimmt.

Informationen zum Anzeigen des Grenzwerts für Dateisysteme pro Plattform finden Sie unter *Einfache Supportmatrix für Dell Technologies PowerStore* auf der PowerStore-Dokumentationsseite.

Bereitstellungsanforderungen

NAS-Services sind nur auf PowerStore T-Modell- und PowerStore Q-Modell-Appliances verfügbar.

Sie müssen während der Erstkonfiguration Ihrer PowerStore T-Modell- oder PowerStore Q-Modell-Appliances **Unified** ausgewählt haben. Wenn Sie während der Ausführung des Assistenten für die Erstkonfiguration **Blockoptimiert** ausgewählt haben, wurden keine NAS-Dienste installiert. Um NAS-Services zu installieren, muss ein/e MitarbeiterIn des technischen Supports Ihr System neu initialisieren. Erneutes Initialisieren des Systems:

- Die Appliance wird in den Werkzustand zurückgesetzt.
- Die gesamte Konfiguration wird entfernt, die auf dem System über den **Assistent für die Erstkonfiguration** durchgeführt wurde.
- Sämtliche Konfigurationen werden entfernt, die in PowerStore nach der Erstkonfiguration vorgenommen werden.

Weitere Überlegungen

Beide Nodes auf der Appliance müssen funktionsfähig sein, um einen NAS-Server zu erstellen. Wenn einer der Nodes auf der Appliance ausgefallen ist, schlägt die Erstellung NAS-Servers fehl.

Erstellen der Netzwerkschnittstelle für NAS-Datenverkehr

Sie können ein NAS-Netzwerk mithilfe von LACP-Bündelungen (Link Aggregation Control Protocol) oder durch Erstellen eines ausfallsicheren Netzwerks für NAS-Datenverkehr konfigurieren.

Erstellen von LACP-Bündelungen für NAS-Datenverkehr

Wenn Ihre Switches mit MC-LAG konfiguriert sind, können Sie die Netzwerkbündelung verwenden, indem Sie eine Link Aggregate Group (LAG) für NAS-Datenverkehr erstellen.

Info über diese Aufgabe

Wenn die Top-of-Rack(ToR)-Switches mit einem MC-LAG-Interconnect konfiguriert sind, wird empfohlen, die NAS-Schnittstelle über LACP-Bündelungen mithilfe von Link Aggregation Groups (LAG) zu konfigurieren. Die LACP-Bündelung ist ein Prozess, bei dem zwei oder mehr Netzwerkschnittstellen zu einer einzigen Schnittstelle zusammengefasst werden. Eine LACP-Bündelung ermöglicht Performanceverbesserungen und Redundanz, indem der Netzwerkdurchsatz und die Bandbreite erhöht werden. Wenn eine der Schnittstellen der Bündelung ausfällt, werden die anderen Schnittstellen für die Aufrechterhaltung einer stabilen Verbindung eingesetzt.

Schritte

1. Wählen Sie **Hardware** > **[Appliance]** > **Ports** aus.
2. Wählen Sie auf dem Node, auf dem Sie eine LACP-Bündelung (Link Aggregate Control Protocol) für NAS-Datenverkehr erstellen möchten, in der Liste der Anschlüsse zwei bis vier Anschlüsse mit derselben Geschwindigkeit aus.

   ANMERKUNG: Die Konfiguration ist über den Peer-Node hinweg symmetrisch.

3. Wählen Sie **Link Aggregation** > **Aggregate Links** aus.
4. Optional können Sie eine Beschreibung für die Bündelung angeben.
5. Wählen Sie **Aggregate** aus.
6. Scrollen Sie durch die Liste der Anschlüsse und suchen Sie den Namen der erstellten Bündelung.

   ANMERKUNG: Sie müssen den Namen der Bündelung auswählen, wenn Sie den NAS-Server erstellen.

Erstellen eines ausfallsicheren Netzwerks

Info über diese Aufgabe

Ein ausfallsicheres Netzwerk (FSN, Fail-Safe Network) sollte erstellt werden, wenn die ToR-Switches (Top-of-Rack) nicht mit einer MC-Lag-Verbindung konfiguriert wurden. Ein FSN erweitert das Link-Failover auf das Netzwerk, indem Redundanz auf Switchebene bereitgestellt wird. Ein FSN kann auf einem Port, einer Link Aggregation oder einer beliebigen Kombination aus beidem konfiguriert sein.

Schritte

1. Wählen Sie **Hardware** > **[Appliance]** > **Ports** aus.
2. Wenn Sie aggregierte Links für das FSN verwenden möchten, erstellen Sie zunächst die Link Aggregation-Gruppen. Weitere Informationen finden Sie unter Erstellen von LACP-Bonds für NAS-Datenverkehr.
3. Wählen Sie zwei Ports oder zwei Link Aggregations oder eine Kombination aus einem Port und einer Link Aggregation aus, die Sie für das FSN auf Node A verwenden möchten, und wählen Sie **FSN** > **FSN erstellen** aus.
4. Wählen Sie im Bereich **FSN erstellen** aus, welche Ports oder Link Aggregation als primäres (aktives) Netzwerk verwendet werden sollen.

   ANMERKUNG: Der primäre Port kann nicht geändert werden, sobald er zum Erstellen eines NAS-Servers verwendet wird.

5. Fügen Sie optional eine Beschreibung des ausfallsicheren Netzwerks hinzu.
6. Klicken Sie auf **Erstellen**.

   PowerStore Manager erstellt automatisch einen Namen für das ausfallsichere Netzwerk im folgenden Format: „BaseEnclosure-<Node>-fsn<nextLACPbondcreated>“
   - BaseEnclosure ist konstant.
   - Node ist der Node, der in der Liste **Node-Module-Name** angezeigt wird.
   - nextLACPbondcreated ist ein numerischer Wert, der durch die Reihenfolge bestimmt wird, in der die Bündelung in PowerStore erstellt wurde, beginnend mit Null für die erste erstellte Bündelung.

   Das erste FSN, das im PowerStore Manager auf Node A erstellt wurde, hätte den Namen BaseEnclosure-NodeA-FSN0.

   Dasselbe FSN wird auf dem gegenüberliegenden Node konfiguriert. Wenn Sie das FSN beispielsweise auf Node A konfiguriert haben, wird dasselbe FSN auf Node B konfiguriert.
7. Erstellen Sie einen NAS-Server mit dem ausfallsicheren Netzwerk.

   Das ausfallsichere Netzwerk wird beim Erstellen des NAS-Servers im PowerStore Manager auf den NAS-Server angewendet. Weitere Informationen finden Sie unter Erstellen eines NAS-Servers für SMB-Dateisysteme.

Erstellen von SMB-Freigaben

Führen Sie die folgenden Verfahren aus, damit Sie SMB-Freigaben in PowerStore erstellen können:

1. Erstellen von NAS-Servern mit SMB-Protokoll
2. Erstellen eines Dateisystems für SMB-Freigaben

Dokumentationsressourcen

Weitere Informationen finden Sie in den folgenden Themen:

Tabelle 2. Dokumentationsressourcen

Dokument	Beschreibung	Position
PowerStore T und Q – Netzwerkleitfaden für Storage-Services	Enthält Informationen zur Netzwerkplanung und -konfiguration.	dell.com/powerstoredocs
PowerStore – Handbuch für die Konfiguration von NFS	Enthält Informationen, die zum Konfigurieren von NFS-Exporten mit PowerStore Manager erforderlich sind.	
Whitepaper zu Dateifunktionen von PowerStore	Beschreibt die Funktionen und Protokolle, die von der Dell PowerStore-Dateiarchitektur unterstützt werden.	
PowerStore-Onlinehilfe	Enthält kontextsensitive Informationen für die in PowerStore Manager geöffnete Seite.	In PowerStore Manager integriert

2

Erstellen von NAS-Servern

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Übersicht über die Konfiguration von NAS-Servern

Bevor Sie den Datei-Storage auf dem PowerStore-Cluster bereitstellen können, muss ein NAS-Server auf dem System ausgeführt werden. Ein NAS-Server ist ein Dateiserver, der das SMB-Protokoll und/oder NFS-Protokoll verwendet, um Daten für Netzwerkhosts freizugeben. Außerdem katalogisiert, organisiert und optimiert er die Lese- und Schreibvorgänge auf den zugehörigen Dateisystemen.

In diesem Dokument wird die Konfiguration eines NAS-Servers mit dem SMB-Protokoll beschrieben, auf dem Dateisysteme mit SMB-Freigaben erstellt werden können.

Erstellen eines NAS-Servers für SMB-Dateisysteme

Sie müssen einen NAS-Server erstellen, bevor Sie Dateisysteme erstellen.

Voraussetzungen

Ermitteln Sie die folgenden Informationen:

- Netzwerkport, IP-Adresse, Subnetzmaske/Präfixlänge und Gatewayinformationen für den NAS-Server.

  ANMERKUNG: Die IP-Adresse und die Subnetzmaske/Präfixlänge sind obligatorisch.

- VLAN-ID, wenn der Switchport VLAN-Tagging unterstützt.

  ANMERKUNG: Sie können keine VLANs wiederverwenden, die für die Management- und Storage-Netzwerke verwendet werden.

- Wenn Sie einen eigenständigen NAS-Server konfigurieren, rufen Sie die Arbeitsgruppe und den NetBIOS-Namen ab. Definieren Sie dann, was für den eigenständigen lokalen Administrator des SMB-Serverkontos verwendet werden soll.
- Wenn Sie den NAS-Server zu Active Directory (AD) hinzufügen, stellen Sie sicher, dass NTP auf dem Speichersystem konfiguriert ist. Beziehen Sie dann den SMB-Systemnamen (für den Zugriff auf SMB-Freigaben), den Windows-Domainnamen sowie den Nutzernamen und das Kennwort eines Domainadministrators oder -nutzers, der ausreichende Zugriffsrechte für die Domain hat, um Active Directory beizutreten.

Schritte

1. Wählen Sie die Optionen **Storage** > **NAS Servers** aus.
2. Wählen Sie **Erstellen** aus.
3. Führen Sie die Anweisungen des Assistenten **Create NAS Server** aus.

Bildschirm „Wizard“	Beschreibung
Details	• Name des NAS-Servers • Beschreibung des NAS-Servers

Bildschirm „Wizard“	Beschreibung
	• Netzwerkschnittstelle – Wählen Sie eine Link Aggregation-Gruppe aus (siehe Erstellen der Netzwerkschnittstelle für NAS-Datenverkehr). **ANMERKUNG:** Wenn Sie ein ausfallsicheres Netzwerk (FSN, Fail-Safe Network) auswählen, kann das primäre Netzwerk nicht mehr geändert werden, sobald ein NAS-Server mithilfe des FSN konfiguriert wurde. • Netzwerkinformationen
Sharing Protocol	**Select Sharing Protocol** Wählen Sie **SMB** aus. **ANMERKUNG:** Wenn Sie sowohl ein SMB- als auch ein NFS-Protokoll auswählen, wird der NAS-Server zur Unterstützung von Multiprotokoll automatisch aktiviert. Die Multiprotokollkonfiguration wird in diesem Dokument nicht beschrieben. **Windows Server Settings** Wählen Sie **Standalone** aus, um einen eigenständigen SMB-Server zu erstellen, oder wählen Sie **Join to the Active Directory Domain** aus, um einen SMB-Server als Domainmitglied zu erstellen. Wenn Sie den NAS-Server zu Active Directory hinzufügen, klicken Sie optional auf **Erweitert**, um den Standard-NetBios-Namen und die Organisationseinheit zu ändern. **DNS** Wenn Sie **Join to the Active Directory Domain** ausgewählt haben, ist es zwingend erforderlich, einen DNS-Server hinzuzufügen. Aktivieren Sie optional DNS, wenn Sie einen DNS-Server für Ihren eigenständigen SMB-Server verwenden möchten. **User Mapping** Die Seite **User Mapping** wird angezeigt, wenn Sie die Active Directory-Domain hinzugefügt haben. Behalten Sie die Standardeinstellung **Enable automatic mapping for unmapped Windows accounts/users** bei, um den Beitritt zur Active Directory-Domain zu unterstützen. Die automatische Zuordnung ist erforderlich, wenn Sie der Active Directory-Domain beitreten.
Schutz-Policy	Wählen Sie optional eine Schutz-Policy aus der Liste aus.
File-QoS-Policy	Wählen Sie optional eine Datei-QoS-Policy aus der Liste aus.
Zusammenfassung	Überprüfen Sie den Inhalt, und wählen Sie **Previous** aus, um zurück zu navigieren und Änderungen vorzunehmen.

