Dell PowerStore

Konfigurieren von Multiprotokoll-Dateifreigaben

4.1

Februar 2025
Rev. A01

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.

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.

Inhaltsverzeichnis

1

Übersicht

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Multiprotokoll-Dateifreigabe in PowerStore

Für den Zugriff auf eine Datendatei, die von einem NAS-Server über das Netzwerk freigegeben wird, verwenden Host-Clients hauptsächlich zwei Dateiprotokolle: SMB und NFS. Windows-Clients nutzen das SMB-Protokoll und UNIX-Clients verwenden das NFS-Protokoll. Die NFS- und SMB-Protokolle weisen viele Unterschiede auf, einschließlich der in der folgenden Tabelle beschriebenen:

Tabelle 1. Hauptunterschiede zwischen den NFS- und SMB-Protokollen

Funktion	NFS	SMB
Benutzeridentifikation	Verwendet eine Unix-Nutzerkennung (UID) und eine Gruppenkennung (GID)	Verwendet eine Sicherheitskennung (SID)
Sperr-Policy	NFSv3-Bereichssperren sind konsultativ und NFSv4-Bereichssperren sind konsultativ oder obligatorisch (Standard).	SMB-Bereichssperren sind obligatorisch.
Benutzerauthentifizierung	Die Authentifizierung wird durchgeführt über: ● Eine vorherige lokale Anmeldung bei einem anderen Unix-System ● Einen UNIX-Verzeichnisdienst (NIS oder LDAP), der nach der UID/GID von NutzerInnen sucht ● Lokale Kennwort- und Gruppendateien, die nach der UID/GID von NutzerInnen suchen	Die Authentifizierung wird durch das Active Directory durchgeführt, das nach der SID eines/einer NutzerIn sucht. Dies erfordert NTP und DNS.
Sicherheitsregeln	Verwendet die Unix-Zugangsdaten, die dem/der authentifizierten NutzerIn zugeordnet sind, um Modusbits (NFSv3) oder Zugriffsrechte in der NFSv4-ACL zu überprüfen.	Verwendet die Windows-Zugangsdaten, die dem/der authentifizierten NutzerIn zugeordnet sind, um die SMB-Zugriffs-ACL zu überprüfen.
Umbenennen von Policies	Das Umbenennen einer Komponente einer geöffneten Datei ist zulässig.	Das Umbenennen einer Komponente einer geöffneten Datei ist nicht zulässig.

PowerStore unterstützt eine gemischte NFS- und SMB-Umgebung, indem es gleichzeitigen Zugriff auf dieselben Daten für NFS (v3 und v4) und SMB bietet. Die NAS-Serverfunktionalität wird durch die Konfiguration des Serverfreigabeprotokolls bestimmt. Um Multiprotokoll zu aktivieren, wählen Sie sowohl SMB- als auch NFS-Freigabeprotokolle als Teil der NAS-Serverkonfiguration aus. Erstellen Sie dann ein Dateisystem auf diesem NAS-Server und schließlich sowohl NFS- als auch SMB-Freigaben auf dem Dateisystem.

Um die Multiprotokollfunktion zu konfigurieren, müssen Sie den NAS-Server zu einer Windows Active Directory-Domäne hinzufügen und einen Unix-Verzeichnisdienst (LDAP oder NIS) oder lokale Kennwort- und Gruppendateien für den NAS-Server oder beides konfigurieren. LDAP muss den IDMU-, RFC2307- oder RFC2307bis-Schemata entsprechen. Einige Beispiele hierfür sind AD-LDAP mit IDMU, iPlanet und OpenLDAP. Der LDAP-Server muss ordnungsgemäß konfiguriert werden, um UIDs für jeden Nutzer bereitzustellen. Zum Beispiel muss der Administrator auf der IDMU die Eigenschaften der jeweiligen Nutzer aufrufen und auf der Registerkarte „UNIX-Attribute“ eine UID hinzufügen.

Die Nutzernamen in einer NFS-Umgebung und einer SMB-Umgebung müssen in jedem Zeichen übereinstimmen. Wenn es Diskrepanzen bei den Nutzernamen gibt, können Sie eine Nutzerzuordnungsdatei (`ntxmap`) konfigurieren, um jeden NFS-Namen dem

entsprechenden SMB-Namen und jeden SMB-Namen dem entsprechenden NFS-Namen zuzuordnen. Sie können auch standardmäßige Unix- und Windows-Kontonamen konfigurieren. Das System verwendet den standardmäßigen Windows-Kontonamen, wenn es keine Übereinstimmung mit einem SMB-Namen auf NFS findet, und den standardmäßigen Unix-Kontonamen, wenn es keine Übereinstimmung mit einem NFS-Namen auf SMB findet.

ANMERKUNG: Wenn mehrere NutzerInnen die Standardkonten verwenden, kann sich dies auf die Quoten auswirken.

Wenn Sie ein Dateisystem mit Multiprotokollzugriff konfigurieren, müssen Sie auch eine Zugriffs-Policy auswählen, um die Nutzerzugriffskontrolle für das Dateisystem zu verwalten. Detaillierte Informationen zur Sicherheit und zum Dateizugriff in einer Multiprotokollumgebung finden Sie unter Ausführliche Informationen: Sicherheit und Zugriff auf Dateisysteme in einer Multiprotokollumgebung.

Die folgenden Abbildungen zeigen die allgemeinen Schritte zur Konfiguration von Multiprotokoll-Dateifreigaben.

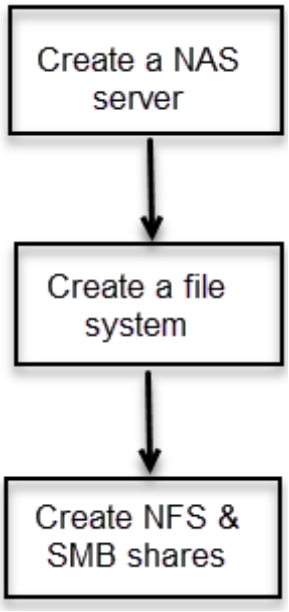

Abbildung 1. Allgemeine Schritte für die Konfiguration von Multiprotokoll-Dateifreigaben

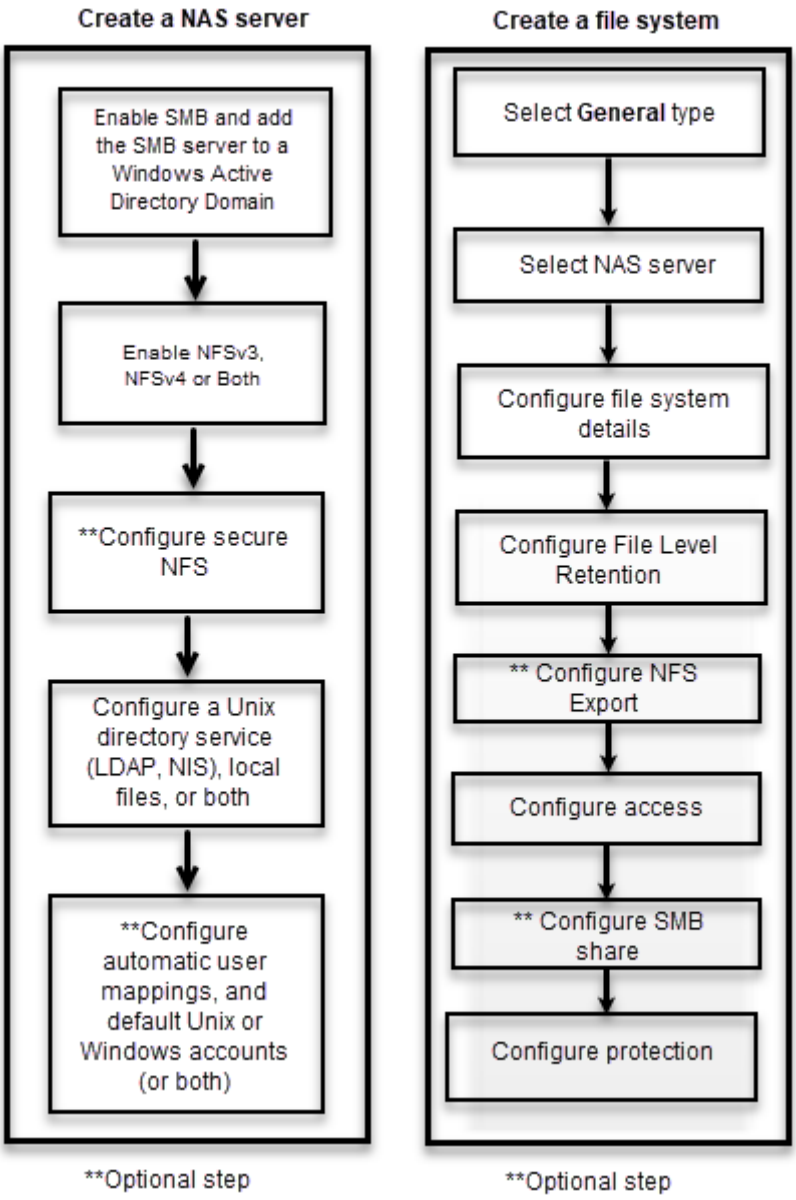

Abbildung 2. Allgemeine Schritte für die Konfiguration von Multiprotokoll-Dateifreigaben (Fortsetzung)

2

Ausführliche Informationen: Sicherheit und Zugriff auf Dateisysteme in einer Multiprotokollumgebung

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Sicherheit auf Dateisystemobjekten

In einer Umgebung mit Multiprotokoll wird die Sicherheits-Policy auf Dateisystemebene festgelegt und ist unabhängig für jedes Dateisystem. Jedes Dateisystem verwendet seine Zugriffs-Policy, um die Zusammenführung der unterschiedlichen Semantiken der NFS- und SMB-Zugriffskontrollen zu bestimmen. Die Auswahl einer Zugriffs-Policy bestimmt, welcher Mechanismus verwendet wird, um Dateisicherheit auf dem jeweiligen Dateisystem durchzusetzen.

Die Standardeinstellung der nativen Sicherheit behält zwei separate Berechtigungssätze für jede Datei bei und das Protokoll, das für den Zugriff auf die Datei verwendet wird, bestimmt, welche Berechtigungssätze überprüft werden. Wenn SMB verwendet wird, werden die ACLs überprüft. Wenn NFS verwendet wird, werden die NFSv3-Modusbits oder die NFSv4-ACL überprüft.

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.

