Dell PowerStore

Konfigurieren von NFS

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:

NFS-Support

PowerStore T-Modell und PowerStore Q-Modell unterstützen NFSv3 und NFSv4. Außerdem unterstützen diese Modelle Secure NFS mit Kerberos für eine starke Authentifizierung. PowerStore T-Modell und PowerStore Q-Modell unterstützen zwar die meisten der in den entsprechenden RFCs beschriebenen Funktionen von NFSv4 und NFSv4.1, bieten aber keine Unterstützung für die Verzeichnisdelegierung und pNFS. Ab PowerStore 3.0 und höher ist auch Basissupport für NFSv4.2 im Kompatibilitätsmodus verfügbar.

Die NFS-Unterstützung wird während oder nach der Erstellung auf einem NAS-Server aktiviert, sodass Sie NFS-fähige Dateisysteme auf diesem NAS-Server erstellen können.

Informationen über sicheres NFS

Sie können beim Erstellen oder Ändern eines NAS-Servers, der UNIX-Freigaben unterstützt, sicheres NFS konfigurieren. Sicheres NFS bietet eine Kerberos-basierte Nutzerauthentifizierung, die Integrität und Sicherheit für Netzwerkdaten bereitstellen kann.

Kerberos ist ein verteilter Authentifzierungsservice, der für eine starke Authentifizierung eine Verschlüsselung mit einem geheimen Schlüssel verwendet. Er funktioniert auf Basis von "Tickets", die es Nodes ermöglichen, über ein nicht sicheres Netzwerk zu kommunizieren, um ihre Identität auf sichere Weise nachzuweisen. Wenn der NFS-Server als sicherer NFS-Server konfiguriert wurde, verwendet dieser das Sicherheits-Framework RPCSEC_GSS und das Kerberos-Authentifizierungsprotokoll, um Benutzer und Services zu überprüfen.

Sicherheitsoptionen

Sicheres NFS unterstützt die folgenden Sicherheitsoptionen:

- krb5: Kerberos-Authentifizierung.
- krb5i: Kerberos-Authentifizierung und Datenintegrität durch Hinzufügen einer Signatur zu jedem über das Netzwerk übertragenen NFS-Paket.
- krb5p: Kerberos-Authentifizierung, Datenintegrität und Datenschutz durch Verschlüsselung der Daten vor der Übertragung über das Netzwerk.

  Die Datenverschlüsselung erfordert zusätzliche Ressourcen für die Systemverarbeitung und kann zu einer langsameren Performance führen.

In einer sicheren NFS-Umgebung wird der Benutzerzugriff auf NFS-Dateisysteme basierend auf Kerberos-Prinzipalnamen gewährt. Die Zugriffskontrolle für Freigaben innerhalb eines Dateisystems basiert jedoch auf der UNIX-UID und -GID oder auf ACLs.

ANMERKUNG: Sicheres NFS unterstützt die NFS-Zugangsdaten mit mehr als 16 Gruppen, was der Option für erweiterte UNIX-Zugangsdaten entspricht.

Konfigurieren von sicherem NFS

Wenn Sie sicheres NFS implementieren, konfigurieren Sie Folgendes:

- Es muss mindestens ein NTP-Server auf der PowerStore-Appliance konfiguriert sein, 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.
- Ein UNIX-Verzeichnisdienst (UDS)
- Ein oder mehrere DNS-Server
- Für die Kerberos-Authentifizierung muss entweder ein Active Directory- oder ein benutzerdefinierter Bereich hinzugefügt werden.
- Eine Keytab-Datei muss auf Ihren NAS-Server hochgeladen werden, wenn Sie einen benutzerdefinierten Bereich in einer Kerberos-Konfiguration verwenden.

Überlegungen zur Planung

Überprüfen Sie die folgenden Informationen, bevor Sie NFS-Exports konfigurieren:

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

NAS-Servernetzwerke

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.

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.

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

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.

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 NFS-Dateisysteme.

Erstellen von NFS-Exporten

Führen Sie die folgenden Verfahren aus, damit Sie NFS-Exporte in PowerStore erstellen können:

1. Erstellen von NAS-Servern mit NFS-Protokoll
2. Erstellen eines Dateisystems für NFS-Exporte

Dokumentationsressourcen

Weitere Informationen finden Sie in den folgenden Themen:

Tabelle 1. Dokumentationsressourcen

Dokument	Beschreibung	Position
PowerStore T und Q – Netzwerkleitfaden für Storage-Services	Das Dokument enthält Informationen zur Netzwerkplanung und -konfiguration.	dell.com/powerstoredocs
PowerStore – Handbuch für die Konfiguration von SMB	Das Dokument enthält Informationen, die zum Konfigurieren von SMB-Freigaben mit PowerStore Manager erforderlich sind.	
Whitepaper zu Dateifunktionen von PowerStore	Das Dokument beschreibt die Funktionen und Protokolle, die von der Dell PowerStore-Dateiarchitektur unterstützt werden.	
PowerStore-Onlinehilfe	Die 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

Damit Sie Dateispeicher auf dem Speichersystem bereitstellen können, muss ein NAS-Server auf dem System ausgeführt werden. Ein NAS-Server ist ein Dateiserver, der das SMB-Protokoll, das NFS-Protokoll oder beide Protokolle 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 NFS-Protokoll beschrieben, auf dem Dateisysteme mit NFS-Exporten erstellt werden können.