4. Wählen Sie **Create NAS Server** aus.
   Nachdem der Server erstellt wurde, wird das Fenster **Status** geöffnet und Sie werden zur Seite **NAS-Server** umgeleitet.

Nächste Schritte

Nachdem Sie den NAS-Server für SMB erstellt haben, können Sie mit der Konfiguration der Servereinstellungen fortfahren oder Dateisysteme erstellen.

Wählen Sie den NAS-Server aus, um die Konfiguration fortzusetzen, oder ändern Sie die Einstellungen des NAS-Servers.

Ändern von NAS-Servereinstellungen

Nachdem Sie einen NAS-Server erstellt haben, können Sie Konfigurationsänderungen an diesem vornehmen.

Info über diese Aufgabe

ANMERKUNG: Wenn eine Remotesystemverbindung besteht, kann es bis zu 15 Minuten dauern, bis Änderungen der NAS-Serverkonfiguration auf dem Remote-NAS-Server wiedergegeben werden.

Schritte

1. Wählen Sie die Optionen **Storage** > **NAS Servers** > **[NAS-Server]** aus.
2. Konfigurieren Sie auf der Seite **Network** optional die Netzwerkschnittstellen oder die Routen zu externen Netzwerken, wie unter Konfigurieren von NAS-Servernetzwerken beschrieben.
3. Auf der Seite **Naming Services** können Sie optional die DNS-Server für den NAS-Server hinzufügen, ändern oder löschen.

   ANMERKUNG: DNS für NAS-Server, die die SMB-Dateifreigabe unterstützen und mit einem Active Directory (AD) verbunden sind, können nicht deaktiviert werden.

4. Auf der Seite **Protokollfreigaben**:
   - Wählen Sie die Karte **SMB-Server** aus, um die Unterstützung für Windows-Freigaben zu aktivieren bzw. zu deaktivieren oder den vom SMB-Server verwendeten Suchtyp zu ändern.

     ANMERKUNG: Wenn Sie den **Windows Server Type** von **Standalone** in **Join to the Active Directory Domain**, müssen Sie zur Registerkarte **User Mapping** wechseln und **Enable automatic mapping for unmapped Windows accounts/users** auswählen.

   - Wählen Sie die Karte **FTP** aus, um FTP oder SFTP zu aktivieren oder zu deaktivieren, die FTP- oder SFTP-Eigenschaften zu ändern und die Nutzerauthentifizierung, ein Nutzerstammverzeichnis und die Authentifizierungsmeldungseinstellungen zu konfigurieren. Weitere Informationen finden Sie unter Konfigurieren des FTP-Freigabeprotokolls.
   - Wählen Sie **Nutzerzuordnung** aus, um dem Server die Verwendung der automatischen Zuordnung für nicht zugeordnete Windows-Nutzerkonten oder des Standardkontos für nicht zugeordnete Windows-Nutzerkonten zu ermöglichen.
5. Aktivieren oder deaktivieren Sie NDMP auf der Seite **Schutz**.

   Weitere Informationen finden Sie unter Aktivieren von NDMP-Schutz und -Ereignissen.
6. Gehen Sie auf der Registerkarte **Sicherheit und Ereignisse** wie folgt vor:
   - Wählen Sie **Kerberos** aus, um den Active Directory-Bereich für die Kerberos-Authentifizierung hinzuzufügen oder einen nutzerdefinierten Kerberos-Bereich zu konfigurieren.
   - Wählen Sie **Antivirus** aus, um den Virenschutzservice zu aktivieren oder zu deaktivieren und die Virenschutz-Konfigurationsdatei abzurufen oder hochzuladen.

   Weitere Informationen finden Sie unter Konfigurieren der NAS-Serversicherheit.

3

Weitere Funktionen des NAS-Servers

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Konfigurieren des FTP- oder SFTP-Freigabeprotokolls

Sie können FTP oder SFTP (FTP over SSH) konfigurieren, nachdem der NAS-Server erstellt wurde.

Voraussetzungen

Der passive FTP-Modus wird nicht unterstützt.

Info über diese Aufgabe

Der FTP-Zugriff kann mit den gleichen Methoden wie SMB authentifiziert werden. Nachdem die Authentifizierung abgeschlossen wurde, erfolgt der Zugriff genauso wie SMB zu Sicherheits- und Berechtigungszwecken. Wenn das Format `domain@user` oder `domain\user` ist, wird die SMB-Authentifizierung verwendet. SMB-Authentifizierung verwendet den Windows Domain Controller.

Schritte

1. Wählen Sie die Optionen **Storage** > **NAS Servers** > **[NAS-Server]** > **Sharing Protocols** > **FTP** aus.
2. Wenn die Option „Disabled“ unter **FTP** aktiviert ist, schieben Sie die Schaltfläche, um zu **Enable** zu wechseln.
3. Aktivieren Sie optional auch SSH FTP. Wenn die Option „Disabled“ unter **SFTP** aktiviert ist, schieben Sie die Schaltfläche, um zu **Enable** zu wechseln.
4. Wählen Sie aus, welcher Typ von authentifizierten Nutzern Zugriff auf die Dateien haben soll.
5. Zeigen Sie optional die **Home Directory and Audit**-Optionen an.
   - Aktivieren oder deaktivieren Sie die **Home directory restrictions**. Geben Sie das **Default home directory** ein, wenn diese Option deaktiviert ist.
   - Aktivieren oder deaktivieren Sie die Option **Enable FTP/SFTP Auditing**. Wenn diese Option aktiviert ist, geben Sie den Verzeichnispfad ein, in dem die Protokolldateien gespeichert werden sollen, und die maximale Größe, die für die Protokolldatei zulässig ist.
6. Optional können Sie auf **Show Messages** klicken und eine standardmäßige Willkommensnachricht und die Tagesbotschaft eingeben.
7. Optional können Sie die **Access Control List** anzeigen und eine Liste der Nutzer, Gruppen und Hosts hinzufügen, denen FTP-Zugriff gewährt oder verweigert wird.
8. Klicken Sie auf **Anwenden**.

Konfigurieren von NAS-Servernetzwerken

Sie können NAS-Servernetzwerke ändern oder konfigurieren.

Konfigurieren Sie Folgendes für NAS-Servernetzwerke:

- Dateischnittstellen
- Routen zu externen Services wie Hosts

Konfigurieren von Dateischnittstellen für einen NAS-Server

Sie können die Dateischnittstellen für einen NAS-Server konfigurieren, nachdem der Server zu PowerStore hinzugefügt wurde.

Info über diese Aufgabe

Sie können weitere Dateischnittstellen hinzufügen und festlegen, welche Sie bevorzugt verwenden möchten. Außerdem können Sie festlegen, welche Schnittstelle für Produktions- und Backupzwecke oder für IPv4 bzw. IPv6 verwendet werden soll.

Schritte

1. Wählen Sie die Optionen **Storage** > **NAS Servers** > **[NAS-Server]** aus.
2. Klicken Sie auf der Seite **Netzwerk** auf **Hinzufügen**, um dem NAS-Server eine weitere Dateischnittstelle hinzuzufügen.
3. Geben Sie die Eigenschaften der Dateischnittstelle ein.

   ANMERKUNG: Sie können keine VLANs wiederverwenden, die für die Management- und Storage-Netzwerke genutzt werden.

4. Sie können die folgenden Schritte für eine Dateischnittstelle durchführen, indem Sie eine Dateischnittstelle aus der Liste auswählen. Wählen Sie Folgendes aus:

Option	Beschreibung
Ändern	Zum Ändern der Eigenschaften der Dateischnittstelle.
Löschen	Zum Löschen der Dateischnittstelle vom NAS-Server.
Ping	Zum Testen der Konnektivität zwischen dem NAS-Server und einer externen IP-Adresse.
Bevorzugte Schnittstelle	Zum Festlegen der standardmäßig von PowerStore zu verwendenden Schnittstelle, wenn mehrere Produktions- und Backupschnittstellen definiert wurden.

Konfigurieren von Routen für die Dateischnittstelle für externe Verbindungen

Sie können die Routen konfigurieren, die das Dateisystem für externe Verbindungen verwendet.

Voraussetzungen

Sie können die Option **Ping** von der Karte **File Interface** verwenden, um festzustellen, ob die Dateischnittstelle Zugriff auf die externe Ressource hat.

Info über diese Aufgabe

Normalerweise werden die NAS-Serverschnittstellen mit einem Standardgateway konfiguriert, das zur Weiterleitung von Anforderungen von einer NAS-Serverschnittstelle an externe Services verwendet wird.

Führen Sie die folgenden Schritte durch:

- Wenn Sie granularere Routen zu externen Services konfigurieren müssen.
- Wenn Sie eine Route hinzufügen, um von einer bestimmten Schnittstelle über ein bestimmtes Gateway auf einen Server zuzugreifen.

Schritte

1. Wählen Sie **Storage** > **NAS-Server** > **[NAS-Server]** > **Netzwerk** > **Routen zu externen Services** aus.
2. Klicken Sie auf **Add**, um die Routeninformationen im Assistenten **Add Route** einzugeben.

Aktivieren des NDMP-Backups

Sie können mithilfe von NDMP standardmäßige Backups für die NAS-Server konfigurieren. Das Network Data Management Protocol (NDMP) bietet einen Standard zur Sicherung von Dateiservern in einem Netzwerk. Sobald NDMP aktiviert wurde, kann eine DMA-

Anwendung (Data Management Application) eines Drittanbieters, z. B. Dell Networker, das PowerStore-NDMP über die IP-Adresse des NAS-Servers erkennen.

Info über diese Aufgabe

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

PowerStore unterstützt:

- 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. Wählen Sie die Optionen **Storage** > **NAS-Server** > **[NAS-Server]** > **Schutz und Ereignisse** aus.
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.

Konfigurieren der NAS-Serversicherheit

Sie können den NAS-Server mit **Kerberos**- oder **Virenschutz**-Sicherheit konfigurieren.

Die Konfiguration der NAS-Serversicherheit umfasst die folgenden Optionen:

- Kerberos
- Virenschutz

Konfigurieren der Kerberos-Sicherheit für den NAS-Server

Sie können den NAS-Server mit Kerberos-Sicherheit konfigurieren.

Info über diese Aufgabe

Fügen Sie den SMB-Server zur Active Directory-Domain hinzu, bevor Sie Kerberos konfigurieren.

Wenn Sie den NAS-Server nur für SMB konfigurieren, benötigen Sie keine Keytab-Datei. Die Keytab-Datei ist nur für die Konfiguration von Secure NFS erforderlich.