Natives Sicherheitsmodell

Das native Sicherheitsmodell ist die Standardeinstellung. Das Modell verwaltet den Zugriff für jedes Protokoll separat anhand der eigenen nativen Sicherheitsmechanismen.

- Für die Sicherheit von NFS-Freigaben werden die Unix-Modusbits oder die NFSv4-ACL (Access Control List, Zugriffskontrollliste) verwendet.
- Für die Sicherheit von SMB-Freigaben wird die SMB-ACL verwendet.

Die beiden Berechtigungssätze sind voneinander unabhängig und werden nicht synchronisiert. Änderungen an den NFSv3-Unix-Modusbits oder NFSv4-ACL-Berechtigungen werden synchronisiert, ohne die SMB-ACL zu ändern. Änderungen an der SMB-ACL wirken sich nicht auf die NFSv3-Unix-Modusbits oder NFSv4-ACL aus.

Welcher Berechtigungssatz erzwungen wird, hängt vom verwendeten Zugriffsprotokoll ab.

Unix-Sicherheitsmodell

Wenn die Unix-Policy ausgewählt ist, werden alle Versuche, die Sicherheit auf Dateiebene über das SMB-Protokoll zu ändern, wie z. B. Änderungen an den Zugriffskontrolllisten (ACLs), ignoriert. Als Unix-Zugriffsrechte werden die NFSv3-Unix-Modusbits oder NFSv4-ACL eines Dateisystemobjekts bezeichnet. Eine Bit-Zeichenfolge steht für Modusbits. Jedes Bit stellt einen Zugriffsmodus oder eine Berechtigung dar, die dem Benutzer, der Eigentümer der Datei ist, der Gruppe, die mit dem Dateisystemobjekt verbunden ist, und allen anderen Benutzern zugeordnet ist. UNIX-Modusbits werden als drei Reihen verketteter rwx-Tripel (für Lesen, Schreiben und Ausführen)

für jede Kategorie von Benutzern (Benutzer, Gruppe oder andere) angezeigt. Eine Zugriffskontrollliste (ACL) ist eine Liste von Benutzern und Benutzergruppen, durch die der Zugriff auf und die Ablehnung von Services gesteuert wird.

Das Unix-Sicherheitsmodell verwendet für beide Protokolle NFSv3-Unix-Modusbits oder die NFSv4-ACL. Wenn eine Anfrage für SMB-Zugriff gesendet wird, werden die aus dem USD/den lokalen Dateien erstellten Unix-Zugangsdaten verwendet, um die NFSv3-Modusbits oder die NVSv4-ACL auf Berechtigungen zu überprüfen. Wenn die NFSv3-Unix-Modusbits oder NFSv4-ACLs geändert werden, werden die SMB-ACL-Berechtigungen aktualisiert.

Änderungen an den SMB-ACL-Berechtigungen sind zulässig, um Unterbrechungen zu vermeiden, diese Berechtigungen werden jedoch nicht beibehalten.

Windows-Sicherheitsmodell

Das Windows-Sicherheitsmodell basiert in erster Linie auf Objektrechten. Dazu gehört die Verwendung einer SD (Security Descriptor, Sicherheitsbeschreibung) und ihrer ACL (Access Control List, Zugriffskontrollliste). Wenn eine SMB-Policy ausgewählt ist, werden Änderungen an den Modusbits durch das NFS-Protokoll ignoriert.

Der Zugriff auf ein Dateisystemobjekt basiert darauf, ob Berechtigungen über eine SD festgelegt wurden, die den Zugriff erlauben oder verweigern. Der SD beschreibt den Eigentümer des Objekts und Gruppen-SIDs für das Objekt zusammen mit seinen ACLs. Eine ACL ist Teil des Sicherheitsdeskriptors für jedes Objekt. Jede ACL enthält Zugriffskontrolleinträge (ACEs). Jeder ACE wiederum enthält eine einzelne SID, die eine/n NutzerIn, eine Gruppe oder eine Systemeinheit identifiziert, sowie eine Liste mit Rechten, die für diese SID verweigert oder gewährt werden.

Das Windows-Sicherheitsmodell verwendet für beide Protokolle die SMB-ACL. Bei Anfragen für NFS-Zugriff werden die von der DC/LGDB erstellten Windows-Zugangsdaten verwendet, um die ACL auf Berechtigungen zu überprüfen. Wenn die SMB-ACL-Berechtigungen geändert werden, werden die NFSv3-Unix-Modusbits oder NFSv4-ACLs aktualisiert. Änderungen an den NFSv3-Unix-Modusbits oder NFSv4-ACL-Berechtigungen werden abgelehnt.

File system access

Der Dateizugriff wird über NAS-Server bereitgestellt, die Dateisysteme enthalten, in denen Daten gespeichert sind. Der NAS-Server bietet Zugriff auf diese Daten für die NFS- und SMB-Dateiprotokolle durch die Freigabe von Dateisystemen über SMB-Shares und NFS-Shares. Der NAS-Server erlaubt die Freigabe derselben Daten zwischen SMB und NFS und bietet gleichzeitigen SMB- und NFS-Zugriff auf ein Dateisystem. Die Zuordnung von Windows-NutzerInnen zu Unix-NutzerInnen und das Festlegen von Sicherheitsregeln (Modusbits, ACLs und Nutzerzugangsdaten) müssen berücksichtigt und für die Multiprotokollfreigabe konfiguriert werden.

Benutzerzuordnung

In einem Multiprotokollkontext muss ein/e Windows-NutzerIn mit einem/einer Unix-NutzerIn übereinstimmen. Allerdings muss ein UNIX-Benutzer nur dann einem Windows-Benutzer zugeordnet werden, wenn die Zugriffs-Policy Windows ist. Diese Zuordnung ist notwendig, damit Dateisystemsicherheit durchgesetzt werden kann, auch wenn sie für das Protokoll nicht systemeigen ist.

Die folgenden Komponenten sind an der Benutzerzuordnung beteiligt:

- Unix-Verzeichnisdienste, lokale Dateien oder beides
- Windows-Resolver
- Sichere Zuordnung (secmap) – ein Cache, der alle Zuordnungen zwischen SIDs und UID oder GIDs enthält, die von einem NAS-Server verwendet werden.
- ntxmap

ANMERKUNG: Die Benutzerzuordnung beeinflusst nicht die Benutzer oder Gruppen, die lokal auf dem SMB-Server sind.

Unix-Verzeichnisdienste und lokale Dateien

UNIX-Verzeichnisdienste (UDS) und lokale Dateien werden für Folgendes verwendet:

- Rückgabe des Unix-Kontonamens für eine bestimmte Nutzerkennung (UID)
- Rückgabe der UID und primären GID (Gruppenkennung) für einen bestimmten Unix-Kontonamen

Die unterstützten Services sind:

- LDAP
- NIS
- Lokale Dateien
- Keine (die einzig mögliche Zuordnung erfolgt über den Standardnutzer)

Für den NAS-Server müssen entweder ein UDS oder lokale Dateien oder sowohl lokale Dateien als auch ein UDS aktiviert sein, wenn die Multiprotokollfreigabe aktiviert ist. Die UDS-Suchreihenfolge bestimmt, was für die Nutzerzuordnung verwendet wird.

Windows-Resolver

Windows-Resolver werden verwendet, um Folgendes für die Benutzerzuordnung zu tun:

- Rückgabe des Windows-Kontonamens für eine bestimmte SID (Sicherheitskennung)
- Rückgabe der SID für einen bestimmten Windows-Kontonamen

Die Windows-Resolver sind:

- Der Domain Controller (DC) der Domain
- Die LGDB (Local Group Database, Datenbank der lokalen Gruppe) des SMB-Servers

Sicherer Zuordnungscache

Ein Secure Mapping Cache (secmap) ist ein Cache, der die Zuordnungen von NutzerInnen enthält, die zuvor mit dem NAS-Server verbunden waren. Für jede/n NutzerIn werden die SID, der Nutzername und die UID gespeichert. secmap speichert nur die Zuordnungen, die vom Standardzuordnungsmechanismus erzeugt werden.

Das Speichern von SID-zu-UID- und Primär-GID-Zuordnungen sowie UID-zu-SID-Zuordnungen sorgt für Kohärenz über alle Dateisystemen des NAS-Servers hinweg.

Das Speichern von Nutzerzuordnungen im secmap reduziert den Netzwerkverkehr und steigert die Effizienz. Sobald eine Nutzerzuordnung im secmap gespeichert wird, nutzt der NAS-Server den lokalen Cache für zukünftige Zuordnungsabfragen.

ntxmap

ntxmap ist eine optionale lokale Datei, die verwendet wird, um Namensübersetzungen zwischen Protokollen bereitzustellen. Wenn Inkonsistenzen zwischen Nutzernamen vorhanden sind, wird ntxmap verwendet, um ein Windows-Konto einem Unix-Konto zuzuordnen. Wenn beispielsweise ein Nutzer ein Konto namens „Gerald“ in Windows hat, sein Konto in Unix aber „Gerry“ lautet, wird ntxmap verwendet, um die Korrelation zwischen diesen beiden herzustellen.

ntxmap kann auch für erweiterte Namensübersetzungen, z. B. für das Konvertieren mehrerer Nutzernamen in einen einzigen Nutzernamen, und das Bereitstellen von Namenskonvertierungen verwendet werden.

ANMERKUNG: ntxmap bietet nur Übersetzungen für Nutzernamen zwischen Protokollen und keine Zuordnungen von IDs zu Nutzernamen.

SID-zu-UID und primäre GID-Zuordnung

Die folgende Sequenz ist der Vorgang für die Auflösung einer SID-zu-UID- und Primär-GID-Zuordnung:

1. secmap wird nach der SID durchsucht. Wenn die SID gefunden wird, wird die UID- und Primär-GID-Zuordnung aufgelöst.
2. Wenn die SID nicht im secmap gefunden wird, muss der Windows-Nutzername, der der SID entspricht, gefunden werden.
   a. Die Datenbank der lokalen Gruppe (LGDB) wird nach der SID durchsucht, um festzustellen, ob es sich um eine/n lokale/n NutzerIn handelt. Wenn die SID gefunden wird, lautet der zugehörige Windows-Name `SMB_SERVER\USER`. Da es sich um eine/n lokale/n NutzerIn für den reinen SMB-Zugriff handelt, ist keine Unix-Zuordnung erforderlich.
   b. Wenn die SID nicht in der LGDB gefunden wird, wird der DC der Domäne durchsucht. Wenn die SID in der Domäne gefunden wird, lautet der zugehörige Windows-Name `DOMAIN\USER`.
   c. Ist die SID nicht auflösbar, wird der Zugriff verweigert. Diese fehlgeschlagene Zuordnung wird der persistenten secmap-Datenbank hinzugefügt.
3. Wenn nicht das Unix-Standardkonto verwendet wird, wird der Windows-Name mithilfe der ntxmap in den Unix-Namen übersetzt.
   a. Wenn der Windows-Name in ntxmap gefunden wird, wird der Eintrag als Unix-Name verwendet.

b. Wenn der Windows-Name nicht in der ntxmap gefunden wird oder die ntxmap deaktiviert ist, wird der Windows-Name als Unix-Name verwendet.