Erstellen eines NAS-Servers für NFS-Dateisysteme

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

Vergewissern Sie sich, dass Ihre NAS-Netzwerkinformationen verfügbar sind.

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 • 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 **ANMERKUNG:** Sie können keine VLANs wiederverwenden, die für die Management- und Storage-Netzwerke verwendet werden.
Sharing Protocol	**Select Sharing Protocol** Wählen Sie NFSv3 oder NFSv4 oder beides aus. **ANMERKUNG:** Wenn Sie SMB und ein NFS-Protokoll auswählen, aktivieren Sie automatisch den NAS-Server für die Unterstützung mehrerer Protokolle. Weitere Informationen zu Multiprotokoll-

Bildschirm „Wizard“	Beschreibung
	Dateifreigaben finden Sie in *Dell PowerStore – Konfigurieren von Multiprotokoll-Dateifreigaben* auf der Dokumentationsseite zu PowerStore. **Unix Directory Services** (Namensservices) Sie können die Namensservices mit einer Kombination aus lokalen Dateien und NIS oder LDAP konfigurieren. Details finden Sie in einem den folgenden Abschnitten: ● Verwenden von lokalen Dateien ● Mit NIS ● Mit LDAP Sie können hier sicheres NFS aktivieren. Sicheres NFS erfordert Folgendes: ● Es muss mindestens ein NTP-Server auf der PowerStore-Appliance konfiguriert sein, 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. ● Ein UNIX-Verzeichnisdienst (UDS) ● Ein oder mehrere DNS-Server ● Für die Kerberos-Authentifizierung muss entweder ein Active Directory- oder ein benutzerdefinierter Bereich hinzugefügt werden. ● Eine Keytab-Datei muss auf Ihren NAS-Server hochgeladen werden, wenn Sie einen benutzerdefinierten Bereich in einer Kerberos-Konfiguration verwenden. **DNS** DNS-Serverinformationen sind in den folgenden Fällen obligatorisch: ● Beitritt zu einer AD-Domain, aber optional für einen eigenständigen NAS-Server ● Konfigurieren von sicherem NFS DNS kann auch verwendet werden, um Hosts aufzulösen, die in NFS-Export-Zugriffslisten definiert sind.
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, um den NAS-Server zu erstellen.
   Das Fenster **Status** wird geöffnet und Sie werden zur Seite **NAS Servers** umgeleitet, sobald der Server auf der Seite aufgeführt wird.

Nachdem Sie den NAS-Server für NFS erstellt haben, können Sie mit der Konfiguration der Servereinstellungen fortfahren.

Wenn Sie sicheres NFS aktiviert haben, müssen Sie mit der Konfiguration von Kerberos fortfahren.

Wählen Sie den NAS-Server aus, um mit der Konfiguration fortzufahren, oder bearbeiten Sie die NAS-Servereinstellungen.

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

Konfigurieren von Namensservices für NAS-Server

Sie können die Namensservices für einen NAS-Server konfigurieren oder ändern.

Die Namensservices umfassen das Konfigurieren einer oder mehrerer der folgenden Komponenten:

- DNS
- NIS für Unix-Verzeichnisdienste (UDS)
- LDAP für UDS
- Lokale Dateien

Konfigurieren von DNS

Sie können DNS deaktivieren oder einen NAS-Server aktivieren und konfigurieren, um DNS zu verwenden.

DNS kann auch verwendet werden, um die in NFS-Exportzugriffslisten definierten Hosts aufzulösen.

DNS ist erforderlich für:

- Sicheres NFS
- Verknüpfen mit einer AD-Domain

Sie können DNS für NAS-Server nicht deaktivieren, wenn diese mit folgenden Funktionen konfiguriert wurden:

- Multiprotokoll-Dateifreigabe
- SMB-Dateifreigabe, die mit einem Active Directory (AD) verknüpft wird
- Sicheres NFS

1. Wählen Sie die Optionen **Storage** > **NAS Servers** > **[NAS-Server]** > **DNS** aus.
2. Aktivieren oder deaktivieren Sie DNS. Wenn Sie DNS aktiviert haben, geben Sie die DNS-Serverinformationen ein.

Konfigurieren des UNIX-Verzeichnisdienstes für NAS-Server für NIS

Sie können für NIS einen UNIX-Verzeichnisdienst (UDS) für NAS-Server konfigurieren.

1. Wählen Sie die Optionen **Storage** > **NAS Servers** > **[NAS-Server]** > **Naming Services** > **Karte UDS** aus.
2. Wenn die Option **Disabled** aktiviert ist, schieben Sie die Schaltfläche, um zu **Enabled** zu wechseln.
3. Wählen Sie aus der Drop-down-Liste **Unix Directory Service** die Option **NIS** aus.
4. Geben Sie eine NIS-**Domain** ein, und fügen Sie die IP-**Addresses** für die NIS-Server hinzu.
5. Klicken Sie auf **Anwenden**.