Schritte

1. Wählen Sie die Optionen **Storage** > **NAS Servers** > **[NAS-Server]** > **Security** > **Kerberos** aus.
2. Wenn die Option deaktiviert ist, schieben Sie die Schaltfläche, um zu **Enabled** zu wechseln.
3. Geben Sie den Namen des Bereichs im Feld **Realm** ein.
4. Geben Sie die Kerberos-IP-Adresse ein, und klicken Sie auf **Add**.
5. Geben Sie den TCP-Port ein, der für Kerberos verwendet werden soll. Der Standardport ist 88.
6. Klicken Sie auf **Apply**.

Verstehen von Common Anti Virus Agent (CAVA)

Common AntiVirus Agent (CAVA) bietet eine Virenschutzlösung für Clients, die einen NAS-Server verwenden. Sie nutzt ein Branchenstandard-SMB-Protokoll in einer Microsoft Windows Server-Umgebung. CAVA nutzt Virenschutzsoftware von Drittanbietern, um bekannte Viren zu identifizieren und zu eliminieren, bevor sie Dateien im Speichersystem infizieren können.

Virenschutzsoftware ist wichtig, auch wenn das Speichersystem aufgrund seiner Architektur gegen das Eindringen von Viren resistent ist. Der NAS-Server führt mithilfe eines eingebetteten Betriebssystems den Datenzugriff in Echtzeit aus. Drittanbieter können auf diesem Betriebssystem keine Programme ausführen, die Viren enthalten. Obwohl die Betriebssystemsoftware gegen Viren geschützt ist, muss auf Windows-Clients, die auf das Speichersystem zugreifen, ebenfalls ein Virenschutz installiert sein. Der Virenschutz auf Clients reduziert das Risiko, dass sie eine infizierte Datei auf dem Server speichern, und schützt sie, wenn sie eine infizierte Datei öffnen. Diese Virenschutzlösung besteht aus einer Kombination aus Betriebssystemsoftware, einem CAVA-Agenten und einer Antivirus-Engine eines Drittanbieters. Die CAVA-Software und eine Drittanbieter-Virenschutz-Engine muss auf einem Windows-Server in der Domain installiert sein.

Informationen zu den CEE-CAVA-Versionen, die für PowerStore erforderlich sind, finden Sie in den *Versionshinweisen zum Common Event Enabler* auf der Dell Technologies Supportwebsite. Weitere Informationen zu CAVA, das Teil des Common Event Enabler (CEE) ist, finden Sie im Abschnitt *Verwenden des Common Event Enabler auf Windows-Plattformen* auf der Dell Technologies Supportwebsite.

Managen von Common Anti Virus Agent (CAVA)

Sie können CAVA aktivieren und konfigurieren, wenn Sie Ihre SMB-Freigaben mit einem Virenschutz versehen möchten.

Voraussetzungen

- Einen Windows-Server, auf dem ein kompatibles A/V-Produkt ausgeführt wird. Weitere Informationen finden Sie in der eLab CEE_CAVA Support Matrix.
- Installieren Sie die EMC_CEE_Pack_8_x_x_x 32- oder 64-Bit-CAVA-Anwendung auf dem Windows-A/V-Server.

  ANMERKUNG: Navigieren Sie nach der Installation der Anwendung zum Abschnitt „Anmelden“ des EMC CAVA-Dienstes und weisen Sie ein Administratornutzerkonto für die Domain als Virenschutznutzer zu. Starten Sie den Dienst anschließend neu.

- Erstellen Sie einen Nutzer im Active Directory.
- Überprüfen Sie, ob SMB auf dem NAS-Server aktiviert ist.

Info über diese Aufgabe

Ab PowerStore Manager 4.x können Sie CAVA konfigurieren, Berechtigungen für die Virenprüfung zuweisen, die CAVA-Konfiguration und den CAVA-Status anzeigen und nach Bedarf Dateisystem-Scans über den PowerStore Manager ausführen.

ANMERKUNG: Sie können diese Aktionen auch über die CLI und REST API ausführen.

Schritte

1. Rufen Sie in PowerStore Manager die Registerkarte **Storage** > **NAS-Server** > **[NAS-Server]** > **Sicherheit und Ereignisse** > **Antivirus** auf.
2. Wählen Sie **Konfigurieren** aus, um das Dialogfeld **Virenschutzeinstellungen konfigurieren** anzuzeigen.
3. Legen Sie die folgenden Parameter fest: die IP-Adresse, die Dateierweiterungen, die gescannt werden sollen, und die Dateierweiterungen, die ausgeschlossen werden sollen.
   - IP-Adresse – Legen Sie die IP-Adresse oder den FQDN des Windows-A/V-Servers fest.
   - Zu scannende Dateierweiterungen – Verwenden Sie das folgende Format: *.txt, *.docx, *.exe.
   - Auszuschließende Dateierweiterungen: Verwenden Sie das gleiche Format wie für die zu scannenden Dateitypen.
4. Wählen Sie **Erweiterte Optionen** aus, um die folgenden Parameter festzulegen:
   - Maximale Dateigröße
   - Erhebungszeit
   - Aktion zum Herunterfahren
   - Oberer Grenzwert
   - Unterer Grenzwert
   - MSRPC User
   - HTTP-Port
   - RPC-Wiederholungs-Timeout
   - RPC-Anfrage-Timeout
5. Wählen Sie **Erstellen** aus.
   Der Virenschutzservice wird als aktiv gekennzeichnet.
6. Wählen Sie das Symbol „Bearbeiten“ aus, um das Dialogfeld **Eigenschaften** zu öffnen.
7. Wählen Sie **Aktivieren** aus, um die Virenüberprüfung zu aktivieren, und wählen Sie dann **Anwenden** aus.

8. Um dem NAS-Server die Rechte für die EMC Virenprüfung zu erteilen, wählen Sie die Registerkarte **Kontoberechtigungen** aus und fügen Sie das Domänen-Virenschutznutzerkonto hinzu. Verwenden Sie das Format Domain\Nutzername (z. B. Lab\Virenschutz).

   ANMERKUNG: Dieses Konto ist dasselbe Nutzerkonto, das im EMC CAVA-Dienst auf dem Windows-Server ausgewählt ist.

9. Um Details zur Virenschutzsoftware und zum Onlinestatus anzuzeigen, wählen Sie die Registerkarte **Auditinformationen** aus.
10. Wählen Sie auf der Registerkarte **Zu scannende Dateisysteme** die Dateisysteme aus, die Sie scannen möchten, und wählen Sie dann **Start** aus, um den Scan zu starten.
11. Wenn der Scan Offlinedateien enthalten soll, wählen Sie die Option in der angezeigten Meldung und dann **Scan starten** aus.
12. Um den Scanfortschritt zu überwachen, wählen Sie die Registerkarte **Status** aus.
13. Wenn der Scan abgeschlossen ist, wird eine Statusmeldung angezeigt.
14. Um einen Scan für ein Dateisystem zu beenden, wählen Sie das Dateisystem und dann die Option **Scan stoppen** aus und bestätigen Sie den Vorgang dann in der angezeigten Meldung.
15. Wenn Sie CAVA mithilfe einer Konfigurationsdatei (viruschecker.conf) konfigurieren möchten, können Sie die aktuelle Datei herunterladen und anpassen oder eine neue Konfigurationsdatei hochladen, indem Sie im Dialogfeld **Eigenschaften** die Option **Konfiguration hochladen/abrufen** auswählen.

    ANMERKUNG: Weitere Informationen zu den Parametern in der viruschecker.conf-Datei finden Sie unter Konfigurierbare Virenschutzparameter.

Konfigurierbare Virenschutzparameter

In der folgenden Tabelle sind die Parameter aufgeführt, die in der CAVA-Konfigurationsdatei `viruschecker.conf` konfiguriert werden können. Sie können die Konfigurationsdatei erstellen und dann in PowerStore hochladen.

Tabelle 3. Virenschutzparameter

Parameter	Beschreibung	Obligatorisch	Beispiel
`addr=`	Legt die IP-Adressen des/der CAVA-Server(s) fest.	Ja	`addr=10.205.20.130`
`masks=`	Konfiguriert Dateierweiterungen, die gescannt werden.	Ja	`masks=*.exe:*.docx:*.com`
`excl=`	Listet Dateierweiterungen auf, die während des Scans ausgeschlossen werden.	Nein	`excl=pagefile.sys`
`maxsize=<n>`	Ganze Zahl. Legt die maximale Größe für Dateien fest, die überprüft werden. Dateien, die größer sind, werden nicht geprüft.	Nein	`maxsize=4294967290`
`surveyTime=<n>`	Legt das Zeitintervall (Sekunden) fest, in dem alle Virenschutzserver gescannt werden, um zu ermitteln, ob sie online oder offline sind. Wenn kein Virenschutzserver antwortet, beginnt der Prozess des Herunterfahrens mithilfe des konfigurierten Parameters für das Herunterfahren (siehe nächste Zeile).	Nein	`surveyTime=600`
`shutdown=`	Gibt an, welche Aktion zum Herunterfahren erfolgen soll, wenn kein Server zur Verfügung steht. Der Standardwert ist `Allow Access`.	Nein	`Allow Access`, `Stop_SMB_Access`, `Disable_Virus_Checker`
`highWaterMark=<n>`	Warnt das System, wenn die Anzahl der derzeit verarbeiteten Anforderungen `highWaterMark` überschreitet.	Nein	`highWaterMark=200`

Tabelle 3. Virenschutzparameter (fortgesetzt)

Parameter	Beschreibung	Obligatorisch	Beispiel
`lowWaterMark=<n>`	Warnt das System, wenn die Anzahl der verarbeiteten Anforderungen niedriger ist als `lowWaterMark`.	Nein	`lowWaterMark=50`

`msrcpuser=`	Gibt den Namen an, der entweder einem einfachen Nutzerkonto zugewiesen ist oder einem Nutzerkonto, das Teil einer Domain ist, unter der der CAVA-Service auf der CEE-Maschine ausgeführt wird.	Nein	Benutzerkonto:
			`msrpcuser=user1`
			Domain-\Nutzerkonto:
			`msrpcuser=CEE1/user1`

`httpport=`	Gibt die HTTP-Portnummer auf der CEE-Maschine an, die das System verwendet.	Nein	`httpport=12228`
`RPCRetryTimeout`	Legt das Timeout (in Millisekunden) der RPC-Wiederholung fest.	Nein	`RPCRetryTimeout=4000 milliseconds`
`RPCRequestTimeout`	Legt das Timeout (in Millisekunden) der RPC-Anforderung fest. Wenn ein RPC an den CAVA-Server gesendet wird und der Server nach dem RPCRetryTimeout antwortet, versucht der NAS-Server es erneut, bis RPCRequestTimeout erreicht ist, und wechselt dann zum nächsten verfügbaren CAVA-Server.	Nein	`RPCRequestTimeout=20000 milliseconds`
`reference time`	Aktiviert einen Scan beim ersten Lesevorgang. Liegt der letzte Zugriffszeitpunkt einer Datei vor der `reference time`, wird die Datei beim Zugriff an den Virus Checker gesendet, bevor dem Client der Zugriff gewährt wird.	Nein	`reference_time=2022-10-27T18:30:00`

4

Erstellen von Dateisystemen und SMB-Freigaben

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Erstellen eines Dateisystems

Es muss ein Dateisystem auf dem NAS-Server erstellt werden, bevor Sie eine SMB-Freigabe erstellen können.

Voraussetzungen

Vergewissern Sie sich, dass ein NAS-Server für die Unterstützung des SMB-Protokolls konfiguriert wurde, wie unter Konfigurieren von NAS-Servern beschrieben.

Schritte

1. Wählen Sie die Optionen **Storage** > **File Systems** aus, und klicken Sie auf **Create**.
2. Fahren Sie dann mit dem Assistenten **Create File System** fort.