4. Die lokalen Dateien oder das UDS werden nach dem Unix-Namen durchsucht, um die UID und primäre GID zu ermitteln.
   a. Wenn der Unix-Nutzername gefunden wird, wird die UID- und Primär-GID-Zuordnung aufgelöst. Die erfolgreiche Zuordnung wird der persistenten secmap-Datenbank hinzugefügt.
   b. Wenn der Unix-Nutzername nicht gefunden wird, die Funktion zur automatischen Zuordnung nicht zugeordneter Windows-Konten jedoch aktiviert ist, wird die UID automatisch zugewiesen. Die erfolgreiche Zuordnung wird der persistenten secmap-Datenbank hinzugefügt.
   c. Wenn der Unix-Nutzername nicht gefunden wird, aber dafür ein Unix-Standardkonto, wird die UID- und Primär-GID-Zuordnung der Zuordnung des Unix-Standardkontos zugeordnet. Diese fehlgeschlagene Zuordnung wird der persistenten secmap-Datenbank hinzugefügt.
   d. Wenn der Unix-Nutzername nicht aufgelöst werden kann, wird der Zugriff verweigert. Diese fehlgeschlagene Zuordnung wird der persistenten secmap-Datenbank hinzugefügt.

Wenn die Zuordnung gefunden wird, wird sie der dauerhaften secmap-Datenbank hinzugefügt. Wenn die Zuordnung nicht gefunden wird, wird die fehlgeschlagene Zuordnung der dauerhaften secmap-Datenbank hinzugefügt.

Im folgenden Diagramm ist der Vorgang zur Auflösung einer SID-zu-UID- und Primär-GID-Zuordnung dargestellt:

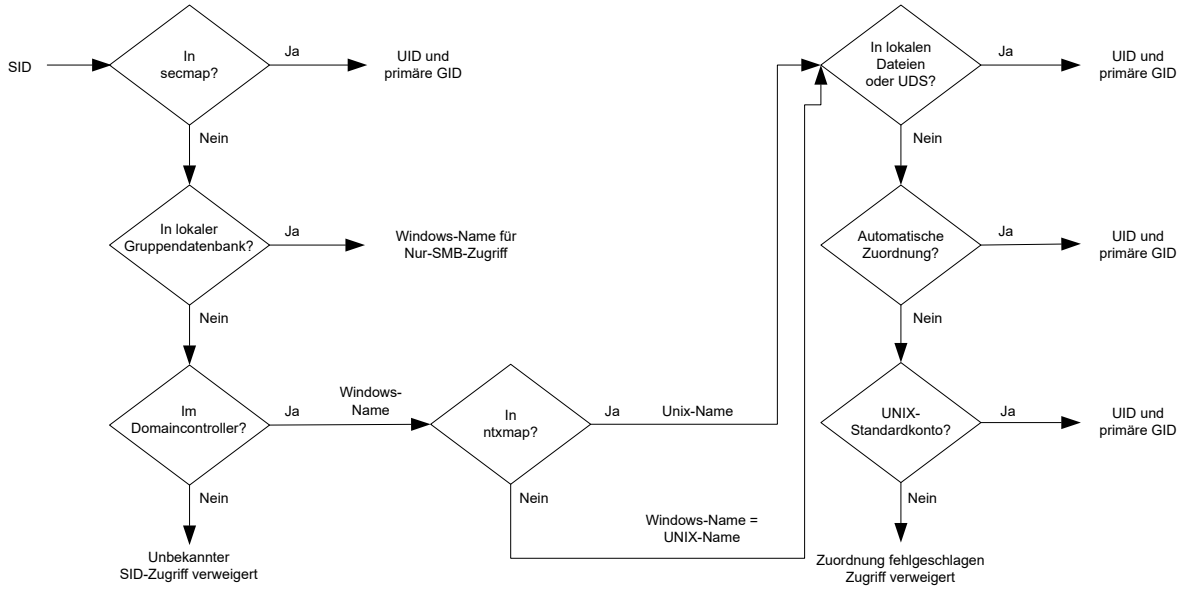

Abbildung 3. Prozess für die Auflösung einer SID in eine UID, die primäre GID-Zuordnung

UID-zu-SID-Zuordnung

Die folgende Sequenz ist der Vorgang für die Auflösung einer UID-zu-SID-Zuordnung:

1. secmap wird nach der UID durchsucht. Wenn die UID gefunden wird, wird die SID-Zuordnung aufgelöst.
2. Wenn die UID nicht in secmap gefunden wird, muss der Unix-Name, der der UID entspricht, gefunden werden.
   a. Die lokalen Dateien oder der UDS werden nach der UID durchsucht. Wenn die UID gefunden wird, ist der zugehörige Unix-Name der Nutzername.
   b. Wenn die UID nicht im UDS gefunden wird, dafür aber ein Windows-Standardkonto, wird die UID dem Windows-Standardkonto zugeordnet. Wenn er nicht vorhanden ist, wird der Standard-Windows-Nutzer der persistenten secmap-Datenbank hinzugefügt.
   c. Ist die UID nicht auflösbar, wird der Zugriff verweigert.
3. Wenn das Windows-Standardkonto nicht verwendet wird, wird der Unix-Name in einen Windows-Namen übersetzt.
   a. Wenn der Unix-Name in ntxmap gefunden wird, wird der Eintrag als Windows-Name verwendet.
   b. Wenn der Unix-Name nicht in der ntxmap gefunden wird oder die ntxmap deaktiviert ist, wird der Unix-Name als Windows-Name verwendet.
4. Der DC oder die LGDB wird nach dem Windows-Namen durchsucht, um die SID zu ermitteln.
   a. Der Windows-Name wird im DC gesucht. Wenn der Windows-Name gefunden wird, wird die SID-Zuordnung aufgelöst.
   b. Wenn der Windows-Name einen Punkt (.) enthält und der Teil des Namens, der auf den letzten Punkt folgt, dem Namen eines SMB-Servers entspricht, wird die Datenbank der lokalen Gruppe (LGDB) dieses SMB-Servers durchsucht, um die SID-Zuordnung aufzulösen. Wenn der Windows-Name gefunden wird, wird die SID-Zuordnung aufgelöst.
   c. Wenn der Windows-Name nicht gefunden wird, es jedoch ein Windows-Standardkonto gibt, wird die SID der des Windows-Standardkontos zugeordnet. Wenn er nicht vorhanden ist, wird der Standard-Windows-Nutzer der persistenten secmap-Datenbank hinzugefügt.
   d. Ist der Windows-Name nicht auflösbar, wird der Zugriff verweigert.

Wenn die Zuordnung gefunden wird, wird sie der dauerhaften secmap-Datenbank hinzugefügt. Wenn die Zuordnung nicht gefunden wird, wird die fehlgeschlagene Zuordnung der dauerhaften secmap-Datenbank hinzugefügt.

Im folgenden Diagramm ist der Vorgang für die Auflösung einer UID-zu-SID-Zuordnung dargestellt:

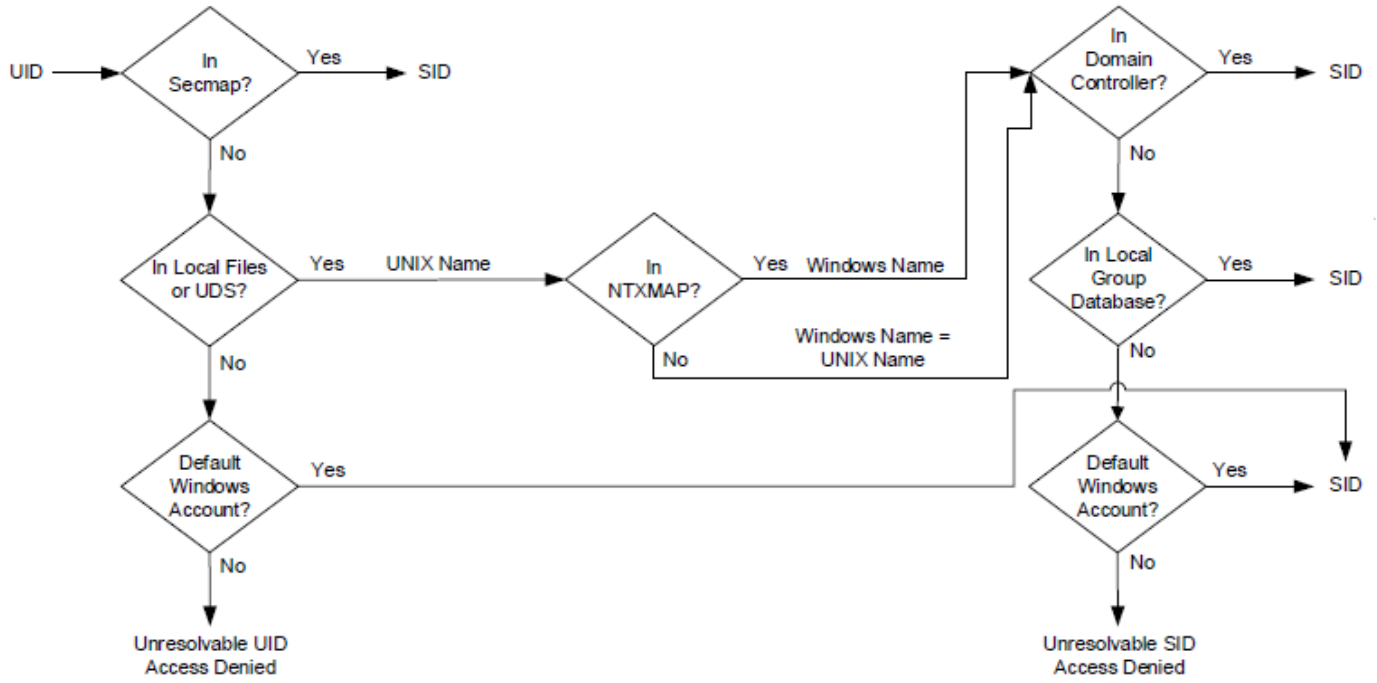

Abbildung 4. Vorgehensweise für die Auflösung einer UID-zu-SID-Zuordnung

Zugriffs-Policies für NFS, SMB und FTP

In einer Multiprotokollumgebung verwendet das Speichersystem Dateisystemzugriffs-Policies, um die Benutzerzugriffskontrolle für die Dateisysteme zu managen. Es gibt zwei Arten von Sicherheit, UNIX und Windows.