Um Probleme bei der Konfiguration eines UDS mithilfe von NIS zu beheben, vergewissern Sie sich, dass Sie die Domain und die IP-Adressen des NIS-Servers richtig eingegeben haben.

Konfigurieren eines UNIX-Verzeichnisdiensts für NAS-Server mithilfe von LDAP

Sie können mithilfe von LDAP einen UNIX-Verzeichnisdienst (UDS) für NAS-Server konfigurieren.

LDAP muss dem IDMU-, RFC2307- oder RFC2307bis-Schema entsprechen. Einige Beispiele hierfür sind AD-LDAP mit IDMU, iPlanet und OpenLDAP. Der LDAP-Server muss ordnungsgemäß konfiguriert werden, um UIDs für jeden Benutzer bereitzustellen. Zum Beispiel muss der Administrator auf der IDMU die Eigenschaften der jeweiligen Benutzer aufrufen und auf der Registerkarte „UNIX-Attribute“ eine UID hinzufügen.

Sie können LDAP für die Verwendung von anonymer, einfacher und Kerberos-Authentifizierung konfigurieren. Wenn Sie die Kerberos-Authentifizierung verwenden, müssen Sie Folgendes konfigurieren, bevor Sie mit dem Konfigurieren von LDAP mit Kerberos fortfahren:

1. Konfigurieren Sie auf der Karte **Naming Services** den DNS-Server, der dazu dient, einen Kerberos-Server mit einem Bereich zu verknüpfen bzw. die Verknüpfung aufzuheben.
2. Fügen Sie den Kerberos-Bereich auf der Karte **Security** hinzu.

1. Wählen Sie die Optionen **Storage** > **NAS Servers** > **[NAS-Server]** > **Naming Services** > **Karte UDS** aus.
2. Wenn die Option **Disabled** aktiviert ist, schieben Sie die Schaltfläche, um zu **Enabled** zu wechseln.
3. Wählen Sie im Drop-Down-Menü **Unix Directory Service** die Option **LDAP** aus.
4. Behalten Sie den Standardwert bei oder geben Sie im Feld **Port Number** einen anderen Port ein.

   ANMERKUNG: LDAP verwendet standardmäßig Port 389 und LDAPS (LDAP over SSL) verwendet Port 636.

5. Fügen Sie die IP-Adressen für die LDAP-Server hinzu.

   Der NAS-Server kann so konfiguriert werden, dass die DNS-Serviceerkennung verwendet wird, um die IP-Adressen des LDAP-Servers automatisch abzurufen.

   ANMERKUNG: Damit dieser Erkennungsprozess funktioniert, muss der DNS-Server Pointer zu den LDAP-Servern enthalten und die LDAP-Server müssen die gleichen Authentifizierungseinstellungen verwenden.

6. Konfigurieren Sie die LDAP-Authentifizierung, wie in der folgenden Tabelle beschrieben.

Option	Beschreibung
Anonym	Geben Sie den Basis-DN und den Profil-DN für den iPlanet/OpenLDAP-Server an.
Einfach	Geben Sie Folgendes an: ● Bei Verwendung von AD, LDAP/IDMU: ○ Bindungs-DN im LDAP-Notationsformat, z. B. **cn=administrator,cn=users,dc=svt,dc=lab,dc=com** ○ Basis-DN im X.509-Format (z. B. **dc=svt,dc=lab,dc=com**). ○ Profil-DN. ● Bei Verwendung des iPlanet-/OpenLDAP-Servers: ○ Bindungs-DN im LDAP-Notationsformat, z. B. **cn=administrator,cn=users,dc=svt,dc=lab,dc=com** ○ Password ○ Basis-DN Beispiel: Bei Verwendung von **svt.lab.com** wäre die Basis-DN **DC=svt,DC=lab,DC=com** ○ Profil-DN (optional) – Für den iPlanet-/OpenLDAP-Server
Kerberos	Konfigurieren Sie einen nutzerdefinierten Bereich, der auf alle Arten von Kerberos-Bereichen (Windows, MIT, Heimdal) zeigt. Mit dieser Option verwendet der NAS-Server den nutzerdefinierten Kerberos-Bereich, der im Unterabschnitt „Kerberos“ der Registerkarte **Sicherheit** des NAS-Servers definiert ist. **ANMERKUNG:** Wenn Sie sicheres NFS mit einem benutzerdefinierten Bereich verwenden, müssen Sie eine Keytab-Datei hochladen.

7. Wählen Sie **Retrieve Current Schema** aus, um die Datei „ldap.conf“ herunterzuladen.
8. Bearbeiten und speichern Sie die Datei `ldap.conf`.
9. Wählen Sie **Upload New Schema** aus , um die aktualisierte Datei `ldap.conf` hochzuladen.
10. Aktivieren Sie optional „LDAP Secure (Use SSL)“ und laden Sie das CA-Zertifikat hoch.

Um Probleme bei der Konfiguration eines UDS mithilfe von LDAP zu beheben, stellen Sie Folgendes sicher:

- Die LDAP-Konfiguration entspricht einem der unterstützten Schemas, wie zuvor in diesem Thema beschrieben.
- Die Container, die in der Datei `ldap.conf` angegeben sind, zeigen auf gültige und vorhandene Container.
- Jeder LDAP-Benutzer wird mit einer eindeutigen UID konfiguriert.