Option	Beschreibung
Typ auswählen	Wählen Sie **Allgemein** als Dateisystemtyp aus.
Select NAS Server	Wählen Sie einen NAS-Server aus, der für SMB aktiviert ist.
Advanced SMB Settings	Wählen Sie optional aus den folgenden Optionen: • **Synchrone Schreibvorgänge aktiviert** • **Oplocks aktiviert** • **Benachrichtigung bei Schreibvorgang aktiviert** • **Benachrichtigung bei Zugriff aktiviert** • **Enable SMB Events Publishing** Weitere Informationen finden Sie unter Erweiterte Dateisystemeinstellungen für SMB-Freigaben.
Details des Dateisystems	Geben Sie den Namen und die Größe des Dateisystems an. Die Größe des Dateisystems kann zwischen 3 GB und 256 TB betragen. **ANMERKUNG:** Alle Thin-Dateisysteme haben unabhängig von der Größe 1,5 GB, die bei der Erstellung für Metadaten reserviert sind. Nach der Erstellung eines 100-GB-Thin-Dateisystems zeigen das PowerStore T-Modell und PowerStore Q-Modell sofort an, dass 1,5 GB verwendet werden. Wenn das Dateisystem auf einem Host gemountet ist, werden 98,5 GB nutzbare Kapazität angezeigt. Dies liegt daran, dass der Metadatenspeicherplatz aus der nutzbaren Dateisystemkapazität reserviert ist.
Aufbewahrung auf Dateiebene	Wählen Sie optional den Dateiaufbewahrungstyp aus: • Enterprise (FLR-E) – Schützt Inhalte vor Änderungen, die von NutzerInnen über CIFS und FTP vorgenommen werden. Ein Administrator kann ein FLR-E-Dateisystem löschen, das geschützte Dateien enthält.

Option	Beschreibung
	• Compliance (FLR-C) – Schützt Inhalte vor Änderungen, die von NutzerInnen und AdministratorInnen vorgenommen werden, und entspricht den Anforderungen der SEC-Regel 17a-4(f). DAS FLR-C-Dateisystem kann nur gelöscht werden, wenn es keine geschützten Dateien enthält. **ANMERKUNG:** FLR-Status und Dateiaufbewahrungstyp werden bei der Dateisystemerstellung festgelegt und können nicht geändert werden. Legen Sie die Aufbewahrungszeiträume fest: • Minimum – Gibt den kürzesten Zeitraum an, für den Dateien gesperrt werden können (Standardwert ist 1 Tag). • Standard – Wird verwendet, wenn eine Datei gesperrt ist und keine Aufbewahrungsfrist angegeben ist. • Maximum: Gibt den längsten Zeitraum an, für den Dateien gesperrt werden können.
SMB-Freigabe	Konfigurieren Sie optional die anfängliche SMB-Freigabe. Sie können dem Dateisystem nach der anfänglichen Dateisystemkonfiguration Freigaben hinzufügen. Weitere Informationen zu den Optionen für die SMB-Freigabe finden Sie unter Erstellen einer SMB-Freigabe.
Schutz-Policy	Geben Sie optional eine Schutz-Policy für das Dateisystem an. PowerStore unterstützt Snapshots und Replikation für Datei-Storage-Schutz.
File-QoS-Policy	Wählen Sie optional eine Datei-QoS-Policy für das Dateisystem aus. **ANMERKUNG:** Wenn die ausgewählte Policy eine Bandbreite festlegt, die die für den NAS-Server festgelegte maximale Bandbreite überschreitet, entspricht die effektive Bandbreite der maximalen Bandbreite des Servers.
Zusammenfassung	Überprüfen Sie die Zusammenfassung. Gehen Sie zurück, um die erforderlichen Aktualisierungen vorzunehmen.

3. Klicken Sie auf **Create File System**.
Das Dateisystem wird in der Liste „File System“ angezeigt. Wenn Sie eine SMB-Freigabe erstellt haben, wird sie in der Liste „SMB Share“ angezeigt.

Erweiterte Dateisystemeinstellungen für SMB

Sie können bei der Erstellung eines Dateisystems erweiterte Einstellungen zu SMB-fähigen Dateisystemen hinzufügen.

Tabelle 4. Erweiterte Dateisystemeinstellungen für SMB

Einstellung	Beschreibung
Synchrone Schreibvorgänge aktiviert	Wenn Sie die Option für synchrone Schreibvorgänge für ein Windows- (SMB-) oder Multiprotokoll-Dateisystem aktivieren, werden die Schreibvorgänge beim Speichern im Speichersystem sofort synchron durchgeführt – unabhängig davon, welcher Schreibvorgang im SMB-Protokoll festgelegt ist. Durch die Aktivierung synchroner Schreibvorgänge können Sie Datenbankdateien (z. B. MySQL) auf SMB-Freigaben des Speichersystems speichern und darauf zugreifen. Diese Option sorgt dafür, dass sämtliche Schreibvorgänge auf den Freigaben synchron ablaufen. Damit sinkt das Risiko eines Datenverlusts oder einer Datenbeschädigung unter verschiedenen Szenarien, wie beispielsweise einem Stromausfall. Diese Option ist standardmäßig deaktiviert. **ANMERKUNG:** Die Option für synchrone Schreibvorgänge kann erhebliche Auswirkungen auf die Performance haben. Sie sollte nur aktiviert werden, wenn Sie Windows-Dateisysteme als Speicher für Datenbankanwendungen einsetzen möchten.
Oplocks aktiviert	(Standardmäßig aktiviert) Oplocks (Opportunistic File Locks, auch bezeichnet als Level-1-Oplocks) ermöglichen SMB-Clients das lokale Puffern von filebasierten Daten, bevor diese an einen Server gesendet werden. SMB-Clients können dann lokal mit Dateien arbeiten und Änderungen am Speichersystem regelmäßig kommunizieren, statt jeden Vorgang über das Netzwerk an das Speichersystem weiterleiten zu müssen. Diese Funktion ist für Windows- (SMB-) und Multiprotokoll-Dateisysteme standardmäßig aktiviert. Solange mit der Anwendung keine kritischen Daten verarbeitet werden oder andere konkrete Gründe gegen diesen Modus

Tabelle 4. Erweiterte Dateisystemeinstellungen für SMB (fortgesetzt)

Einstellung	Beschreibung
	sprechen, sollte oplocks aktiviert bleiben. Die folgenden oplocks-Implementierungen werden unterstützt: ● Level-II-Oplocks, die einen Client darüber informieren, dass mehrere Clients auf eine Datei zugreifen, jedoch kein Client diese bisher geändert hat. Ein Level-II-Oplock gestattet dem Client Schreibvorgänge und das Abrufen von Dateiattributen mithilfe von zwischengespeicherten oder lokalen Read-ahead-Daten. Alle anderen Dateizugriffsanfragen müssen an den Server gesendet werden. ● Exklusives Oplock, das einen Client darüber informiert, dass er der einzige Client ist, der die Datei öffnet. Ein exklusives Oplock ermöglicht einem Client bis zum Schließen der Datei die Durchführung aller Dateivorgänge mithilfe von zwischengespeicherten oder Read-ahead-Daten. Wenn die Datei geschlossen wird, muss der Server mit den am Dateistatus vorgenommenen Änderungen (Inhalte und Attribute) aktualisiert werden. ● Batch-Oplock, das einen Client darüber informiert, dass er der einzige Client ist, der die Datei öffnet. Ein Batch-Oplock gestattet einem Client die Durchführung aller Dateivorgänge mithilfe von zwischengespeicherten oder Read-ahead-Daten (einschließlich das Öffnen und Schließen). Der Server kann eine Datei für einen Client geöffnet lassen, selbst wenn die Datei vom lokalen Prozess auf der Clientmaschine geschlossen wurde. Dieser Mechanismus verringert den Netzwerkverkehr, da Clients auf diese Weise die irrelevanten Anfragen zum Schließen und Öffnen überspringen können.
Benachrichtigung bei Schreibvorgang aktiviert	Aktivieren Sie die Benachrichtigung bei Schreibvorgängen in ein Dateisystem. Diese Option ist standardmäßig deaktiviert.
Benachrichtigung bei Zugriff aktiviert	Aktivieren Sie die Benachrichtigung bei Zugriffen auf ein Dateisystem. Diese Option ist standardmäßig deaktiviert.
SMB-Ereignisveröffentlichung aktivieren	Aktivieren Sie die Verarbeitung von SMB-Ereignissen für dieses Dateisystem.

Erstellen einer SMB-Freigabe

Sie können eine SMB-Freigabe auf einem Dateisystem erstellen, das mit einem SMB-fähigen NAS-Server erstellt wurde.

Schritte

1. Wählen Sie die Optionen **Storage** > **File System** > **SMB Share** aus.
2. Klicken Sie auf **Create**, und führen Sie die Anweisungen des Assistenten **Create SMB Share** aus.

Option	Beschreibung
Dateisystem auswählen	Wählen Sie ein Dateisystem aus, das für SMB aktiviert wurde.
Select a snapshot of the file system	Wählen Sie optional einen der Dateisystem-Snapshots aus, auf dem die Freigabe erstellt werden soll. Es werden nur Snapshots für Dateisystemschutz-Policies unterstützt. Die Replikation wird für Dateisysteme nicht unterstützt.
SMB Share Details	Geben Sie einen Namen und den lokalen Pfad für die Freigabe ein. Bei der Eingabe des lokalen Pfads: ● Sie können mehrere Freigaben mit demselben lokalen Pfad auf einem einzelnen SMB-Dateisystem erstellen. In diesen Fällen können Sie unterschiedliche hostseitige Zugriffskontrollen für die verschiedenen Nutzer festlegen, die Freigaben innerhalb des Dateisystems greifen jedoch auf gemeinsame Inhalte zu. ● Ein Verzeichnis muss vorhanden sein, damit Sie Freigaben darin erstellen können. Wenn die SMB-Freigaben im gleichen Dateisystem auf unterschiedliche Inhalte zugreifen sollen, müssen Sie zuerst ein Verzeichnis auf dem Windows-Host erstellen, der dem Dateisystem zugeordnet ist. Dann können Sie entsprechende Freigaben mithilfe von PowerStore erstellen. Sie können auch SMB-Shares über die Microsoft Management Console erstellen und managen. PowerStore hat auch den SMB-Freigabepfad erstellt, der den Host zur Verbindungsherstellung mit der Freigabe verwendet.

Option	Beschreibung
	Beim Exportpfad handelt es sich um die IP-Adresse des Dateisystems und den Namen der Freigabe. Hosts verwenden entweder den Dateinamen oder den Freigabepfad zum Mounten oder Zuordnen der Freigabe von einem Netzwerkhost aus.
Advanced SMB Properties	Aktivieren Sie eine oder mehrere der erweiterten SMB-Einstellungen. ● Kontinuierliche Verfügbarkeit ● Protokollverschlüsselung ● Access-based Enumeration ● Branch Cache aktiviert Legen Sie fest, welche Objekte verfügbar sind, wenn die Freigabe offline ist. Weitere Informationen finden Sie unter Erweiterte SMB-Eigenschaften.

Nächste Schritte

Nachdem Sie eine Freigabe erstellt haben, können Sie sie in PowerStore oder mithilfe der Microsoft Management Console ändern.

Um die Freigabe in PowerStore zu ändern, wählen Sie sie auf der Seite **SMB Share** in der Liste aus und klicken Sie auf **Modify**.