Bei der Unix-Sicherheitsauthentifizierung werden die Zugangsdaten aus dem UDS (Unix Directory Services) erstellt, außer für den nicht sicheren NFS-Zugriff, bei dem die Zugangsdaten vom Host-Client bereitgestellt werden. Nutzerrechte werden von den Modusbits und NFSv4-ACL bestimmt. Die Benutzer- und Gruppenkennungen (UID bzw. GID) werden zur Identifizierung verwendet. Es sind keine Berechtigungen mit UNIX-Sicherheit verbunden.

Bei der Windows-Sicherheitsauthentifizierung werden die Zugangsdaten aus dem Windows-Domain-Controller (DC) und der Datenbank der lokalen Gruppe (LGDB) des SMB-Servers erstellt. Benutzerrechte werden von den SMB-ACLs festgelegt. Die Sicherheitskennung (SID) wird für die Identifizierung verwendet. Berechtigungen im Zusammenhang mit der Windows-Sicherheit, darunter TakeOwnership, Backup und Wiederherstellung, werden von der LGDB oder dem Gruppenrichtlinienobjekt (GPO) des SMB-Servers gewährt.

In der folgenden Tabelle werden die Zugriffs-Policies beschrieben, die definieren, welche Sicherheit von welchen Protokollen verwendet wird:

Tabelle 2. Zugriffs-Policies

Zugriffs-Policy	Beschreibung
Nativ (Standardeinstellung)	• Jedes Protokoll managt den Zugriff gemäß den nativen Sicherheitsmechanismen. • Die Sicherheit für NFS-Freigaben verwendet die UNIX-Zugangsdaten, die mit der Anforderung zur Überprüfung der NFSv3-UNIX-Modusbits oder der NFSv4-ACL verknüpft sind. Der Zugriff wird dann gewährt oder verweigert. • Die Sicherheit für SMB-Freigaben verwendet die Windows-Zugangsdaten, die mit der Anforderung zur Überprüfung der SMB-ACL verknüpft sind. Der Zugriff wird dann gewährt oder verweigert. • Die Änderungen der NFSv3-UNIX-Modusbits und der NFSv4-ACL-Berechtigungen werden miteinander synchronisiert. • Es gibt keine Synchronisation zwischen den UNIX- und Windows-Berechtigungen.
Windows	• Stellt den Zugriff auf Dateiebene für Windows und UNIX mithilfe der Windows-Sicherheit sicher. • Verwendet Windows-Anmeldedaten zur Prüfung der SMB-ACL. • Eine SMB-ACL-Konvertierung legt die Berechtigungen für neu erstellte Dateien fest. Die Änderungen der SMB-ACL-Berechtigungen werden für die NFSv3-UNIX-Modusbits oder die NFSv4-ACL synchronisiert. • Änderungen der NFSv3-Modusbits und der NFSv4-ACL-Berechtigungen werden abgelehnt.
UNIX	• Stellt den Zugriff auf Dateiebene für Windows und UNIX mithilfe der UNIX-Sicherheit sicher. • Auf Anforderung des SMB-Zugriffs werden die aus den lokalen Dateien oder UDS erstellten UNIX-Zugangsdaten verwendet, um die NFSv3-Modusbits oder die NFSv4-ACL auf Berechtigungen zu überprüfen. • UMASK bestimmt Berechtigungen für neu erstellte Dateien. • Die Änderungen der NFSv3-UNIX-Modusbits oder der NFSv4-ACL-Berechtigungen werden für die SMB-ACL synchronisiert. • Änderungen der SMB-ACL-Berechtigungen sind zulässig, um Unterbrechungen zu vermeiden, diese Berechtigungen werden jedoch nicht beibehalten.

Bei FTP hängt die Authentifizierung mit Windows oder UNIX vom Format des Nutzernamens ab, der für die Authentifizierung am NAS-Server verwendet wird. Bei Verwendung der Windows-Authentifizierung ähnelt die FTP-Zugriffskontrolle der für SMB, andernfalls der für NFS. FTP- und SFTP-Clients werden bei Herstellung der Verbindung mit dem NAS-Server authentifiziert. Dies kann eine SMB-Authentifizierung (wenn der Nutzernamen das Format `domain\user` oder `user@domain` hat) oder eine UNIX-Authentifizierung sein (bei anderen Formaten eines einzelnen Nutzernamens). Der Windows-DC der Domain, die im NAS-Server definiert ist, stellt die SMB-Authentifizierung sicher. Der NAS-Server stellt die Unix-Authentifizierung anhand des verschlüsselten Kennworts sicher, das entweder in einem Remote-LDAP-Server, einem Remote-NIS-Server oder in der lokalen Kennwortdatei des NAS-Servers gespeichert ist.

Zugangsdaten für Sicherheit auf Dateiebene

Zur Durchsetzung der Sicherheit auf Dateiebene muss das Storage-System Zugangsdaten erstellen, die mit der zu verarbeitenden SMB- oder NFS-Anfrage verknüpft sind. Es gibt zwei Arten von Zugangsdaten, Windows und UNIX. Der NAS-Server erstellt Unix- und Windows-Zugangsdaten für die folgenden Anwendungsfälle:

- Erstellen von Unix-Zugangsdaten mit mehr als 16 Gruppen für eine NFS-Anfrage. Die Eigenschaft „Erweiterte Zugangsdaten“ des NAS-Servers muss festgelegt werden, um diese Möglichkeit bereitzustellen.
- Erstellen von Unix-Zugangsdaten für eine SMB-Anfrage, wenn die Zugriffs-Policy für das Dateisystem Unix ist
- Erstellen von Windows-Zugangsdaten für eine SMB-Anfrage
- Erstellen von Windows-Zugangsdaten für eine NFS-Anfrage, wenn die Zugriffs-Policy für das Dateisystem Windows ist

ANMERKUNG: Wenn für eine NFS-Anfrage die Eigenschaft „Erweiterte Zugangsdaten“ nicht festgelegt ist, werden die Unix-Zugangsdaten aus der NFS-Anfrage verwendet. Wenn für eine SMB-Anfrage Kerberos-Authentifizierung verwendet wird, sind die Windows-Zugangsdaten des/der DomänennutzerIn im Kerberos-Ticket der Anfrage für die Sitzungseinrichtung enthalten.

Ein persistenter Zugangsdatencache wird für Folgendes verwendet:

- Windows-Zugangsdaten, die für den Zugriff auf ein Dateisystem mit einer Windows-Zugriffs-Policy erstellt wurden.
- Unix-Zugangsdaten für den Zugriff über NFS, wenn die Option für erweiterte Zugangsdaten aktiviert ist

Es gibt eine Cacheinstanz für jeden NAS-Server.

Gewähren von Zugriff für nicht zugeordnete Benutzer

Multiprotokoll erfordert Folgendes:

- Ein Windows-Benutzer muss einem UNIX-Benutzer zugeordnet sein.
- Ein UNIX-Benutzer muss einem Windows-Benutzer zugeordnet sein, damit die Windows-Zugangsdaten erstellt werden können, wenn der Benutzer auf ein Dateisystem zugreift, das eine Windows-Zugriffs-Policy aufweist.

Dem NAS-Server sind in Bezug auf nicht zugeordnete NutzerInnen zwei Eigenschaften zugeordnet:

- Der standardmäßige UNIX-Benutzer
- Der standardmäßige Windows-Benutzer

Wenn ein nicht zugeordneter Windows-Benutzer versucht, eine Verbindung zu einem Multiprotokolldateisystem herzustellen, und das Unix-Standardbenutzerkonto für den NAS-Server konfiguriert ist, werden die Benutzerkennung (UID) und primäre Gruppenkennung (GID) für den Unix-Standardbenutzer in den Windows-Zugangsdaten verwendet. Auf ähnliche Weise wird, wenn ein nicht zugeordneter Unix-Benutzer versucht, eine Verbindung zu einem Multiprotokolldateisystem herzustellen, und das Windows-Standardbenutzerkonto für den NAS-Server konfiguriert ist, die Windows-Zugangsdaten des Windows-Standardbenutzers verwendet.

ANMERKUNG: Wenn der Unix-Standardbenutzer nicht in den Unix-Verzeichnisdiensten (Unix Directory Services, UDS) festgelegt ist, wird der SMB-Zugriff für nicht zugeordnete Benutzer verweigert. Wenn der Windows-Standardnutzer nicht im Windows-DC oder in der LGDB gefunden wird, wird der NFS-Zugriff auf ein Dateisystem, das einer Windows-Zugriffs-Policy unterliegt, für nicht zugeordnete Nutzer verweigert.

ANMERKUNG: Der Unix-Standardnutzer kann ein gültiger vorhandener UNIX-Kontoname sein oder das neue Format `@uid=xxxx,gid=yyyy@` aufweisen, wobei *xxxx* und *yyyy* für die numerischen Dezimalwerte der UID bzw. für die primäre GID stehen. Diese Werte können auf dem System über die CLI konfiguriert werden.

Da das PowerStore-Dateisystem Unix-basiert ist, müssen alle geschriebenen Daten einer gültigen UID und primären GID zugeordnet sein. NFS-Nutzer verfügen nativ über eine UID und eine primäre GID. SMB-Nutzer benötigen jedoch eine Zuordnung, die ihre native SID in eine UID und primäre GID konvertiert. Eine umgekehrte Zuordnung von UID zu SID ist nur dann notwendig, wenn Windows-Berechtigungen erzwungen werden (Windows-Zugriffs-Policy).

Die automatische Zuordnungsfunktion ermöglicht die automatische Erstellung und Zuweisung einer eindeutigen UID zu Windows-NutzerInnen, die keine UID-Zuordnung haben. Diese Funktion ermöglicht den Zugriff auf die Freigabe für nicht zugeordnete NutzerInnen, anstatt ihnen den Zugriff zu verweigern. Da jede/r NutzerIn über eine eindeutige UID verfügt, können UID-basierte Funktionen, wie z. B. Nutzerquoten, die Nutzung jedes/jeder NutzerIn weiterhin ordnungsgemäß nachverfolgen.