Konfigurieren des NAS-Servers zur Verwendung lokaler Dateien für Namensservices

Sie können Ihre Namensservices zur Verwendung lokaler Dateien konfigurieren.

- Lokale Dateien können anstelle von oder auch mit DNS-, LDAP- und NIS-Verzeichnisdiensten verwendet werden.
- Wenn Sie lokale Dateien mit einem UNIX-Verzeichnisdienst (UDS) konfigurieren, fragt das Speichersystem zuerst die lokalen Dateien ab.
- Nachdem Sie die Erstellung des NFS-Servers abgeschlossen haben, können Sie zurück navigieren und weitere lokale Dateien hochladen.
- Wenn der NAS-Server erstellt wurde, aktivieren Sie die lokalen Dateien wie in den folgenden Schritten beschrieben:

1. Wählen Sie die Optionen **Storage** > **NAS Servers** > **[NAS-Server]** > **Naming Services** > **Local Files** aus.
2. Klicken Sie für jeden Typ lokaler Dateien auf den Pfeil nach unten, um die aktuelle Datei herunterzuladen. Wenn keine Datei auf dem Speichersystem vorhanden ist, lädt das System eine Vorlage herunter.
3. Aktualisieren Sie die Datei mit den Systeminformationen.

   Um lokale Dateien für den FTP-Zugriff zu verwenden, muss die Datei `passwd` ein verschlüsseltes Kennwort für die Nutzer enthalten. Dieses Passwort wird nur für FTP-Zugriff verwendet. Die Datei `passwd` verwendet das gleiche Format und die gleiche Syntax wie ein standardmäßiges UNIX-System, daher können Sie das Kennwort anwenden, um die lokale `passwd`-Datei zu erzeugen. Verwenden Sie auf einem UNIX-System den Befehl `useradd`, um einen Nutzer hinzuzufügen, und `passwd`, um das Kennwort für diesen Nutzer festzulegen. Kopieren Sie dann das Hash-Kennwort aus der Datei `/etc/shadow`, fügen Sie es in das zweite Feld in der Datei `/etc/passwd` ein und laden Sie die Datei `/etc/passwd` auf den NAS-Server hoch.
4. Speichern Sie die aktualisierte Datei auf Ihrem lokalen Rechner.
5. Wählen Sie **Upload Local Files** aus, navigieren Sie zum Speicherort der bearbeiteten Datei, und wählen Sie die hochzuladende Datei aus.
6. Wiederholen Sie diese Schritte für jeden Dateityp.

Um Probleme bei der Konfiguration von lokalen Dateien zu beheben, stellen Sie Folgendes sicher:

- Die Datei wurde mit der richtigen Syntax erstellt. (Sechs Doppelpunkte sind für jede Codezeile erforderlich.) Weitere Informationen zur Syntax und Beispiele erhalten Sie in der Vorlage.
- Jeder Benutzer verfügt über einen eindeutigen Namen und eine eindeutige UID.

Konfigurieren von NAS-Serverfreigabeprotokollen

Sie können die für einen NAS-Server konfigurierten Freigabeprotokolle konfigurieren oder ändern.

Das Konfigurieren der NFS-Freigabeprotokolle beinhaltet die Einrichtung einer oder mehrerer der folgenden Komponenten:

- NFS-Server
- FTP

Konfigurieren des NFS-Servers

Konfigurieren Sie den NAS-Server nur für UNIX-Systeme oder ändern Sie die Einstellungen des NFS-Servers.

Vor der Konfiguration eines sicheren NFS-Servers müssen DNS und NTP konfiguriert werden.

1. Wählen Sie die Optionen **Storage** > **NAS Servers** > **[NAS-Server]** > **Sharing Protocols** > **NFS Server** aus.
2. Aktivieren Sie die Option **Linux/UNIX shares**, um den NAS-Server für UNIX-Unterstützung zu definieren.
3. Aktivieren Sie entweder **NFSv3**, **NFSv4** oder beide Optionen.
4. Optional können Sie sicheres NFS aktivieren oder deaktivieren.
   Die erweiterten UNIX-Zugangsdaten sind ebenfalls aktiviert.
5. Aktivieren oder deaktivieren Sie die Zugangsdaten für **Enable or disable Extend Unix**.

   ANMERKUNG: Sicheres NFS unterstützt die NFS-Zugangsdaten mit mehr als 16 Gruppen, was der Option für erweiterte UNIX-Zugangsdaten entspricht.

   - Wenn dieses Feld aktiviert ist, verwendet der NAS-Server die Benutzer-ID (UID), um die primäre Gruppen-ID (GID) und alle Gruppen-GIDs, zu denen sie gehört, abzurufen. Der NAS-Server ruft die GIDs aus der lokalen Kennwortdatei oder dem UDS ab.
   - Wenn dieses Feld deaktiviert ist, werden die UNIX-Zugangsdaten der NFS-Anforderung direkt aus den Netzwerkinformationen extrahiert, die im Frame enthalten sind. Diese Methode bietet bessere Performance, ist jedoch auf höchstens 16 Gruppen-GIDs beschränkt.
6. Geben Sie im Feld **Credential Cache Retention** einen Zeitraum (in Minuten) an, über den Zugangsdaten im Cache aufbewahrt werden sollen.
7. Klicken Sie auf **Apply**, um die Änderungen zu übernehmen.