Erweiterte SMB-Share-Eigenschaften

Sie können die folgenden erweiterten SMB-Share-Eigenschaften konfigurieren, wenn Sie eine SMB-Share erstellen oder ihre Eigenschaften ändern:

Tabelle 5. Advanced SMB Properties

Option	Beschreibung
Kontinuierliche Verfügbarkeit	Ermöglicht, dass Hostanwendungen nach einem Failover des NAS-Servers im System kontinuierlich transparent auf eine Share zugreifen können (der interne Status des NAS-Servers wird während des Failover-Prozesses gespeichert oder wiederhergestellt). **ANMERKUNG:** Aktivieren Sie die kontinuierliche Verfügbarkeit für eine Freigabe nur, wenn Microsoft Server Message Block (SMB) 3.0-Protokollclients mit der Freigabe verwendet werden sollen.
Protokollverschlüsselung	Aktiviert die SMB-Verschlüsselung des Netzwerkverkehrs durch die Share. Die SMB-Verschlüsselung wird von SMB 3.0-Clients und höher unterstützt. Standardmäßig wird der Zugriff verweigert, wenn ein SMB 2-Client versucht, auf eine Freigabe mit aktivierter Protokollverschlüsselung zuzugreifen. Sie können dies steuern, indem Sie den Registrierungsschlüssel „RejectUnencryptedAccess“ auf dem nicht verschlüsselten NAS-Server konfigurieren (der Schlüsselpfad lautet „HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\RejectUnencryptedAccess“). „1“ (Standardwert) lehnt den Zugriff ab und „0“ ermöglicht Clients, die keine Verschlüsselung unterstützen, ohne Verschlüsselung auf das Dateisystem zuzugreifen.
Access Based Enumeration	Filtert die Liste der verfügbaren Dateien und Verzeichnisse auf der Share, sodass nur Dateien angezeigt werden, für die der anfragende Benutzer Lesezugriff hat. **ANMERKUNG:** Administratoren können immer alle Dateien auflisten.
Branch Cache aktiviert	Kopiert Inhalte aus der Share und speichert sie in Zweigstellen zwischen. Dadurch können Clientcomputer in Zweigstellen lokal auf Inhalte zugreifen anstatt über das WAN. BranchCache wird von Microsoft-Hosts gemanagt.
Offlineverfügbarkeit	Konfiguriert die clientseitige Zwischenspeicherung von Offlinedateien: ● **Keine**: Das clientseitige Zwischenspeichern von Offlinedateien ist nicht konfiguriert (Standardwert). ● **Manuell**: Dateien werden nur zwischengespeichert und sind offline verfügbar, wenn dies ausdrücklich angefordert wird.

Tabelle 5. Advanced SMB Properties (fortgesetzt)

Option	Beschreibung
	• **Programme**: Alle Dateien, die Clients aus der Freigabe öffnen, sind automatisch offline verfügbar. Ausführbare Dateien, die zuvor lokal zwischengespeichert wurden, werden von der zwischengespeicherten Kopie ausgeführt, auch wenn die Freigabe verfügbar ist. • **Dokumente**: Alle Dateien, die Clients aus der Freigabe öffnen, sind automatisch offline verfügbar. Wenn ein Nutzer über eine Freigabe auf eine Datei zugreift, wird der Inhalt automatisch zwischengespeichert, damit er für diesen Nutzer im Offlinemodus verfügbar ist. Alle geöffneten Dateien werden weiterhin zwischengespeichert und stehen für den Offlinezugriff zur Verfügung, bis der Cache voll ist. Cacheinhalte werden weiterhin mit der Version auf dem Server synchronisiert. Dateien, die nicht geöffnet wurden, sind nicht offline verfügbar.

Managen von ACLs

Der Windows-Client legt die Zugriffsberechtigungen (auch als Zugriffskontrolllisten oder ACLs bezeichnet) für SMB-Freigaben über die MMC-Konsole fest und ändert sie. Sie können jetzt ACLs von SMB-Freigaben auf dem SDNAS-Cluster direkt in PowerStore über die Benutzeroberfläche oder die REST API managen.

ANMERKUNG: Weitere Informationen dazu, wie Sie ACLs über die REST API festlegen, finden Sie im *Referenzhandbuch für die Dell PowerStore-REST API* auf dell.com/powerstoredocs.

ANMERKUNG: Zugriffsberechtigungen von Dateien und Verzeichnissen in den SMB-Freigaben können nur mit dem Windows-Client verwaltet werden.

Um den Bildschirm „Zugriffskontrollliste“ mit dem PowerStore Manager zu öffnen, wählen Sie **Storage** > **Dateisysteme** > **SMB-Freigaben** > **[SMB-Freigabe]** > **Weitere Aktionen** > **zugriffskontrollliste** aus.

Der Bildschirm „Zugriffskontrollliste“ zeigt die Liste der ACEs (Access Control Entries) an, die für den ausgewählten SMB definiert sind. Für jeden ACE werden der Name oder die ID des Bevollmächtigten, die Zugriffsebene und der Zugriffstyp aufgeführt. Sie können die Liste nach einem der Attribute filtern.

ANMERKUNG: Der Standard-ACE gewährt jedem Nutzer eine vollständige Berechtigung.

Im Dialogfeld „Zugriffskontrollliste“ können Sie die folgenden Schritte ausführen:

- ACE hinzufügen – Weitere Informationen finden Sie unter Hinzufügen eines Zugriffskontrolleintrags.
- ACE ändern: Ermöglicht die Bearbeitung eines der ausgewählten ACE-Felder.
- Löschen Sie den ausgewählten ACE.
- ACL aktualisieren (unter **Weitere Aktionen**) – Verwenden Sie diese Option, wenn Sie die ACL über die Windows MMC-Konsole oder REST API geändert haben. Mit der Option „Aktualisieren“ wird die ACL mit den Änderungen aktualisiert.

Hinzufügen eines Zugriffskontrolleintrags

Info über diese Aufgabe

Ein ACE weist die folgenden Attribute auf:

- Typ des Bevollmächtigten – Nutzer, Gruppe, Sicherheitskennung (Security Identifier, SID) oder WellKnown
- Name/ID des Bevollmächtigten – Das Format dieses Felds richtet sich nach dem Typ des Bevollmächtigten:
  - Nutzername – Domain/Nutzername
  - Gruppenname – Domain/Gruppenname
  - SID – SID-Format (z. B. S-1-2-34-567890123-456789012-3456789012-34)
  - WellKnown – Beispielsweise „Jeder“
- Zugriffsebene – Lesen, Ändern oder Vollständig
- Zugriffstyp – Zulassen oder Verweigern

Schritte

1. Wählen Sie **Storage** > **Dateisysteme** > **SMB-Freigaben** > **[SMB-Freigabe]** > **Weitere Aktionen** > **Zugriffskontrollliste** aus.
2. Wählen Sie im Fenster **Zugriffskontrollliste** die Option **ACE hinzufügen** aus.

3. Füllen Sie die erforderlichen ACE-Felder aus, und klicken Sie auf **Speichern**.
   Das neue ACE wird der ACL hinzugefügt.
4. Klicken Sie auf **Apply**, um die Änderungen zu speichern.

5

Weitere Dateisystemfunktionen

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Aufbewahrung auf Dateilevel

Mit der Aufbewahrung auf Dateiebene (File-Level Retention, FLR) können Sie Änderungen oder die Löschung von gesperrten Dateien für eine bestimmte Aufbewahrungsfrist verhindern. Durch den Schutz eines Dateisystems mithilfe von FLR können Sie einen permanenten und unveränderlichen Satz von Dateien und Verzeichnissen erstellen. FLR sorgt für die Integrität und Zugänglichkeit von Daten, es vereinfacht Archivierungsverfahren für Administratoren und verbessert die Flexibilität des Storage-Managements.

Es gibt zwei Ebenen der Aufbewahrung auf Dateiebene:

- Enterprise (FLR-E): Schützt Daten vor Änderungen, die von Nutzern und Storage-Administratoren mithilfe von SMB, NFS und FTP vorgenommen werden. Ein Administrator kann ein FLR-E-Dateisystem löschen, das gesperrte Dateien enthält.
- Compliance (FLR-C): Schützt Daten vor Änderungen, die von Nutzern und Storage-Administratoren mithilfe von SMB, NFS und FTP vorgenommen werden. Ein Administrator kann kein FLR-C-Dateisystem löschen, das gesperrte Dateien enthält. FLR-C entspricht der SEC-Regel 17a-4(f).

Es gelten folgende Einschränkungen:

- Die Aufbewahrung auf Dateiebene ist auf dem vereinten PowerStore-System 3.0 oder höher verfügbar.
- FLR wird in VMware-Dateisystemen nicht unterstützt.
- Die Aktivierung einer Aufbewahrung auf Dateiebene für ein Dateisystem und die FLR-Ebene werden zum Zeitpunkt der Dateisystemerstellung festgelegt und können nicht geändert werden.
- FLR-C bietet keine Unterstützung für die Wiederherstellung von einem Snapshot.
- Bei der Aktualisierung mit einem Snapshot müssen beide Dateisysteme die gleiche FLR-Ebene aufweisen.
- Bei der Replikation eines Dateisystems müssen Quell- und Zieldateisysteme dieselbe FLR-Ebene haben.
- Ein geklontes Dateisystem hat die gleiche FLR-Ebene wie die Quelle (kann nicht geändert werden).

Der FLR-Modus wird auf dem Bildschirm **Dateisysteme** angezeigt.

Konfigurieren des DHSM-Servers

Voraussetzungen

Für die Aufbewahrung auf Dateiebene sind DHSM-Serveranmeldedaten erforderlich.

Der DHSM-Server ist auch für Windows-Hosts erforderlich, die FLR verwenden möchten und das FLR-Toolkit installieren müssen, mit dem FLR-fähige Dateisysteme verwaltet werden können.

Schritte

1. Wählen Sie die Optionen **Storage** > **NAS-Server** > **[NAS-Server]** > **Sicherheit** > **Kerberos** aus.
2. Wenn diese Option deaktiviert ist, schieben Sie die Schaltfläche auf **Aktiviert**.
3. Geben Sie den Nutzernamen und das Kennwort für den DHSM-Server ein und überprüfen Sie das Kennwort.
4. Klicken Sie auf **Anwenden**.

Konfigurieren der Aufbewahrung auf Dateiebene

Die Aufbewahrung auf Dateiebene wird bei der Dateisystemerstellung konfiguriert. Weitere Informationen finden Sie unter Erstellen eines Dateisystems.

ANMERKUNG: Die Parameter für die Aufbewahrungsfrist können zu einem späteren Zeitpunkt geändert werden.

Ändern der Aufbewahrung auf Dateiebene

Info über diese Aufgabe

Die Parameter für die Aufbewahrungsfrist können bei der Dateisystemerstellung oder später festgelegt und geändert werden. Das Ändern des Aufbewahrungsfristparameters hat keinen Einfluss auf die bereits gesperrten Dateien.

Schritte

1. Wählen Sie **Storage** > **Dateisysteme** > **[Dateisystem]** > **Sicherheit & Ereignisse** > **Aufbewahrung auf Dateiebene** aus.
2. Legen Sie die Parameter des Aufbewahrungszeitraums fest:
   - Minimale Aufbewahrungsfrist: Gibt den kürzesten Zeitraum an, für den ein FLR-fähiges Dateisystem geschützt werden kann (Der Standardwert ist ein Tag.).
   - Standardaufbewahrungsfrist: Wird verwendet, wenn eine Datei gesperrt und keine Aufbewahrungsfrist angegeben ist (Der Standardwert ist ein Jahr.).
   - Maximale Aufbewahrungsfrist: Gibt den längsten Zeitraum an, für den ein FLR-fähiges Dateisystem geschützt werden kann (Der Standardwert ist unbegrenzt.).
3. Konfigurieren Sie optional die erweiterten Einstellungen:
   - Automatische Dateisperre: Sie können einstellen, ob Dateien in einem FLR-fähigen Dateisystem automatisch gesperrt werden sollen, und ein Policy-Intervall bestimmen, das den Zeitraum zwischen Dateiänderung und automatischer Sperrung festlegt (Der Standardwert für das Policy-Intervall ist eine Stunde.).
   - Automatisches Löschen von Dateien: Sie können festlegen, ob gesperrte Dateien nach Ablauf ihrer Aufbewahrungsfrist automatisch gelöscht werden sollen. Der erste Scan zum Suchen von zu löschenden Dateien erfolgt sieben Tage nach der Aktivierung der Funktion.
4. Klicken Sie auf **Anwenden**.