Die automatische Zuordnung ist auf reinen SMB- und Multiprotokoll-NAS-Servern standardmäßig aktiviert. Wenn diese Funktion aktiviert ist, ist die Option zum Konfigurieren von Standardkonten deaktiviert. Da das System jede UID automatisch zuweist, sollten Sie diese Funktion nur in Umgebungen verwenden, in denen die UID dieser NutzerInnen nicht kritisch ist. In Umgebungen, in denen AdministratorInnen UID-Zuweisungen steuern möchten, deaktivieren Sie die Funktion. Wenn die automatische Zuordnung deaktiviert ist und keine anderen Zuordnungsmethoden für nicht zugeordnete NutzerInnen verfügbar sind, wird ihnen der Zugriff auf die Freigabe verweigert.

UNIX-Zugangsdaten für NFS-Anforderungen

Es müssen Unix-Zugangsdaten verwendet werden, um NFS-Anfragen für ein reines NFS- oder Multiprotokoll-Dateisystem mit einer Unix- oder nativen Zugriffs-Policy zu verarbeiten. Die UNIX-Zugangsdaten werden immer in jeder Anforderung integriert; allerdings sind die Zugangsdaten auf 16 Extragruppen beschränkt.

Um die Eigenschaft „Erweiterte Zugangsdaten“ zu aktivieren, wählen Sie **Storage** > **NAS-Server** > **[NAS-Server]** > **Freigabeprotokolle** > **NFS-Server** aus und schalten Sie die Option **Erweiterte Zugangsdaten** ein. Durch die Aktivierung erweiterter Unix-Zugangsdaten ist es möglich, Zugangsdaten mit mehr als 16 Gruppen zu erstellen. Wenn diese Option festgelegt ist, wird das aktive

UDS mit der UID abgefragt, um die primäre GID und alle Gruppen-GIDs abzurufen, zu denen sie gehört. Wenn die UID im UDS nicht gefunden wird, werden die in der Anfrage enthaltenen Unix-Zugangsdaten verwendet.

ANMERKUNG: Für sicheren NFS-Zugriff werden die Zugangsdaten immer mit dem UDS erstellt.

UNIX-Zugangsdaten für SMB-Anforderungen

Wenn die Sitzung eingerichtet ist, müssen für den/die SMB-NutzerIn Windows-Zugangsdaten erstellt werden. Die Erstellung der Zugangsdaten ermöglicht die Verarbeitung von SMB-Anfragen für ein Multiprotokoll-Dateisystem mit einer Unix-Zugriffs-Policy. Die SID des Windows-Benutzers wird verwendet, um den Namen in Active Directory zu finden. Dieser Name wird dann verwendet (optional auch über ntxmap), um eine Unix-UID und -GID im UDS oder in einer lokalen Datei (Kennwortdatei) zu finden. Die Eigentümer-UID des/der NutzerIn ist Teil der Windows-Zugangsdaten. Beim Zugriff auf ein Dateisystem mit einer UNIX-Zugriffs-Policy wird die ID des Benutzers zum Abfragen der UDS verwendet, um die UNIX-Zugangsdaten zu erstellen, ähnlich wie bei der Erstellung von erweiterten Zugangsdaten für NFS. Die UID ist für das Quotenmanagement erforderlich.

Windows-Zugangsdaten für SMB-Anforderungen

Es müssen Windows-Zugangsdaten verwendet werden, um SMB-Anfragen für ein reines SMB- oder Multiprotokoll-Dateisystem mit einer Windows- oder nativen Zugriffs-Policy zu verarbeiten. Die Windows-Zugangsdaten für SMB müssen nur einmal zum Zeitpunkt der Anfrage für eine Sitzungseinrichtung erstellt werden, wenn sich der/die NutzerIn verbindet.

Wenn Kerberos-Authentifizierung verwendet wird, sind die Zugangsdaten des/der NutzerIn im Kerberos-Ticket der Anfrage für die Sitzungseinrichtung enthalten, anders als bei der Verwendung von NTLM (NT LAN Manager). Weitere Informationen werden vom Windows-DC oder der LGDB abgefragt. Für Kerberos wird die Liste der Extragruppen-SIDs dem Kerberos-Ticket und der Liste der lokalen Extragruppen-SIDs entnommen. Die Liste der Rechte werden der LGDB entnommen. Für NTLM wird die Liste der Extragruppen-SIDs dem Windows-DC und der Liste der lokalen Extragruppen-SIDs entnommen. Die Liste der Berechtigungen wird der LGDB entnommen.

Darüber hinaus wird die entsprechende UID und primäre GID auch aus der Nutzerzuordnungskomponente abgerufen. Da die Primärgruppen-SID für die Zugriffsprüfung nicht verwendet wird, wird stattdessen die primäre UNIX-GID verwendet.

ANMERKUNG: NTLM ist eine ältere Suite proprietärer Sicherheitsprotokolle, die Authentifizierung, Integrität und Vertraulichkeit für Benutzer bereitstellt. Kerberos ist ein offenes Standardprotokoll, das schnellere Authentifizierung durch den Einsatz eines Ticketing-Systems bietet. Kerberos verleiht Systemen in einem Netzwerk mehr Sicherheit als NTLM.

Windows-Anmeldedaten für NFS-Anforderungen

Die Windows-Zugangsdaten werden nur dann erstellt oder abgerufen, wenn ein/e NutzerIn über eine NFS-Anfrage versucht, auf ein Dateisystem zuzugreifen, das über eine Windows-Zugriffs-Policy verfügt. Die UID wird aus der NFS-Anforderung extrahiert. Es gibt einen globalen Cache für Windows-Anmeldedaten. Damit wird vermieden, dass die Anmeldedaten bei jeder NFS-Anforderung mit einer zugehörigen Aufbewahrungszeit erstellt werden müssen. Wenn die Windows-Anmeldedaten in diesem Cache gefunden werden, ist keine weitere Aktion erforderlich. Wenn die Windows-Anmeldedaten nicht gefunden werden, wird der UDS oder die lokale Datei abgefragt, um den Namen für die UID zu finden. Der Name wird dann verwendet (optional über ntxmap), um eine/n Windows-NutzerIn zu finden, und die Zugangsdaten werden vom Windows-DC oder aus der LGDB abgerufen. Wenn die Zuordnung nicht gefunden wird, werden stattdessen die Windows-Anmeldedaten des standardmäßigen Windows-Benutzers verwendet oder der Zugriff wird verweigert.

Sicherheitseinstellungen für das Multiprotokolldateisystem

PowerStore bietet Zugriffsanpassungs-, Umbenennungs- und Sperr-Policies für ein Multiprotokoll-Dateisystem.

Zugriffs-Policies für Dateisystem

Sie können eine der folgenden Zugriffs-Policies für ein Multiprotokolldateisystem auswählen.

- Systemeigene Sicherheit
- Unix-Sicherheit
- Windows-Sicherheit

Weitere Informationen zu diesen Zugriffs-Policies finden Sie unter Zugriffs-Policies für NFS, SMB und FTP.

Umbenennungs-Policies für Dateisysteme

Sie können eine der folgenden Umbenennen-Policies für ein Multiprotokolldateisystem auswählen. Eine Umbenennungs-Policy steuert die Bedingungen, unter denen NFS- und SMB-Clients ein Verzeichnis umbenennen können. Folgende Einstellungen sind möglich:

Tabelle 3. Umbenennungs-Policies für ein Multiprotokoll-Dateisystem

Einstellung	Beschreibung
Alle zulässig	Alle NFS- und SMB-Clients können Verzeichnisse ohne Einschränkungen umbenennen.
SMB nicht zulässig	Nur NFS-Clients können ohne Einschränkungen Verzeichnisse umbenennen. Wenn mindestens eine Datei im Verzeichnis oder in einem seiner Unterverzeichnisse geöffnet ist, kann ein SMB-Client das Verzeichnis nicht umbenennen. Wenn der Pfad zu einer Datei beispielsweise C:\Dir1\Dir2\Dir3\File1.txt lautet und ein SMB-Client File1 öffnet, können Dir1, Dir2 oder Dir3 nicht umbenannt werden.
Alle verboten	(Standard) Wenn mindestens eine Datei im Verzeichnis oder in einem seiner Unterverzeichnisse geöffnet ist, können NFS- und SMB-Clients das Verzeichnis nicht umbenennen.

Sperren-Policies für Dateisystem

SMB und NFS haben ihre eigene Sperrsemantik. Protokollspezifikationen definieren Sperrbereiche als obligatorisch für SMB, aber nur als konsultativ für NFS. NFSv3 verwendet ein separates Protokoll (NLM), das immer konsultativ ist. Bei NFSv4 ist die Sperrverwaltung in das Protokoll selbst integriert, kann aber je nach Implementierung möglicherweise ebenfalls konsultativ oder obligatorisch sein.

Eine Sperr-Policy-Eigenschaft wird verwendet, um das Verhalten zu definieren. Sie können eine der folgenden Sperren-Policies für ein Multiprotokolldateisystem auswählen:

Tabelle 4. Sperr-Policies für Dateisysteme

Einstellung	Beschreibung
Obligatorisch	Diese Policy verwendet die Protokolle KMU und NFSv4, um Bereichssperren für eine Datei zu managen, die von einem anderen Nutzer verwendet wird. Wenn gleichzeitig auf dieselben gesperrten Daten zugegriffen werden kann, verhindert eine obligatorische Sperr-Policy die Beschädigung von Daten.
Empfohlen	(Standard) Als Reaktion auf Sperranfragen meldet die Policy, dass es einen Konflikt bei der Bereichssperre gibt, der Zugriff auf die Datei wird jedoch nicht verhindert. Diese Policy ermöglicht es NFSv3-Anwendungen, die nicht bereichssperrenkonform sind, die Arbeit fortzusetzen, riskiert jedoch Datenbeschädigung durch gleichzeitige Schreibvorgänge.