Konfigurieren des FTP- oder SFTP-Freigabeprotokolls

Sie können die FTP- oder SFTP (FTP over SSH)-Einstellungen nur für einen vorhandenen NAS-Server konfigurieren.

Der passive FTP-Modus wird nicht unterstützt.

Der FTP-Zugriff kann mit den gleichen Methoden wie NFS authentifiziert werden. Nachdem die Authentifizierung abgeschlossen wurde, erfolgt der Zugriff genauso wie NFS zu Sicherheits- und Berechtigungszwecken. Wenn das Format nicht `user@domain` oder `domain\user` ist, wird die NFS-Authentifizierung verwendet. Die NFS-Authentifizierung verwendet lokale Dateien, LDAP, NIS oder lokale Dateien mit LDAP oder NIS.

Um lokale Dateien für den NFS-FTP-Zugriff zu verwenden, muss die Datei `passwd` ein verschlüsseltes Kennwort für die Nutzer enthalten. Dieses Passwort wird nur für FTP-Zugriff verwendet. Die Datei `passwd` verwendet das gleiche Format und die gleiche Syntax wie ein standardmäßiges Unix-System, daher können Sie dies nutzen, um die lokale Datei `passwd` zu erzeugen. Verwenden Sie auf einem Unix-System den Befehl `useradd`, um einen neuen Nutzer hinzuzufügen, und den Befehl `passwd`, um das Kennwort für diesen Nutzer festzulegen. Kopieren Sie dann das Hash-Kennwort aus der Datei `/etc/shadow`, fügen Sie es in das zweite Feld in der Datei `/etc/passwd` ein und laden Sie die Datei `/etc/passwd` auf den NAS-Server hoch. Weitere Informationen zum Hochladen der Datei `/etc/passwd` finden Sie unter Konfigurieren des NAS-Servers zur Verwendung lokaler Dateien für Benennungsservices.

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 unter **FTP/SFTP Server Access** den Typ der authentifizierten Nutzer aus, die Zugriff auf die Dateien haben.
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 **Welcome message** und die **Message of the day** eingeben.
7. Optional können Sie die **Access Control List** anzeigen, um Zugriff auf **Filtered Users**, **Filtered Groups** und **Filtered hosts** zu gewähren oder zu verweigern.
8. Klicken Sie auf **Anwenden**.

Konfigurieren von Kerberos für die NAS-Serversicherheit

Sie können den NAS-Server mit Kerberos konfigurieren.

Kerberos ist ein verteilter Authentifzierungsservice, der für eine starke Authentifizierung eine Verschlüsselung mit einem geheimen Schlüssel verwendet. Er funktioniert auf Basis von "Tickets", die es Nodes ermöglichen, über ein nicht sicheres Netzwerk zu kommunizieren, um ihre Identität auf sichere Weise nachzuweisen. Wenn der NFS-Server als sicherer NFS-Server konfiguriert wurde, verwendet dieser das Sicherheits-Framework RPCSEC_GSS und das Kerberos-Authentifizierungsprotokoll, um Benutzer und Services zu überprüfen.

Wenn der NAS-Server nur mit NFS konfiguriert wurde und Sie sicheres NFS oder LDAP mit Kerberos konfigurieren, müssen Sie vor der Konfiguration der Sicherheit in PowerStore Kerberos mit einem nutzerdefinierten Bereich konfigurieren.

Wenn der NAS-Server sowohl mit dem NFS- als auch dem SMB-Protokoll konfiguriert wurde, haben Sie die Möglichkeit, Kerberos zu verwenden, der mit AD übernommen wird, da der mit der Domain verbundene SMB-Server auf dem NAS Server vorhanden ist.

Das Speichersystem muss mit einem NTP-Server konfiguriert werden. Kerberos ist abhängig von der korrekten Zeitsynchronisation zwischen KDC, Servern und Client im Netzwerk.

Konfigurieren von Kerberos für sicheres NFS

Beachten Sie bei der Konfiguration von Kerberos für sicheres NFS Folgendes:

- Wenn der NAS-Server nur für NFS konfiguriert wird, müssen Sie den NAS-Server mit einem benutzerdefinierten Bereich konfigurieren. Wenn Sie den NAS-Server mit NFS und SMB konfiguriert haben, können Sie den AD- oder den benutzerdefinierten Bereich verwenden.
- Die Verwendung von LDAPS oder LDAP mit Kerberos wird für höhere Sicherheit empfohlen.
- Auf der NAS-Serverebene muss ein DNS-Server konfiguriert sein. Alle Mitglieder des Kerberos-Bereichs, einschließlich KDC, NFS-Server und NFS-Clients, müssen auf dem DNS-Server registriert werden.
- Der vollständig qualifizierte Domainname für den Hostnamen des NFS-Clients und der vollständig qualifizierte Domainname des NAS-Servers müssen auf dem DNS-Server registriert sein. Clients und Servern müssen die vollständig qualifizierten Domainnamen jedes Mitglieds des Kerberos-Bereichs in eine IP-Adresse auflösen können.
- Der vollständig qualifizierte Domainnamenteil des NFS-Client-SPN muss auf dem DNS-Server registriert sein.
- Wenn ein sicheres NFS konfiguriert wird, muss eine Keytab-Datei auf Ihren NAS-Server hochgeladen werden.