Dateisystem-Quotas

Sie können die Belegung des Laufwerksspeichers durch Konfigurieren von Quoten für Dateisysteme auf Dateisystem- oder Verzeichnisebene begrenzen und nachverfolgen. Sie können Quotas jederzeit aktivieren oder deaktivieren. Es wird jedoch empfohlen, diese außerhalb der Produktionsspitzenzeiten zu aktivieren oder deaktivieren, um eine Beeinträchtigung des Dateisystembetriebs zu vermeiden.

ANMERKUNG: Sie können keine Quoten für schreibgeschützte Dateisysteme aktivieren.

ANMERKUNG: Kontingente werden in VMware-Dateisystemen nicht unterstützt.

ANMERKUNG: Wenn Sie eine Replikationssitzung erstellen, sind keine Quoten auf dem Zielsystem sichtbar, selbst wenn sie auf dem Quellsystem aktiviert sind.

Quota-Typen

Es gibt drei Quota-Typen, die Sie auf einem Dateisystem festlegen können.

Tabelle 6. Quota-Typen

Typ	Beschreibung
Benutzerquoten	Begrenzt die Menge an Storage, die durch einen einzelnen Nutzer, der Daten im Dateisystem speichert, belegt werden kann.

Tabelle 6. Quota-Typen (fortgesetzt)

Typ	Beschreibung
Struktur-Quota	Struktur-Quotas begrenzen die Gesamtmenge des Storage, der in einer bestimmten Verzeichnisstruktur verbraucht wird. Sie können Struktur-Quotas verwenden für: • das Festlegen von Speicherbegrenzungen auf Projektbasis. Beispielsweise können Sie Struktur-Quotas für ein Projektverzeichnis erstellen, in dem mehrere Nutzer Dateien gemeinsam verwenden und erstellen. • Verfolgen Sie die Nutzung des Verzeichnisses nach, indem Sie das harte und das weiche Limit der Struktur-Quotas auf 0 (null) festlegen. **ANMERKUNG:** Wenn Sie die Begrenzungen für Struktur-Quotas ändern, werden die Änderungen sofort übernommen, ohne die Dateisystemabläufe zu unterbrechen.
Benutzerquote in einer Quotenstruktur	Begrenzt die Menge an Storage, die durch einen einzelnen Nutzer, der Daten in der Quota-Struktur speichert, belegt werden kann.

Quota-Begrenzungen

Tabelle 7. Harte und weiche Limits

Typ	Beschreibungen
Hart	Ein hartes Limit ist ein absoluter Grenzwert für die Storage-Nutzung. Wenn ein hartes Limit für eine Nutzerquote auf einem Dateisystem oder in einer Quotenstruktur erreicht ist, kann der/die NutzerIn keine Daten mehr in das Dateisystem oder den Strukturbaum schreiben, bis mehr Speicherplatz verfügbar ist. Wenn ein hartes Limit für eine Quotenstruktur erreicht ist, kann kein(e) NutzerIn mehr Daten in den Strukturbaum schreiben, bis mehr Speicherplatz verfügbar ist.
Weiches Limit:	Ein weiches Limit ist ein bevorzugtes Limit für die Storage-Nutzung. Der/die NutzerIn darf Speicherplatz verwenden, bis eine Toleranzperiode erreicht ist. Der/die NutzerIn wird benachrichtigt, wenn das weiche Limit erreicht ist, bis die Toleranzperiode abgelaufen ist. Danach wird der Zustand „Out of Space“ erreicht, bis der/die NutzerIn wieder unter das weiche Limit kommt.

Quota-Toleranzperiode

Die Toleranzperiode für Quoten ermöglicht das Festlegen einer bestimmten Toleranzperiode für die Strukturquote in einem Dateisystem. Die Toleranzperiode zählt die Zeit zwischen dem weichen und dem harten Limit herunter und benachrichtigt den/die NutzerIn über die verbleibende Zeit, bevor das harte Limit erreicht wird. Wenn die Toleranzperiode abläuft, können NutzerInnen nicht mehr in das Dateisystem oder die Quotenstruktur schreiben, bis mehr Speicherplatz hinzugefügt wurde, selbst wenn das harte Limit nicht erreicht ist.

Sie können ein Ablaufdatum für die Toleranzperiode festlegen. Der Standardwert ist 7 Tage. Alternativ können Sie das Ablaufdatum der Toleranzperiode auf eine unendliche Zeitdauer (die Toleranzperiode läuft nie ab) oder für die angegebene Anzahl von Tagen, Stunden oder Minuten festlegen. Sobald das Ablaufdatum für die Toleranzperiode erreicht ist, gilt die Toleranzperiode nicht mehr für das Dateisystemverzeichnis.

Weitere Informationen

Weitere Informationen zu Quotas finden Sie im *Whitepaper zu Dateifunktionen von Dell PowerStore*.

Aktivieren von Nutzerquoten

Sie müssen Quoten aktivieren und die Standardeinstellungen für Nutzerquoten festlegen, bevor Sie einem Dateisystem eine Nutzerquote hinzufügen können.

Schritte

1. Wählen Sie die Optionen **Storage** > **File Systems** > **[Dateisystem]** > **Quotas** aus.
2. Wählen Sie die Optionen **Storage** > **File Systems** > **[Dateisystem]** > **Quotas** > **Properties** aus.
3. Schieben Sie den Schieberegler von **Deaktiviert** zu **Aktiviert**.
4. Geben Sie die standardmäßige **Toleranzperiode** für die Nutzerquote des Dateisystems ein, in der die Zeit vom Erreichen des weichen Limits bis zum Erreichen des harten Limits heruntergezählt wird.
5. Geben Sie ein standardmäßiges **Soft Limit** und ein standardmäßiges **Hard Limit** ein, und klicken Sie auf **Update**.

Hinzufügen einer Nutzerquote zu einem Dateisystem

Erstellen Sie eine Benutzer-Quota auf einem Dateisystem, um die Menge des Speicherplatzes zu begrenzen oder zu verfolgen, die einzelne Benutzer auf diesem Dateisystem belegen. Beim Erstellen oder Ändern von Nutzerquoten können Sie standardmäßige harte und weiche Limits verwenden, die auf Ebene des Dateisystems festgelegt werden.

Voraussetzungen

Sie müssen Quoten aktivieren und die Standardeinstellungen für Nutzerquoten festlegen, bevor Sie einem Dateisystem eine Nutzerquote hinzufügen können. Weitere Informationen finden Sie unter Aktivieren von Benutzerquoten.

ANMERKUNG: Sie können keine Quotas für schreibgeschützte Dateisysteme erstellen.

Schritte

1. Wählen Sie die Optionen **Storage** > **File Systems** > **[file system]** > **Quotas** > **User** aus.
2. Wählen Sie auf der Seite **User Quota** die Option **Add** aus.
3. Geben Sie im Assistenten **Add User Quota** die erforderlichen Informationen ein. Um den Speicherplatzverbrauch ohne Festlegung von Limits nachzuverfolgen, legen Sie **Soft Limit** und **Hard Limit** auf 0 fest (was kein Limit bedeutet).
4. Wählen Sie **Add**.

Hinzufügen einer Quotenstruktur zu einem Dateisystem

Info über diese Aufgabe

Erstellen Sie eine Quotenstruktur auf der Verzeichnisebene eines Dateisystems, um den durch dieses Verzeichnis belegten gesamten Speicherplatz zu begrenzen oder nachzuverfolgen.

Schritte

1. Wählen Sie die Optionen **Storage** > **File Systems** > **[Dateisystem]** > **Quotas** > **Tree Quotas** aus.
2. Wählen Sie **Add**.
3. Schieben Sie die Option **Enforce User Quota** nach rechts, um die standardmäßigen Benutzerquoten für die Strukturquote zu aktivieren.
4. Geben Sie die erforderlichen Informationen an.
   - Geben Sie eine **Grace Period** ein, um die Zeit zwischen dem weichen und dem harten Limit herunterzuzählen. Sie erhalten Warnmeldungen, sobald die Toleranzperiode erreicht ist.
   - Um den Speicherplatzverbrauch ohne Festlegung von Limits nachzuverfolgen, legen Sie die Felder **Soft Limit** und **Hard Limit** auf 0 fest. Dies entspricht keinem Limit.
5. Wählen Sie **Add**.

Hinzufügen einer Nutzerquote zu einer Quotenstruktur

Erstellen Sie eine Benutzer-Quota in einer Quota-Struktur, um die Menge des Speicherplatzes zu begrenzen oder zu verfolgen, die einzelne Benutzer in dieser Struktur belegen. Beim Erstellen von Benutzerquoten in einer Struktur können Sie die standardmäßige Toleranzperiode und standardmäßige harte und weiche Limits verwenden, die auf Ebene der Quotenstruktur festgelegt werden.

Schritte

1. Wählen Sie die Optionen **Storage** > **File Systems** > **[Dateisystem]** > **Quotas** > **Tree Quotas** aus.
2. Wählen Sie einen Pfad aus und klicken Sie auf **Add User Quota**.
3. Geben Sie auf dem Bildschirm **Add User Quota** die erforderlichen Informationen ein. Um den Speicherplatzverbrauch ohne Festlegung von Limits nachzuverfolgen, legen Sie die Felder **Soft Limit** und **Hard Limit** auf 0 fest. Dies entspricht keinem Limit.

Datei-QoS (Quality of Service)

In einem System, auf dem unterschiedliche Workloads mit unvorhersehbaren Anforderungen ausgeführt werden, sorgt Quality of Service dafür, dass kritische Anwendungen Priorität erhalten, und bietet eine vorhersehbare Performance für jede Anwendung.

Sie können QoS-Policies (Quality of Service) anwenden, um die maximale Bandbreite für NAS-Server und Dateisysteme festzulegen.

Wenn Sie einem NAS-Server oder Dateisystem eine QoS-Richtlinie zuweisen, setzt SDNAS die Richtlinie auf NFS/SMB-Diensten durch.

Bandbreitenbegrenzungen werden basierend auf NFS/SMB- und SFTP/FTP-Protokollen angewendet.

Wenn die festgelegte Bandbreite die für den NAS-Server festgelegte maximale Bandbreite überschreitet, ist die effektive Bandbreite die maximale Bandbreite des Servers.

ANMERKUNG: Es kann einige Zeit dauern, bis eine QoS-Policy wirksam wird.

ANMERKUNG: QoS wird bei NAS-Server-Clones, Dateisystem-Clones, Snapshots, Snapshot-Clones und Snapshot-Aktualisierung nicht unterstützt.

ANMERKUNG: Die Bandbreite, die im Rahmen einer zugewiesenen QoS-Policy auf NAS-Server und Dateisysteme angewendet wird, kann innerhalb einer Marge von 10 % abweichen.

Beschränkungen für Datei-QoS:

- Eine QoS-Policy kann eine I/O-Limit-Regel enthalten.
- Es können bis zu 100 Datei-QoS-Policies definiert werden.
- Es können bis zu 100 Datei-QoS-Regeln definiert werden.
- Es kann nur eine QoS-Policy auf einen NAS-Server oder ein Dateisystem angewendet werden.
- Dieselbe QoS-Policy kann mehreren NAS-Servern und Dateisystemen zugewiesen werden.