3

Konfigurieren eines NAS-Servers für die Multiprotokoll-Dateifreigabe

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Konfigurieren von NAS-Servern für die Multiprotokoll-Dateifreigabe

Für die Konfiguration eines Multiprotokoll-NAS-Servers in der Benutzeroberfläche müssen die folgenden Informationen angegeben werden:

- Netzwerkinformationen für den NAS-Server (IP-Schnittstellen, Netzmaske, Gateway, VLAN usw.)
- Die IP-Adresse des DNS-Servers und die DNS-Domain für die Kontaktaufnahme mit AD
- Die Zugangsdaten eines AD-Nutzers (Active Directory) mit Berechtigungen für den Beitritt zu AD
- Die Informationen zum UNIX-Verzeichnisdienst (UDS). Für NIS umfassen diese Informationen den Domänennamen und die IP-Adresse der NIS-Server. Für LDAP umfassen diese Informationen die IP-Adresse der LDAP-Server, baseDN und Authentifizierungsinformationen. Für lokale Dateien umfassen diese Informationen passwd- und Gruppendateien.

In der folgenden Tabelle werden die verfügbaren NAS-Serverkonfigurationen für Multiprotokoll-NAS-Server beschrieben:

Tabelle 5. NAS-Serverkonfigurationen für Multiprotokoll-NAS-Server

Betriebsumgebung	NAS-Serverfunktion	Empfohlene Konfigurationsoptionen
Ausgewogene UNIX- und Windows-Umgebung, d. h., wenn Ihr System eine 1:1-Zuordnung aller oder der meisten Nutzer erfordert.	Ermöglicht SMB- und NFS-Zugriff auf dieselben Dateisystemdaten.	1. Gehen Sie im Assistenten zur Erstellung eines NAS-Servers wie folgt vor: • Wählen Sie auf der Registerkarte **Freigabeprotokolle** die Option **SMB** zusammen mit **NFSv3** und/oder **NFSv4** aus. • Verbinden Sie den NAS-Server mit einer Windows AD-Domain. • Konfigurieren Sie einen UDS (LDAP oder NIS), lokale Dateien oder sowohl lokale Dateien als auch einen UDS, um Nutzeridentitäten zu managen. • Konfigurieren von DNS • Konfigurieren Sie optional die automatische Nutzerzuordnung oder Standardkonten. • Konfigurieren Sie die UDS-Suchreihenfolge. 2. Passen Sie optional die Zuordnungen zwischen Windows-Nutzerkonten und UNIX-Nutzerkonten an, indem Sie eine Nutzerzuordnungsdatei mit erweiterten Benennungsregeln (ntxmap) ändern und hochladen. Sie sollten diese Option nur dann auswählen, wenn die Namen derselben Nutzer

Tabelle 5. NAS-Serverkonfigurationen für Multiprotokoll-NAS-Server (fortgesetzt)

Betriebsumgebung	NAS-Serverfunktion	Empfohlene Konfigurationsoptionen
		unterschiedliche Benennungsregeln in Windows- und UNIX befolgen.
UNIX-Umgebung mit Zugriffsmöglichkeit auf die Dateisystemdaten über SMB	Ermöglicht NFS-Zugriff auf die Dateisystemdaten sowie optional SMB-Zugriff auf dieselben Dateisystemdaten für einige Windows-Konten.	1. Befolgen Sie die Schritte in der Zeile „Ausgeglichene UNIX- und Windows-Umgebung“, um einen NAS-Server zu erstellen, einen UNIX-Verzeichnisdienst oder lokale Dateien zu konfigurieren und optional die Zuordnungen zwischen Windows- und UNIX-Nutzerkonten anzupassen. 2. Konfigurieren Sie optional ein standardmäßiges UNIX-Nutzerkonto. Alle nicht zugeordneten Windows-Konten werden diesem Nutzerkonto zugeordnet. Wenn Sie sich für die Verwendung automatischer Nutzerzuordnungen entscheiden, können Sie nicht steuern, welche UID jeder Nutzer hat, Sie können jedoch Quoten verwenden. **ANMERKUNG:** Wenn Sie für SMB-Nutzer ein UNIX-Standardkonto verwenden, werden diese einer UID zugewiesen. Daher wird nur eine Nutzerquote auf alle diese Nutzer angewendet. 3. Wenn Sie Dateisysteme für den NAS-Server erstellen, wird empfohlen, eine Zugriffs-Policy für das Dateisystem von UNIX anzugeben.
Windows-Umgebung mit Zugriffsmöglichkeit auf die Dateisystemdaten über NFS	Bietet SMB-Zugriff auf die Dateisystemdaten sowie optional NFS-Zugriff auf dieselben Dateisystemdaten für einige UNIX-Konten.	1. Befolgen Sie die Schritte in der Zeile „Ausgeglichene UNIX- und Windows-Umgebung“, um einen NAS-Server zu erstellen und optional ntxmap zu verwenden, um die Zuordnungen zwischen Windows- und UNIX-Nutzerkonten anzupassen. 2. Konfigurieren Sie optional ein standardmäßiges Windows-Nutzerkonto. Alle nicht zugeordneten UNIX-Konten werden diesem Standardnutzerkonto zugeordnet. **ANMERKUNG:** Wenn Sie für Windows-Nutzer ein UNIX-Standardkonto verwenden, werden diese einer SID zugewiesen. Daher wird nur eine Nutzerquote auf alle diese Nutzer angewendet. 3. Wenn Sie Dateisysteme für den NAS-Server erstellen, wird empfohlen, eine Zugriffs-Policy für das Dateisystem von Windows anzugeben.

Erstellen eines NAS-Servers für die Multiprotokoll-Dateifreigabe (SMB und NFS)

Voraussetzungen

Ermitteln Sie die folgenden Informationen:

- Netzwerkinformationen für den NAS-Server (IP-Schnittstellen, Netzmaske, Gateway, VLAN usw.)
- VLAN-ID, wenn der Switchport VLAN-Tagging unterstützt.
- AD-Informationen, darunter der Name des SMB-Systems (verwendet für den Zugriff auf SMB-Shares) und entweder die Zugangsdaten des Domainadministrators oder eines Nutzers der Domain, der über Berechtigungen für den Beitritt zu Active Directory verfügt. Sie können optional den NetBIOS-Namen und die Organisationseinheit angeben. Der NetBIOS-Name besteht standardmäßig aus den ersten 15 Zeichen des SMB-Servernamens. Die Organisationseinheit lautet standardmäßig „CN=Computers“.
- Informationen zum UNIX-Verzeichnisdienst (UNIX Directory Service, UDS) für NIS, LDAP oder andere lokale Dateien. Der UDS stellt die UNIX-UID und -GID für jeden AD-Nutzer bereit.

ANMERKUNG: Sie können Zuordnungen für einige NutzerInnen im UDS konfigurieren und die anderen über das Standardkonto oder die automatische Nutzerzuordnung zuordnen lassen.

- DNS-Server- und Domaininformationen
- Schutz-Policy (optional)

Info über diese Aufgabe

Es wird empfohlen, die Anzahl der NAS-Server auf beiden Nodes auszugleichen.

In einer Multiprotokollkonfiguration wird empfohlen, den SMB-Server mit einer Active Directory-Domain zu verbinden, um SIDs zu und von Windows-Nutzernamen aufzulösen. Bei der Verbindung mit einem Multiprotokoll-Dateisystem führen Domänen-NutzerInnen die Nutzerzuordnung durch, um eine Zuordnung von der Windows-SID zur Unix-UID und primären GID zu erstellen.

Eigenständige SMB-Server unterstützen nur lokale Nutzer (die für den reinen SMB-Zugriff vorgesehen und nicht zugeordnet sind) und verfügen nicht über die erforderlichen Zuordnungen für eine ordnungsgemäße Multiprotokollkonfiguration.

Da es unwahrscheinlich ist, dass die UID des lokalen Nutzers im Dateisystem mit der auf dem UNIX-Client konfigurierten UID übereinstimmt, werden die beiden UIDs aus Sicht des NAS-Servers als zwei verschiedene Nutzer betrachtet. Demzufolge verfügt derselbe Nutzer über inkonsistente Berechtigungen für verschiedene Protokolle.

Sie können eine der folgenden Problemumgehungen verwenden:

- UIDs manuell konfigurieren, um sicherzustellen, dass sie mit dem lokalen SMB-Server konsistent sind – Erstellen Sie alle lokalen Nutzer auf einem SMB-Server, bestimmen Sie deren UIDs und konfigurieren Sie dann die UNIX-Clients, um diese UIDs zu verwenden.
- Wenn die Sicherheit kein Problem darstellt, können Sie offene Berechtigungen verwenden.
- Wenn die Dateien für alle zugänglich sind, müssen konsistente Berechtigungen nicht protokollübergreifend beibehalten werden.

Schritte

1. Wählen Sie die Optionen **Storage** > **NAS Servers** aus.
2. Klicken Sie auf der Registerkarte **NAS-Server** auf **Erstellen**.
3. Geben Sie auf der Seite **Details** den Namen des NAS-Servers, die Netzwerkschnittstelle, die IP-Adresse, die Subnetzmaske und die VLAN-ID an.
4. Wählen Sie **Weiter** aus, um die Seite **Freigabeprotokoll** zu öffnen.
5. Wählen Sie auf der Seite **Freigabeprotokoll auswählen** die Option **SMB** und **NFSv3** und/oder **NFSv4** und dann **Weiter** aus.
6. Wählen Sie auf der Registerkarte **Windows Server-Einstellungen** im Feld „Windows Server-Typ“ die Option **Zu Active Directory-Domain hinzufügen** aus und geben Sie die erforderlichen AD-Informationen ein.
7. Klicken Sie optional auf **Erweitert**, um die Standardwerte für den NetBIOS-Namen und die Organisationseinheit zu ändern. Wählen Sie **Speichern** aus und klicken Sie dann auf **Weiter**.
8. Konfigurieren Sie auf der Registerkarte **Unix-Verzeichnisdienste** einen der folgenden Verzeichnisdienste:
   - Lokale Dateien
   - NIS
   - LDAP
   - Lokale Dateien und NIS oder LDAP
9. Wählen Sie optional **Sicheres NFS** aus und schalten Sie dann die **Einstellungen für sicheres NFS** ein, um sicheres NFS zu aktivieren.
10. Wählen Sie auf der Seite **DNS** die Option **DNS-Server aktivieren** aus und geben Sie die folgenden Informationen an:
    - DNS-Transportprotokoll – UDP (Standard), TCP
    - Domain
    - IP-Adresse der DNS-Server
11. Wählen Sie auf der Seite **Schutz-Policy** optional eine Schutz-Policy für den NAS-Server aus.
12. Wählen Sie auf der Seite **Datei-QoS-Policy** optional eine Datei-QoS-Policy für den NAS-Server aus.
13. Wählen Sie **Beenden** aus, um den NAS-Server auszuwählen.