Erstellen eines nutzerdefinierten Bereichs für Kerberos

Sie können einen nutzerdefinierten Bereich für die Verwendung mit Kerberos konfigurieren.

Mit einem nutzerdefinierten Kerberos-Bereich können Sie jede Art von KDC (MIT/Heimdal oder AD) konfigurieren. Verwenden Sie diese Methode, wenn Sie nicht über eine auf dem NAS-Server konfigurierte SMB-Serverdomain verfügen oder einen anderen Kerberos-Bereich als den für den SMB-Server konfigurierten verwenden möchten.

Erstellen eines nutzerdefinierten Bereichs für einen reinen NFS-Server

Wenn Sie ein UNIX-basiertes KDC verwenden möchten, führen Sie vor dem Konfigurieren von Kerberos in PowerStore die folgenden Schritte aus. Bei den Schritten wird davon ausgegangen, dass Sie „myrealm“ im Kerberos-Bereich „linux.dellemc.com“ als Hostname des NFS-Servers verwenden möchten.

1. Führen Sie das Tool `kadmin.local` aus.
2. Erstellen Sie die Prinzipale und ihre Schlüssel:

```
kadmin.local: addprinc -randkey nfs/myrealm.linux.dellemc.com
```

und/oder

```
kadmin.local: addprinc -randkey nfs/myrealm
```

3. Legen Sie den Schlüssel des Prinzipals in der Keytab-Datei „myrealm.linux.dellemc.fr“ ab:

```
kadmin.local: ktadd -k myrealm.linux.dellemc.com.keytab nfs/myrealm.linux.dellemc.fr
```

Erstellen eines nutzerdefinierten Bereichs für Multiprotokoll-NAS-Server (NFS und SMB)

Wenn Sie ein Windows-basiertes KDC ohne Verwendung des SMB-Serverkontos auf dem NAS-Server nutzen möchten, führen Sie vor dem Konfigurieren von Kerberos in PowerStore die folgenden Schritte aus. Bei den Schritten wird davon ausgegangen, dass Sie „myrealm.windows.dellemc.com“ als den vollständig qualifizierten Domainnamen für den NFS-Server verwenden möchten.

1. Erstellen Sie das Konto „myrealm“ für den NAS-Server in Active Directory (AD) der Windows-Domain „windows.dellemc.com“.
2. Registrieren Sie den Service-SPN beim Computerkonto, das Sie erstellt haben:

```
C:\setspn -S nfs/myrealm.windows.dellemc.com myrealm
```

3. Überprüfen Sie, ob der SPN erstellt wurde.

```
C:\setspn myrealm
```

4. Erzeugen Sie eine Keytab-Datei für den SPN:

```
C:\ktpass -princ nfs/myrealm.windows.dellemc.com@WINDOWS.DELLEMC.COM -mapuser
WINDOWS\myrealm
 -crypto ALL +rndpass -ptype KRB5_NT_PRINCIPAL -out myrealm.windows.dellemc.com.keytab
```

Konfigurieren der Kerberos-Sicherheit für den NAS-Server

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

Wenn Sie die Konfiguration für NFS vornehmen, müssen DNS und UDS für den NAS-Server konfiguriert und alle Mitglieder des Kerberos-Bereichs im DNS-Server registriert sein.

Wenn Sie einen NAS-Server verwenden, der für SMB und NFS konfiguriert ist, fügen Sie den SMB-Server zur Active Directory-Domain hinzu.

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 Address** ein, und klicken Sie auf **Add**.
5. Geben Sie den TCP-Port ein, der von Kerberos verwendet werden soll. Der Standardport ist 88.
6. Klicken Sie auf **Apply**.

Wenn Sie sich dafür entscheiden, nach der erfolgreichen Erstellung des NAS-Servers mit sicherem NFS von einem AD-Bereich zu einem nutzerdefinierten Bereich zu wechseln, können Sie NFS-Exporte erst mounten, nachdem Sie die folgenden Verfahren durchgeführt haben:

1. Erstellen Sie eine Keytab-Datei.
2. Entfernen Sie den AD-Bereich vom NAS-Server.

3. Geben Sie den Nutzernamen und das Kennwort für den AD-Server ein.
4. Geben Sie den benutzerdefinierten Bereich ein.
5. Laden Sie die Keytab-Datei hoch.