QoS und Dateireplikation:

- Wenn der NAS-Server über eine Replikationsregel verfügt, wird die zugewiesene QoS-Policy auf den Zielserver repliziert.
- Wenn Sie QoS-Policies ändern, die dem NAS-Server zugewiesen sind, werden die Änderungen auf den Zielserver repliziert.
- Es ist nicht möglich, die replizierte QoS-Policy-Konfiguration auf dem Zielserver zu ändern.
- Es ist nicht möglich, eine QoS-Policy einem NAS-Server oder Dateisystem auf dem Zielserver zuzuweisen.
- Nach dem Zuweisen einer QoS-Policy zu einem NAS-Server oder Dateisystem auf dem Quellserver ist es nicht möglich, die Zuweisung der Policy zum Zielserver aufzuheben.
- Nachdem Sie die Zuweisung einer QoS-Policy zu einem NAS-Server aufgehoben haben, sollte die Zuweisung der Policy auch am Ziel aufgehoben werden.
- Nach dem Failover können Sie replizierte QoS-Policies zuweisen, die Zuweisung aufheben und ändern.

Datei-QoS-Limits

Sie können I/O-Limit-Regeln für NAS-Server und Dateisysteme erstellen. Eine I/O-Limit-Regel definiert die zulässige maximale Bandbreite.

- Jeder NAS-Server oder jedes Dateisystem kann nur einer Limit-Regel zugeordnet werden.
- Jede Policy kann nur eine Regel enthalten.
- Sie können bis zu 100 Regeln erstellen.

I/O-Limit-Regeln gelten nur für I/O von externen Hosts und nicht für interne asynchrone oder synchrone Replikationsvorgänge oder Migrations-I/O.

I/O-Limit-Regeln werden nicht auf intern erstellte Objekte angewendet, z. B. NDMP-Backups, die von einem NDMP-Server in SDNAS bedient werden.

Spezifische Warnmeldungen für Datei-QoS-Limits werden nicht unterstützt. Um zu erfahren, ob die festgelegten Limits angepasst werden müssen, können Sie die Diagramme für Latenz, IOPS und Bandbreite für jeden NAS-Server und Dateisystem überwachen.

Erstellen einer QoS-Bandbreitenbegrenzungsregel und Policy (Quality of Service)

Info über diese Aufgabe

Sie können eine Bandbreitenbegrenzungsregel erstellen und sie zu einer QoS-Policy hinzufügen.

Schritte

1. Wählen Sie **Storage** > **Quality of Service (QoS)** > **Datei-I/O-Limit-Regeln** aus.
2. Wählen Sie **Erstellen** aus.
3. Legen Sie auf dem Slide-Out **Datei-I/O-Limit-Regel erstellen** den Regelnamen und die maximale Bandbreite (MB/s) fest.
4. Wählen Sie **Erstellen** aus.
   Die Regel wird der Tabelle „Datei-I/O-Limit-Regeln“ hinzugefügt.
5. Wählen Sie **Datei-QoS-Policies**.
6. Wählen Sie **Erstellen** aus.
7. Legen Sie auf dem Slide-Out **Datei-QoS-Policy erstellen** den Policy-Namen fest. Sie können auch eine Beschreibung hinzufügen.
8. Wählen Sie aus der Regelliste die Regel aus, die Sie der Policy hinzufügen möchten.
9. Wählen Sie **Erstellen** aus.
   Die Policy wird der Tabelle „Datei-QoS-Policies“ hinzugefügt.

Datei-QoS-Policy zuweisen

Info über diese Aufgabe

Nachdem Sie eine I/O-Limit-Regel als Teil einer Datei-QoS-Policy definiert haben, können Sie sie einem NAS-Server oder einem Dateisystem zuweisen. Sie können auch die zugewiesene QoS-Policy ändern.

ANMERKUNG: Es ist auch möglich, eine QoS-Policy als Teil des Verfahrens zum Erstellen eines NAS-Servers oder Dateisystems zuzuweisen.

Schritte

1. Wählen Sie **Storage** > **NAS-Server** oder **Storage** > **Dateisysteme** aus.
2. Aktivieren Sie das Kontrollkästchen neben dem entsprechenden NAS-Server oder Dateisystem.
3. Wählen Sie **Weitere Aktionen** > **QoS-Policy ändern** aus.
4. Wählen Sie auf dem Slide-Out **QoS-Policy ändern** eine Datei-QoS-Policy aus und wählen Sie dann **Anwenden** aus.
   Die Policy ist zugewiesen. Sie können den zugewiesenen Policy-Namen in der Spalte **QoS-Policy** in den Tabellen NAS-Server und Dateisysteme anzeigen. Sie können die Auswirkungen der zugewiesenen Policy auf die Performance anzeigen, indem Sie **Storage** > **NAS Servers** > **[NAS Server]** > **Performance** oder **Storage** > **Dateisysteme** > **[Dateisystem]** > **Performance** auswählen.
   ANMERKUNG: Sie können die QoS-Policy auch festlegen, indem Sie den entsprechenden NAS-Server oder das Dateisystem auswählen und dann **Ändern** auswählen.

Datei-QoS-Policy ändern

Sie können eine QoS-Policy ändern, indem Sie eine andere I/O-Limit-Regel auswählen.

Voraussetzungen

Sie können keine Policy ändern, die einem NAS-Server oder Dateisystem zugewiesen ist.

Schritte

1. Wählen Sie **Storage** > **Quality of Service (QoS)** aus.
2. Wählen Sie in der Tabelle **Datei-QoS Policies** das Kontrollkästchen neben der QoS-Policy aus, die Sie ändern möchten.
3. Wählen Sie **Ändern** aus.

4. Im Fenster **QoS-Policy ändern** können Sie den Namen und die Beschreibung der Policy ändern und eine andere I/O-Limit-Regel auswählen.
5. Klicken Sie auf **Anwenden**.

ANMERKUNG: Sie können eine QoS-Policy auch über den Bildschirm **Eigenschaften** der Storage-Ressource ändern.

Datei-QoS-Policy löschen

Voraussetzungen

Stellen Sie sicher, dass die QoS-Policy, die Sie löschen möchten, keinem NAS-Server oder Dateisystem zugewiesen ist.

Schritte

1. Wählen Sie **Storage** > **Quality of Service (QoS)** aus.
2. Wählen Sie in der Tabelle **Datei-QoS Policies** die QoS-Policy aus, die Sie ändern möchten.
3. Wählen Sie **More Actions** > **Delete** aus.
4. Wählen Sie **Löschen** aus, um den Vorgang zu bestätigen.

6

NAS-Serverreplikation

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Übersicht

Um erweiterte Redundanz und Recovery bei Datenverlust zu aktivieren, ermöglicht PowerStore es Ihnen, NAS-Server von einem lokalen System auf ein Remotesystem zu replizieren.

Die Replikation erfolgt standardmäßig auf NAS-Serverebene, d. h. alle Dateisysteme innerhalb des replizierten NAS-Servers werden auf das Remotesystem repliziert. Sie können Dateisysteme zum NAS-Server hinzufügen oder Dateisysteme vom NAS-Server löschen, wenn er Teil einer Replikationssitzung ist.

Sie können asynchrone Replikation auswählen, bei der die Systeme basierend auf einer festgelegten RPO synchronisiert werden, oder synchrone Replikation, bei der auftretende Änderungen sofort vom Quellsystem auf das Zielsystem repliziert werden.

Die folgenden Voraussetzungen sind erforderlich, um die Dateireplikation zu aktivieren:

- Ein Datei-Remotesystem
- Ein Dateimobilitätsnetzwerk muss konfiguriert und zugeordnet werden (siehe *PowerStore T und Q – Netzwerkleitfaden für Storage-Services* auf der PowerStore-Dokumentationsseite).
- Eine Schutz-Policy, die eine Replikationsregel enthält.

Beachten Sie bei der NAS-Serverreplikation Folgendes:

- Es ist nicht erforderlich, separate Schutz-Policies für NAS-Server zu definieren. Dieselben Schutz-Policies können sowohl auf die Block- als auch auf die Dateireplikation angewendet werden.
- Sie können Dateisysteme vom Quellsystem einer Replikationssitzung löschen. Nach dem Löschen werden nur die verbleibenden Dateisysteme auf das Ziel repliziert. Der Status des Zielsystems wird durch das Löschen der Dateisysteme nicht beeinträchtigt. Wenn Sie Dateisysteme von einem replizierten NAS-Quellserver löschen und dann ein Failover auf das Zielsystem durchführen, werden die Dateisysteme, die von der alten Quelle gelöscht wurden, nicht von der neuen Quelle repliziert. Wenn Sie diese Dateisysteme replizieren möchten, erzeugen Sie replizierbare Clones und löschen Sie die Dateisysteme.
- Sie können den Failover einer Replikationssitzung zum Remotesystem ausführen. Der Failover tritt für alle Dateisysteme innerhalb des Failover-NAS-Servers auf.
- Wenn Sie eine Replikationssitzung erstellen, sind keine Quoten auf dem Zielsystem sichtbar, selbst wenn sie auf dem Quellsystem aktiviert sind.
- Für die asynchrone Replikation wird die RPO auf NAS-Serverebene konfiguriert und ist für alle zugehörigen Dateisysteme identisch.
- 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.

Detaillierte Informationen zu NAS-Serverreplikationsverfahren finden Sie unter *Schützen Ihrer Daten* auf der PowerStore-Dokumentaktionsseite.

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.
- Durchführen eines geplanten Failovers.

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 NAS-Serverreplikation.
   b. Führen Sie ein geplantes Failover zum Ziel durch. Weitere Informationen finden Sie unter Geplantes Failover.
   c. Überprüfen Sie, ob der Host auf die Daten zugreifen kann.
9. Wenn Sie den replizierten Produktionsserver auf dem Zielsystem geklont haben, ist kein Failover erforderlich. Überprüfen Sie den Hostzugriff.

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

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

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

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

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

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

So testen Sie DR mithilfe einer isolierten Testumgebung:

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

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

Voraussetzungen und Einschränkungen

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

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

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

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

Konfigurieren der Disaster Recovery-Testumgebung mithilfe von PSTCLI

Schritte

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

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> nas_server show
# | id | name | operational_status |  current_node_id  | file_interfaces.ip_addre~
--+------------+--------+--------------------+-------------------
```

```
1 |647f545a-4b11-5cdd-4d4c-eeeba81eb143 | File80| Started | R2C4-appliance-1-node~|
127.1.1.1
```

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

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

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

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

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

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

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

5. Zeigen Sie die Dateischnittstelle an:

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> file_interface_show
# |id | nas_server_id | ip_address | prefix_length | gateway | is_disabled
--+-------------+--------+--------------------+-------------------
  1 |647f5509-11f4-a52d-ee1f-82772509648e | 647f545a-4b11-5cdd-4d4c-eeeba81eb143 |
10.10.10.10 |24 | 10.10.10.1 | no
  2 |64830ae5-2760-59ce-4c90-82772509648e | 6483092f-3e71-8a92-0a0b-82772509648e |
10.10.10.10 |24 | 10.10.10.1 | no
```

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

Info über diese Aufgabe

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

Schritte

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

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

Ergebnisse

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

Durchführen eines geplanten Failovers

Sie können die Disaster Recovery mit einem geplanten Failover testen. Wenn Sie ein geplantes Failover durchführen, erfolgt ein manuelles Failover der NAS-Server-Replikationssitzung vom Quellsystem zum Zielsystem. Vor dem Failover wird das Zielsystem mit dem Quellsystem synchronisiert, um Datenverlust zu vermeiden.