Konfigurieren eines Unix-Verzeichnisdiensts für NAS-Server

Wenn Sie einen NAS-Server konfigurieren, der Multiprotokoll-Dateifreigaben unterstützt, müssen Sie eine Möglichkeit zur Suche nach Identitätsinformationen, z. B. UIDs, GIDs, Netzwerkgruppen, konfigurieren.

Es gibt drei Möglichkeiten, Identitätssuchen zu konfigurieren:

- Verwenden Sie lokale Dateien, allein oder mit einem UDS.
- Konfigurieren Sie einen Unix-Verzeichnisdienst (UDS) mithilfe von NIS.
- Konfigurieren Sie einen UDS mithilfe von LDAP.

Wenn Sie einen NAS-Server erstellen, verwenden Sie das Fenster **Unix-Verzeichnisdienst konfigurieren** im Assistenten **Erstellen eines NAS-Servers**, um Identitätssuchen zu konfigurieren.

Wenn Sie einen UDS für einen vorhandenen NAS-Server konfigurieren, finden Sie die Optionen zur Identitätssuche auf der Registerkarte **Namensservices**:

1. Wählen Sie im PowerStore Manager **Storage** > **NAS-Server** aus.
2. Klicken Sie auf einen NAS-Server, um ihn auszuwählen.
3. Wählen Sie die Registerkarte **Namensservices** aus.

Um die Suchreihenfolge für einen vorhandenen NAS-Server festzulegen, wählen Sie die Registerkarte **Nutzerzuordnung** aus und konfigurieren Sie die Suchreihenfolge. Die Verzeichnisdienste, die Sie zuvor konfiguriert haben, können im Drop-down-Menü ausgewählt werden. Es sind folgende Optionen verfügbar:

- LDAP
- NIS
- Lokale Dateien
- Lokal dann NIS
- Lokal dann LDAP

Verwenden von lokalen Dateien

Lokale Kennwort- und Gruppendateien können verwendet werden, um IDs und Nutzernamen aufzulösen. Die Kennwortdatei verwendet dasselbe Format und dieselbe Syntax wie Unix-basierte Betriebssysteme, sodass eine vorhandene Datei von einem Host auch für den NAS-Server genutzt werden kann.

Die für den NAS-Server relevanten Elemente sind der Nutzername, das gehashte Kennwort (wird für die FTP-Authentifizierung verwendet), die UID und die primäre GID. Die restlichen Elemente in der Kennwortdatei können leer bleiben.

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

- Die Datei wird mit der richtigen Syntax erstellt (für jede Zeile sind sechs Doppelpunkte erforderlich). Weitere Details finden Sie in der Vorlage.
- Jeder Benutzer verfügt über einen eindeutigen Namen und eine eindeutige UID.

Aktivieren lokaler Dateien für einen neuen NAS-Server

Voraussetzungen

Sie können die aktuelle Version der lokalen Dateien vom NAS-Server herunterladen, auf dem auch die Syntax, Beispiele und weitere Details bereitgestellt werden. Nachdem Sie die Datei mit den Nutzerdetails bearbeitet haben, laden Sie sie wieder auf den NAS-Server hoch.

Info über diese Aufgabe

So aktivieren Sie die Verwendung lokaler Dateien für Verzeichnisdienste, wenn Sie einen NAS-Server erstellen:

Schritte

1. Wählen Sie im Fenster **Unix-Verzeichnisdienste** im Assistenten **Erstellen eines NAS-Servers** die Option **Lokale Dateien verwenden** aus.

2. Erstellen Sie die Kennwortdatei für den UDS. Wählen Sie zur Anzeige der Vorlage für die Kennwortdatei **Vorlage für Kennwortdatei** aus.
3. Um die Kennwortdatei auf den NAS-Server hochzuladen, wählen Sie **Kennwortdatei auswählen** aus.

Aktivieren lokaler Dateien für einen vorhandenen NAS-Server

Schritte

1. Wählen Sie im PowerStore Manager **Storage** > **NAS-Server** aus.
2. Wählen Sie den NAS-Server und dann die Registerkarte **Namensservices** aus.
3. Wählen Sie die Registerkarte **Lokale Dateien** aus.
4. Klicken Sie auf den Abwärtspfeil der entsprechenden Datei, um sie abzurufen, und nehmen Sie die erforderlichen Änderungen vor.
5. Um die Dateien hochzuladen, wählen Sie **Lokale Dateien hochladen** aus.
6. Wählen Sie den Dateityp aus und klicken Sie auf **Datei auswählen**.
7. Wählen Sie die Datei aus und klicken Sie auf **Hochladen**.

Konfigurieren eines Unix-Verzeichnisdienstes über NIS

Sie können für den UDS NIS verwenden. Um NIS zu konfigurieren, geben Sie die folgenden Informationen an:

- NIS-Domain
- IP-Adressen für NIS-Server

Wenn Sie IP-Adressen für mehrere NIS-Server angeben, können diese in der Prioritätsliste nach oben oder unten verschoben werden.

Konfigurieren eines UDS über NIS für einen neuen NAS-Server

Schritte

1. Wählen Sie im Fenster **Unix-Verzeichnisdienste** im Assistenten **Erstellen eines NAS-Servers** die Option **Unix-Verzeichnisdienst über NIS oder LDAP aktivieren** aus.
2. Wählen Sie im Fenster **Unix-Verzeichnisdienste** die Option **NIS** aus.
3. Geben Sie eine NIS-Domäne ein und fügen Sie bis zu drei IP-Adressen für die NIS-Server hinzu.

Konfigurieren eines UDS über NIS für einen vorhandenen NAS-Server

Schritte

1. Wählen Sie im PowerStore Manager **Storage** > **NAS-Server** aus.
2. Wählen Sie den NAS-Server und dann die Registerkarte **Namensservices** aus.
3. Wählen Sie die Registerkarte **UDS**.
4. Wählen Sie im Feld **Unix-Verzeichnisdienst** die Option **NIS** aus.
5. Geben Sie eine NIS-Domäne ein und fügen Sie bis zu drei IP-Adressen für die NIS-Server hinzu.
6. Klicken Sie auf **Anwenden**.

Konfigurieren eines Unix-Verzeichnisdienstes über LDAP

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 müssen AdministratorInnen auf der IDMU die Eigenschaften der jeweiligen NutzerInnen aufrufen und auf der Registerkarte „UNIX-Attribute“ eine UID hinzufügen.

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

- Die LDAP-Konfiguration entspricht einem der unterstützten Schemata.
- Alle Container, die in der Datei `ldap.conf` angegeben sind, sind gültige und vorhandene Container.

- Jeder LDAP-Benutzer wird mit einer eindeutigen UID konfiguriert.

Mithilfe der Option `-ldap` des Servicebefehls `svc_nas_tools` können Sie ebenfalls LDAP-Probleme beheben. Mit diesem Befehl kann eine erweiterte Diagnose für die Verbindung zum LDAP-Server angezeigt und eine Auflösung des Nutzernamens ausgeführt werden, um sicherzustellen, dass die LDAP-Einstellungen korrekt sind.

Konfigurieren eines UDS über LDAP für einen neuen NAS-Server

Schritte

1. Wählen Sie im Fenster **Unix-Verzeichnisdienste** im Assistenten **Erstellen eines NAS-Servers** die Option **Unix-Verzeichnisdienst über NIS oder LDAP aktivieren** aus.
2. Wählen Sie im Fenster **Unix-Verzeichnisdienste** die Option **LDAP** aus.
3. Geben Sie die Portnummer ein.

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

4. Geben Sie die IP-Adressen (eine einzelne Adresse, mehrere durch Kommas getrennte Adressen oder einen Adressbereich) ein und wählen Sie **Hinzufügen** aus.
5. Konfigurieren Sie die LDAP-Authentifizierung, wie unter LDAP-Authentifizierung beschrieben.
6. Geben Sie den Basis-DN im X.509-Format ein.
7. Geben Sie für einen iPlanet-LDAP-Server den Profil-DN ein (optional).
8. Wenn Sie sicheres LDAP verwenden möchten, wählen Sie die entsprechende Option aus.
9. Wählen Sie **Bestätigen** aus.

Konfigurieren eines UDS über LDAP für einen vorhandenen NAS-Server

Schritte

1. Wählen Sie im PowerStore Manager **Storage** > **NAS-Server** aus.
2. Wählen Sie den NAS-Server und dann die Registerkarte **Namensservices** aus.
3. Wählen Sie die Registerkarte **UDS**.
4. Wählen Sie im Feld **Unix-Verzeichnisdienst** die Option **LDAP** aus.
5. Geben Sie die Portnummer ein.

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

6. Geben Sie die IP-Adressen (eine einzelne Adresse, mehrere durch Kommas getrennte Adressen oder einen Adressbereich) ein und wählen Sie **Hinzufügen** aus.
7. Konfigurieren Sie die LDAP-Authentifizierung, wie unter LDAP-Authentifizierung beschrieben.
8. Geben Sie den Basis-DN im X.509-Format ein.
9. Geben Sie für einen iPlanet-LDAP-Server den Profil-DN ein (optional).
10. Um ein LDAP-Schema hochzuladen, wählen Sie **Neues Schema hochladen** und dann **Datei auswählen** aus.
11. Wenn Sie sicheres LDAP verwenden möchten, wählen Sie die entsprechende Option aus.
12. Wählen Sie **Bestätigen** aus.

LDAP-Authentifizierung

In der folgenden Tabelle sind die möglichen LDAP-Authentifizierungsoptionen zusammengefasst:

Tabelle 6. LDAP-Authentifizierung

Option	Überlegungen
LDAP mit anonymer oder einfacher Authentifizierung	Fügen Sie für eine anonyme Authentifizierung die LDAP-Server hinzu und geben Sie die von den LDAP-Servern verwendete Portnummer, den Basis-DN und den Profil-DN für den iPlanet/OpenLDAP-Server an.