3

Konfigurieren von NFS-Exporten

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Übersicht über Dateisysteme und NFS-Exporte

Beim Erstellen von Dateisystemen und NFS-Exporten ist Folgendes hilfreich:

- Ein NAS-Server muss so konfiguriert werden, dass er das NFS-Protokoll unterstützt, bevor ein Dateisystem erstellt wird.
- Sie können auswählen, ob Sie NFS-Exporte beim ersten Anlegen des Dateisystems hinzufügen wollen, oder ob Sie NFS-Exporte zu einem Dateisystem hinzufügen wollen, nachdem es bereits angelegt wurde.

Erstellen eines Dateisystems für NFS Exporte

Sie können ein Dateisystem für NFS-Exporte erstellen.

Vergewissern Sie sich, dass ein NAS-Server für die Unterstützung des NFS-Protokolls konfiguriert wurde.

1. Wählen Sie die Optionen **Storage** > **File Systems** aus.
2. Klicken Sie auf **Erstellen**.
   Der Assistent **Dateisystem hinzufügen** wird gestartet.
3. Wählen Sie **Allgemein** oder **VMware-Dateisystem** als Dateisystemtyp aus.

   ANMERKUNG: Das VMware-Dateisystem ist ein PowerStore-Dateisystem, das für VMware optimiert und für VMware-Workloads verwendet wird. Diese Option sollte nur für VMware NFS-Datenspeicher ausgewählt werden. Wählen Sie für alle anderen Dateisysteme **Allgemein** aus.

4. Wählen Sie einen NFS-fähigen NAS-Server für das Dateisystem aus.
5. Geben Sie die Details des Dateisystems an, einschließlich Name und Größe des Dateisystems, eine Mindestgröße von 3 GB und eine maximale Größe von 256 TB.

   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 die Modelle PowerStore T-Modell und PowerStore Q 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.

6. Optional können Sie den Dateiaufbewahrungstyp auswählen (nur für allgemeine Dateisysteme verfügbar):
   - Enterprise (FLR-E) – Schützt Inhalte vor Änderungen, die von NutzerInnen über NFS und FTP vorgenommen werden. Ein Administrator kann ein FLR-E-Dateisystem löschen, das geschützte Dateien enthält.
   - Compliance (FLR-C) – Schützt Inhalte vor Änderungen, die von Nutzern und Administratoren vorgenommen werden und mit den Anforderungen der SEC-Regel 17a-4(f) übereinstimmen. 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.

7. Konfigurieren Sie optional den ersten Export für das Dateisystem.

   ANMERKUNG: Sie können NFS-Exporte später zum Dateisystem hinzufügen.

8. Wenn Sie den ersten Export konfiguriert haben, konfigurieren Sie den Hostzugriff.

Option	Beschreibung
Minimum Security	Wählen Sie **Sys** aus, um Nutzern mit einem nicht sicheren NFS oder einem sicheren NFS das Mounten und den NFS-Export im Dateisystem zu ermöglichen. Wenn Sie kein sicheres NFS konfigurieren, müssen Sie diese Option auswählen. Wenn Sie ein Dateisystem mit sicherem NFS erstellen, stehen die folgenden Optionen zur Auswahl: • **Kerberos**, um jede Art von Kerberos-Sicherheit für die Authentifizierung (krb5/krb5i/krb5p) zuzulassen. • **Kerberos mit Integrität**, um Kerberos mit Integrität und Kerberos mit Verschlüsselungssicherheit für die Nutzerauthentifizierung (krb5i/krb5p) zu ermöglichen. • **Kerberos mit Verschlüsselung**, um nur Kerberos mit Verschlüsselungssicherheit für die Nutzerauthentifizierung (krb5p) zuzulassen.
Default Access	Der Typ des Zugriffs, der standardmäßig auf die Hosts angewendet wird. Optional können Sie einen anderen Typ von Zugriff auf den Host auswählen, wenn Sie einzelne Hosts hinzufügen. Zu den Optionen gehören: • **Kein Zugriff** – Es besteht kein Zugriff auf die Storage-Ressource oder die Freigabe. • **Lesen/Schreiben** – Hosts haben Lese- und Schreibzugriff auf den NFS-Datenspeicher oder die NFS-Freigabe. • **Schreibgeschützt** – Hosts haben die Berechtigung zur Anzeige des Inhalts der Storage-Ressource oder Freigabe, jedoch keinen Schreibzugriff. **ANMERKUNG:** ESXi-Hosts müssen über **Read//Write**-Zugriff verfügen, um einen NFS-Datenspeicher mithilfe von NFSv4 mit **Kerberos NFS owner**-Authentifizierung einzuhängen. • **Read/Write, allow Root**: Hosts haben Lese- und Schreibzugriff auf die Storage-Ressource oder die Freigabe und für andere Anmeldekonten, die auf den Speicher zugreifen, können sie widerrufene Zugriffsberechtigungen erteilen (beispielsweise die Berechtigung zum Lesen, Ändern und Ausführen bestimmter Dateien und Verzeichnisse). Das Root-Verzeichnis des NFS-Clients verfügt über Root-Zugriff auf die Share. **ANMERKUNG:** Wenn die Hosts nicht Teil einer unterstützten Clusterkonfiguration sind, vermeiden Sie es, mehr als einem Host Lese-/Schreibzugriff zu gewähren. **ANMERKUNG:** ESXi-Hosts müssen über **Lesen/Schreiben, Root zulassen**-Zugriff verfügen, um einen NFS-Datenspeicher mithilfe von NFSv4 mit „NFS-Eigentümer: root“-Authentifizierung zu mounten. • **Read-Only, allow Root** – Hosts verfügen über die Berechtigung zum Anzeigen des Inhalts der Freigabe, jedoch nicht über Schreibzugriff. Das Root-Verzeichnis des NFS-Clients verfügt über Root-Zugriff auf die Share.
Host hinzufügen	Geben Sie die Hosts einzeln. Sie können auch Hosts hinzufügen, indem Sie eine ordnungsgemäß formatierte CSV-Datei hochladen. Sie können die CSV-Datei zuerst herunterladen, um eine Vorlage zu erhalten. So können Sie eine CSV-Dateivorlage herunterladen, bearbeiten und verwenden: a. Klicken Sie auf das Symbol **Export Hosts**. b. Aktualisieren Sie die CSV-Datei mit den Hosts und den Zugriffstypen, die Sie importieren möchten. c. Speichern Sie die CSV-Datei auf Ihrem lokalen Rechner. d. Klicken Sie auf **Import CSV file**. e. Navigieren Sie zur CSV-Datei, und klicken Sie im Microsoft-Datei-Explorer-Fenster auf **Open**. Die Hosts aus der CSV-Datei werden in der **Import Host List** mit dem **Access Type** angezeigt, den Sie in der CVS-Datei definiert haben.