ANMERKUNG: Ein Failover des Produktions-NAS-Servers auf das Zielsystem kann sich auf die Produktion auswirken.

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

Bei normalem Betrieb werden Änderungen, die während des DR-Tests am NAS-Server und den Dateisystemen vorgenommen wurden, beibehalten und wieder auf die ursprüngliche Quelle repliziert, wenn der erneute Schutz initiiert wird (entweder manuell oder automatisch). Wenn Sie die während des DR-Tests vorgenommenen Änderungen (an Daten oder Konfiguration) jedoch nicht speichern möchten, können Sie die Änderungen über REST API- oder PSTCLI-Befehle verwerfen:

- REST-API – `POST /replication_session/{id}/reprotect discard_changes_after_failover`
- PSTCLI – `replication_session -id <value> reprotect [-discard_changes_after_failover]`

Änderungen, die verworfen werden:

- Für NAS-Server:
  - Konfigurationsänderungen
- Für Dateisysteme:
  - Konfigurationsänderungen
  - Änderungen bei Dateisystemdaten
  - Snapshot-Ressourcen
  - Änderungen bei Dateisystemgröße
  - Änderungen bei Quoten
- Für Exporte und Freigaben:
  - Änderungen bei NFS-Exporten
  - Änderungen bei SMB-Freigaben

ANMERKUNG: Diese Option wird nur für die asynchrone Replikation unterstützt.

Weitere Informationen zur Verwendung der REST API und CLI zum Verwerfen von Änderungen nach einem Failover finden Sie im *Referenzhandbuch für die Dell PowerStore-REST API* und im *Referenzhandbuch für die Dell PowerStore-CLI* auf dell.com/powerstoredocs.

Nachdem der NAS-Server erneut geschützt wurde, können Sie ein geplantes Failover erneut initiieren, um die Ressourcen auf dem ursprünglichen Quellsystem online zu schalten.

ANMERKUNG: Führen Sie kein ungeplantes Failover für Disaster-Recovery-Zwecke durch. Ein ungeplantes Failover sollte nur verwendet werden, wenn auf das Quellsystem nicht zugegriffen werden kann.

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

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

Nach einem geplanten Failover ist die Replikationssitzung inaktiv. Verwenden Sie die Aktion **Neu schützen**, um die 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: Nach dem Failover sind keine Nutzerquoten auf dem Zielsystem (das zur neuen Quelle geworden ist) sichtbar. Um die Nutzerquoten anzuzeigen, aktualisieren Sie die Quoten manuell, indem Sie **Storage** > **Dateisysteme** auswählen, das Kontrollkästchen neben dem entsprechenden Dateisystem aktivieren und dann **Weitere Aktionen** > **Quoten aktualisieren** auswählen.

Netzwerktrennung während eines DRT

Bei der Durchführung eines DRT wird nicht empfohlen, einen Netzwerkfehler zwischen dem lokalen und dem Remote-System zu simulieren und dann ein ungeplantes Failover auf das Zielsystem durchzuführen, um den Zugriff auf den DR-NAS-Server zu ermöglichen.

Da keine Kommunikation zwischen den Systemen besteht, kann PowerStore nicht sicherstellen, dass sich beide NAS-Server in einem kompatiblen Zustand befinden. Nachdem die Verbindung wiederhergestellt wurde, befinden sich beide NAS-Server im Produktionsmodus (Split Brain). Demzufolge wechseln beide Systeme in den Wartungsmodus, um zu verhindern, dass Daten auf beide Speicherorte geschrieben werden.

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

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

7

Verwenden von CEPA mit PowerStore

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Ereignisveröffentlichung

CEE ermöglicht es Drittanbieteranwendungen, Ereignisinformationen vom Storage-System beim Zugriff auf Dateisysteme zu erhalten.

Der Common Event Enabler (CEE) bietet eine Ereignisveröffentlichungslösung für PowerStore-Clients, mit der Anwendungen von Drittanbietern beim Zugriff auf Dateisysteme Ereignisbenachrichtigungen und Kontext vom Storage-System registrieren und empfangen können. Durch das Empfangen von Ereignisbenachrichtigungen können Sie ereignisgesteuerte Aktionen auf dem Storage durchführen, um Sicherheitsbedrohungen wie Ransomware oder unbefugte Zugriffe zu verhindern.

Der CEE Common Events Publishing Agent (CEPA) besteht aus Anwendungen, die für die Verarbeitung von SMB- und NFS-Dateien sowie Verzeichnisereignisbenachrichtigungen entwickelt wurden. Der CEPA stellt der Anwendung sowohl Ereignisbenachrichtigungen als auch zugehörigen Kontext in einer Meldung bereit. Der Kontext kann aus Metadaten der Datei oder Verzeichnismetadaten bestehen, die erforderlich sind, um Entscheidungen zur Unternehmens-Policy zu treffen.

Zur Aktivierung der CEE CEPA-Unterstützung müssen Sie CEE CEPA aktivieren und einen Ereignisveröffentlichungspool auf dem NAS-Server erstellen.

Ein Ereignisveröffentlichungspool definiert die CEPA-Server und die spezifischen Ereignisse, die Benachrichtigungen auslösen.

Nach der Konfiguration des NAS-Servers können Sie die Ereignisveröffentlichung auf dem Dateisystem aktivieren, von dem Sie Ereignisse empfangen möchten. Wenn ein Host ein Ereignis auf dem Dateisystem über SMB oder NFS generiert, werden diese Informationen über eine HTTP-Verbindung an den CEPA-Server weitergeleitet. Die CEE CEPA-Software auf dem Server empfängt das Ereignis und veröffentlicht es, sodass die Drittanbietersoftware es verarbeiten kann.

Zur Verwendung des Ereignisveröffentlichungsagenten benötigen Sie ein PowerStore-System mit mindestens einem im Netzwerk konfigurierten NAS-Server.

Weitere Informationen zu CEPA, das Teil des Common Event Enabler (CEE) ist, finden Sie im Abschnitt *Verwenden des Common Event Enabler auf Windows-Plattformen* auf der Dell Technologies Supportwebsite.

Erstellen eines Veröffentlichungspools

Voraussetzungen

Um einen Ereignisveröffentlichungspool zu erstellen, müssen Sie über einen CEPA-Server-FQDN (Events Publishing) verfügen.

Info über diese Aufgabe

Ein Ereignisveröffentlichungspool definiert den CEPA-Server und die spezifischen Ereignisse, die Benachrichtigungen auslösen. Definieren Sie mindestens eine der folgenden Ereignisoptionen:

- Vorabereignisse: Ereignisse, die vor der Verarbeitung zur Genehmigung an den CEPA-Server gesendet werden.
- Folgeereignisse: Ereignisse, die nach ihrem Auftreten für Protokollierungs- oder Auditingzwecke an den CEPA-Server gesendet werden.
- Fehlerfolgeereignisse: Fehlerereignisse, die nach ihrem Auftreten für Protokollierungs- oder Auditingzwecke an den CEPA-Server gesendet werden.

Schritte

1. Wählen Sie die Optionen **Storage** > **NAS Servers** aus.
2. Wählen Sie **NAS-Einstellungen**.
3. Wählen Sie im Fenster **Ereignisveröffentlichung** die Option **Veröffentlichungspools** und dann **Erstellen** aus.
4. Geben Sie einen **Poolnamen** ein.
5. Geben Sie den CEPA-Server-FQDN ein.
6. Klicken Sie im Abschnitt „Ereigniskonfiguration“ auf die Ereignistypen und wählen Sie die Ereignisse aus, die Sie dem Pool hinzufügen möchten.
7. Klicken Sie auf **Übernehmen**, um den Ereignisveröffentlichungspool zu erstellen.

Erstellen eines Ereignis-Publishers

Info über diese Aufgabe

Erstellen Sie nach der Konfiguration von Veröffentlichungspools einen Ereignis-Publisher, um die Antwort auf die verschiedenen Ereignistypen festzulegen.

ANMERKUNG: Ereignis-Publisher werden auf Systemebene erstellt und ein Ereignis-Publisher kann mehreren NAS-Servern zugeordnet werden.

Schritte

1. Wählen Sie die Optionen **Storage** > **NAS Servers** aus.
2. Wählen Sie **NAS-Einstellungen**.
3. Wählen Sie **Ereignis-Publisher** und dann **Erstellen** aus.
4. Befolgen Sie die Anweisungen des Assistenten **Ereignis-Publisher erstellen** aus.

Assistentenfenster	Description
Veröffentlichungspools auswählen	• Geben Sie einen Namen ein. • Wählen Sie bis zu 3 Veröffentlichungspools aus. Um einen neuen Veröffentlichungspool zu erstellen, klicken Sie auf **Erstellen**.
Konfigurieren des Ereignis-Publishers	• Vorabereignis-Fehler-Policy: Wählen Sie das gewünschte Verhalten aus, wenn alle CEPA-Server für Vorabereignisse offline sind: ○ Ignorieren (Standardeinstellung): Davon ausgehen, dass alle Ereignisse bestätigt werden. ○ Verweigern: Verweigern von Ereignissen, die eine Genehmigung erfordern, bis CEPA-Server online sind. • Folgeereignis-Fehler-Policy: Wählen Sie das gewünschte Verhalten aus, wenn alle CEPA-Server für Folgeereignisse offline sind: ○ Ignorieren (Standardeinstellung): Fortsetzen des Betriebsvorgangs. Ereignisse, die während des Ausfalls der CEPA-Server aufgetreten sind, gehen verloren. ○ Akkumulieren: Fortsetzen des Betriebsvorgangs und Speichern von Ereignissen in einem lokalen Puffer (bis zu 500 MB). ○ Garantieren: Fortsetzen des Betriebsvorgangs und Speichern von Ereignissen in einem lokalen Puffer (bis zu 500 MB). Verweigern des Zugriffs, wenn der Puffer voll ist. ○ Verweigern: Verweigern des Zugriffs auf Dateisysteme, wenn die CEPA-Server offline sind. • HTTP/Microsoft RPC • HTTP-Port

5. Wählen Sie **Übernehmen** aus, um den Ereignis-Publisher zu erstellen.

Aktivieren eines Ereignis-Publishers für einen NAS-Server

Info über diese Aufgabe

Nachdem Sie einen Ereignis-Publisher konfiguriert haben, müssen Sie ihn für den NAS-Server und alle darauf definierten Dateisysteme aktivieren.

Schritte

1. Wählen Sie die Optionen **Storage** > **NAS-Server** > **[NAS-Server]** aus.
2. Wählen Sie auf der Seite **Sicherheit & Ereignisse** die Option **Ereignisveröffentlichung** aus.
3. Wählen Sie einen Ereignis-Publisher aus der Liste aus und aktivieren Sie ihn.
4. Wählen Sie aus, ob der Ereignis-Publisher für alle Dateisysteme aktiviert werden soll, die auf dem NAS-Server definiert sind.
   Alternativ können Sie den Ereignis-Publisher nur für bestimmte Dateisysteme aktivieren. Weitere Informationen finden Sie unter Aktivieren des Ereignis-Publishers für das Dateisystem.
5. Klicken Sie auf **Anwenden**.

Aktivieren des Ereignis-Publishers für ein Dateisystem

Info über diese Aufgabe

Sie können den Ereignis-Publisher für ausgewählte Dateisysteme aktivieren.

Schritte

1. Wählen Sie die Optionen **Storage** > **Dateisysteme** > **[Dateisystem]** Kontingente aus.
2. Wählen Sie auf der Seite **Schutz** die Option **Ereignisveröffentlichung** aus.
3. Aktivieren Sie den Ereignis-Publisher für das Dateisystem und wählen Sie das Protokoll aus.
4. Klicken Sie auf **Anwenden**.