9. Fügen Sie optional eine Schutz-Policy zum Dateisystem hinzu.

   Wenn Sie dem Dateisystem eine Schutz-Policy hinzufügen, muss die Policy vor der Erstellung des Dateisystems erstellt worden sein. Die ausgewählte Schutz-Policy kann sowohl Snapshot- als auch Replikationsregeln enthalten.

10. Fügen Sie optional eine QoS-Policy zum Dateisystem hinzu.

    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.

11. Prüfen Sie die Informationen in der Übersicht und klicken Sie auf **Create File System**.
Das Dateisystem wird der Registerkarte **File System** hinzugefügt. Wenn Sie gleichzeitig einen Export erstellt haben, wird dieser auf der Registerkarte **NFS-Export** angezeigt.

Erstellen eines NFS-Exports

Sie können einen NFS-Export in einem Dateisystem erstellen.

1. Wählen Sie die Optionen **Storage** > **File Systems** > **NFS Export** aus.
2. Klicken Sie auf **Create**.
Der Assistent **Create NFS Export** wird geöffnet.
3. Geben Sie die erforderlichen Informationen ein und beachten Sie dabei Folgendes:
   - Wenn Sie einen Export basierend auf einem Snapshot erstellen möchten, müssen die Snapshots vor der Erstellung des NFS-Exports erstellt werden.
   - Der Name für **Local Path** muss mit einem vorhandenen Ordnernamen in dem Dateisystem übereinstimmen, das auf Hostseite erstellt wurde.
   - Der im Bereich **NFS-Exportdetails** im Feld **Name** angegebene Wert bildet zusammen mit der IP-Adresse des NAS-Servers den Exportpfad.

     ANMERKUNG: Sie können den Export auch über die IP-Adresse des NAS-Servers und den lokalen Pfad einhängen.

   - Die Namen des NFS-Exports müssen auf der Ebene des NAS-Servers für jedes Protokoll eindeutig sein. Sie können jedoch denselben Namen für eine SMB-Freigabe sowie für NFS-Exporte angeben.
4. Nachdem Sie die Einstellungen akzeptiert haben, klicken Sie auf **Create NFS Export**.
Der NFS-Export wird auf der Seite **NFS Export** angezeigt.

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

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.

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

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.

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**.

4

Weitere Funktionen des NAS-Servers

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Festlegen des bevorzugten UNIX-Verzeichnisdiensts

Nachdem Sie einen NAS-Server erstellt haben, können Sie die Suchreihenfolge für den bevorzugten UNIX-Verzeichnisdienst (UDS) für den Nutzerzugriff festlegen.

1. Wählen Sie die Optionen **Storage** > **NAS Servers** aus.
2. Aktivieren Sie das Kontrollkästchen in der Spalte **Name** links neben dem NAS-Server.
3. Klicken Sie auf **Bearbeiten**.
4. Wählen Sie die bevorzugte UDS-Suchreihenfolge aus der Dropdownliste **Unix Directory Service Search Order** aus.
5. Klicken Sie auf **Apply**.

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.

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.

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.

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

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.

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.

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

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**.

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

5

Weitere Dateisystemfunktionen

Dieses Kapitel enthält die folgenden Informationen:

Themen:

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 2. Quota-Typen

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

Typ	Beschreibungen
Hart	Ein hartes Limit ist ein absoluter Grenzwert für die Storage-Nutzung.

Tabelle 3. Harte und weiche Limits (fortgesetzt)

Typ	Beschreibungen
	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.

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.

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.

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

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

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.

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)

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

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

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.

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.

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

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

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

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

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).

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

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

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

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.

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

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

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.

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

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.

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

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

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

Sie können den Ereignis-Publisher für ausgewählte Dateisysteme aktivieren.

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**.