Tabelle 6. LDAP-Authentifizierung (fortgesetzt)

Option	Überlegungen
	Fügen Sie für die einfache Authentifizierung die LDAP-Server hinzu und geben Sie Folgendes an: ● Bei Verwendung von AD, LDAP/IDMU: ○ Von den LDAP-Servern verwendete Portnummer ○ Nutzerkonto im LDAP-Format, z. B. cn=administrator,cn=users,dc=svt,dc=lab,dc=com ○ Passwort für das Benutzerkonto ○ Basis-DN, der mit dem vollständig qualifizierten Domainnamen (z. B. svt.lab.com) identisch ist ● Bei Verwendung des iPlanet/OpenLDAP-Servers: ○ Nutzerkonto im LDAP-Format, z. B. cn=administrator,cn=users,dc=svt,dc=lab,dc=com ○ Password ○ Basis-DN Beispiel: Bei Verwendung von svt.lab.com wäre der Basis-DN „DC=svt,DC=lab,DC=com“ ○ Profil-DN für den iPlanet/OpenLDAP-Server
LDAP mit Kerberos-Authentifizierung	Es gibt zwei Methoden zur Konfiguration von Kerberos: ● Sie authentifizieren sich bei der SMB-Domain. Mit dieser Option können Sie sich entweder über das SMB-Serverkonto oder mit anderen Anmeldedaten authentifizieren. ● Konfigurieren Sie einen nutzerdefinierten Bereich, um auf alle Arten von Kerberos-Bereichen (Windows, MIT, Heimdal) zu verweisen. Mit dieser Option verwendet der NAS-Server den nutzerdefinierten Kerberos-Bereich, der im Unterabschnitt „Kerberos“ auf der Registerkarte **Sicherheit** des NAS-Servers festgelegt wurde. Die AD-Authentifizierung des SMB-Servers wird nicht verwendet, wenn Sie diese Option auswählen. **ANMERKUNG:** Wenn Sie sicheres NFS mit einem benutzerdefinierten Bereich verwenden, müssen Sie eine Keytab-Datei hochladen.

Bearbeiten des OpenLDAP-Schemas für Linux

Möglicherweise muss das OpenLDAP-Schema für Linux geändert werden, wenn bestimmte NFS-Dateisysteme in Netzwerkgruppen exportiert werden.

Beim Herunterladen von OpenLDAP von der OpenLDAP-Organisation hat der LDAP-Server ein Schema, das sich strikt an RFC 2307 hält:

```
( nisSchema.1.14 NAME 'nisNetgroupTriple'
DESC 'Netgroup triple'
SYNTAX 'nisNetgroupTripleSyntax' )
```

Das LDAP-Serverschema kann auch RFC 2307bis entsprechen:

```
( 1.3.6.1.1.1.1.14 NAME 'nisNetgroupTriple'
DESC 'Netgroup triple'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Mit PowerStore werden sowohl RFC 2307 als auch RFC 2307bis unterstützt.

In RFC 2307 muss bei der Syntax der Netzwerkdreiergruppe die Groß- und Kleinschreibung beachtet werden, obwohl bei Hostnamen in Netzwerkdreiergruppen üblicherweise nicht zwischen Groß- und Kleinschreibung unterschieden werden sollte. Wenn Sie Hostnamen mit unterschiedlicher Groß- und Kleinschreibung (z. B. werden für die Hostnamen in DNS Großbuchstaben und in den Netzwerkdreiergruppen Kleinbuchstaben verwendet, wie im LDAP-Verzeichnis definiert) abgleichen wollen, muss das LDAP-Schema geändert werden.

Da es sich bei RFC 2037bis um einen Entwurf handelt, der von der OpenLDAP-Organisation nicht erkannt wird, muss das OpenLDAP-Schema für Linux geändert werden, damit es mit PowerStore kompatibel ist. Das OpenLDAP-Schema für PowerStore muss wie folgt geändert werden:

Suchen Sie in der Datei `/etc/openldap/schema/nis.schema` auf Ihrem OpenLDAP-Server den folgenden Eintrag:

```
attributetype ( 1.3.6.1.1.1.1.14 NAME 'nisNetgroupTriple'
DESC 'Netgroup triple'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Bearbeiten Sie den Eintrag wie folgt (fügen Sie die EQUALITY-Richtlinie hinzu):

```
attributetype ( 1.3.6.1.1.1.1.14 NAME 'nisNetgroupTriple'
DESC 'Netgroup triple'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Hochladen oder Anzeigen eines LDAPS-CA-Zertifikats für einen NAS-Server

Info über diese Aufgabe

ANMERKUNG: Dieses Verfahren ist nur erforderlich, wenn Sie LDAPS verwenden.

Schritte

1. Wählen Sie die Optionen **Storage** > **NAS Servers** aus.
2. Wählen Sie den NAS-Server und dann die Registerkarte **Namensservices** aus.
3. Wählen Sie die Option **LDAP Secure (SSL verwenden)** und dann die Option **Zertifizierungsstellen-(CA-)Zertifikat erzwingen** aus.

   ANMERKUNG: Diese Optionen sind für die anonyme und die einfache Authentifizierung verfügbar.

4. Wenn bereits ein CA-Zertifikat hochgeladen wurde, wählen Sie **CA-Zertifikat abrufen** aus, um es anzuzeigen.
5. Wählen Sie **CA-Zertifikat hochladen** aus, suchen Sie das hochzuladende Zertifikat und klicken Sie auf **Hochladen**.

Ändern der Unix-Zugangsdaten für NAS-Server

Schritte

1. Wählen Sie die Optionen **Storage** > **NAS Servers** aus.
2. Wählen Sie den NAS-Server aus der Liste aus und wählen Sie anschließend die Registerkarte **Freigabeprotokolle**.
3. Wählen Sie die Registerkarte **NFS-Server** aus.
4. Nehmen Sie die erforderlichen Änderungen vor, wie in der folgenden Tabelle beschrieben.

Tabelle 7. Unix-Zugangsdateneinstellungen für NAS-Server

Aufgabe	Beschreibung
Erweitern Sie die Unix-Zugangsdaten, damit das Storage-System mehr als 16 Gruppen-GIDs erhält. **ANMERKUNG:** Dies ist nur erforderlich, wenn Sie NutzerInnen mit mehr als 16 GIDs haben. **ANMERKUNG:** Da bei sicherem NFS die Unix-Zugangsdaten immer vom NAS-Server erstellt werden, wird diese Option nicht angewendet.	Aktivieren oder deaktivieren Sie die Option **Erweiterte Zugangsdaten**. ● Wenn diese Option aktiviert ist, verwendet der NAS-Server die Nutzer-ID (UID), um die primäre Gruppen-ID (GID) sowie alle Gruppen-GIDs, zu denen sie gehört, abzurufen. Der NAS-Server ruft die GIDs aus der lokalen Passwortdatei oder dem UDS ab. ● Wenn diese Option deaktiviert ist, werden die Unix-Zugangsdaten der NFS-Anfrage direkt aus den Netzwerkinformationen extrahiert, die im Frame enthalten sind. Diese Methode bietet bessere Performance, ist jedoch auf höchstens 16 Gruppen-GIDs beschränkt.
Geben Sie eine Aufbewahrungsfrist für Unix-Zugangsdaten im Cache an. Diese Option kann zu einer besseren Performance führen, da die Unix-Zugangsdaten aus dem Cache verwendet werden anstatt sie bei jeder Anfrage neu aufzubauen.	Geben Sie im Feld **Credential cache retention** einen Zeitraum (in Minuten) an, während dem Zugangsdaten im Cache aufbewahrt werden sollen. Der Bereich ist 1 bis 35.791.394, wobei der Standardwert 15 Minuten beträgt.

Konfigurieren von Benutzerzuordnungen für Multiprotokoll-NAS-Server

Eine Multiprotokollumgebung erfordert folgende Arten von Benutzerzuordnungen:

- Um auf ein Dateisystem zuzugreifen, das mit einer Unix-Zugriffs-Policy konfiguriert ist, muss ein Windows-Nutzername einem entsprechenden Unix-Nutzernamen zugeordnet werden. Darüber hinaus muss das Storage-System den Unix-Nutzernamen in eine UID auflösen können.
- Ein Unix-Nutzername muss einem entsprechenden Windows-Nutzernamen zugeordnet werden, wenn NFS verwendet wird, um auf ein Dateisystem zuzugreifen, das mit einer Windows-Zugriffs-Policy konfiguriert ist.
- Ein/e Unix-NutzerIn muss keinem/keiner entsprechenden Windows-NutzerIn zugeordnet werden, wenn NFS verwendet wird, um auf ein Dateisystem zuzugreifen, das mit einer Unix- oder einer nativen Zugriffs-Policy konfiguriert ist.

Das System erstellt automatisch eine Zuordnung zwischen einem/einer Windows-NutzerIn und einem/einer Unix-NutzerIn, wenn im Unix-Verzeichnisdienst (UDS) oder in der lokalen Kennwortdatei und im Windows Active Directory (AD) der gleiche Nutzername festgelegt ist. Bei Unix-Nutzernamen muss die Groß- und Kleinschreibung beachtet werden. Beispiel: Windows-NutzerIn1 wird automatisch Unix-NutzerIn1 zugeordnet. Wenn die Nutzernamen unterschiedlich sind, können Sie eine nutzerdefinierte Zuordnungsdatei (ntxmap) hochladen, um spezifische Zuordnungsregeln zu erstellen. Diese Regeln können bidirektional sein oder sie können verwendet werden, um Windows-NutzerInnen zu Unix-NutzerInnen oder Unix-NutzerInnen zu Windows-NutzerInnen zuzuordnen. Die Regeln unterstützen Platzhalter und Substitutionen.

Um NutzerInnen mit nicht zugeordneten Nutzernamen den Zugriff auf ein Dateisystem zu ermöglichen, können Sie die automatische Nutzerzuordnung festlegen (dadurch werden Quoten aktiviert). Eine weitere Option ist das Festlegen von Unix- und Windows-Standardkonten für den NAS-Server.

Automatischer Nutzerzuordnungsprozess

Der automatische Nutzerzuordnungsprozess ordnet die Unix-UID der Windows-SID zu. Die Zuordnung erfolgt durch den Abgleich des Nutzernamens aus dem UDS oder den lokalen Dateien mit dem Nutzernamen aus dem AD.

Automatische Zuordnung für Windows-Benutzer

Wenn Sie die Freigabeprotokolle des NAS-Servers ändern, können Sie das System optional anweisen, automatisch eine Unix-UID für jede/n Windows-NutzerIn zu erstellen, der/die nicht bereits über einen Verzeichnisdienst (LDAP oder NIS) oder über lokale Dateien einem Unix-Konto zugeordnet wurde.

ANMERKUNG: Verwenden Sie die automatische Zuordnung nur, wenn es keine Rolle spielt, welche UID welchem/welcher NutzerIn zugewiesen wird.

Diese Option ist verfügbar, wenn kein Unix-Standardnutzer konfiguriert ist. Sie ist für Multiprotokoll-Konfigurationen vorgesehen, bei denen die meisten NutzerInnen Windows-NutzerInnen sind. Mit dieser Option können die Dateisystem-Quoten für jede/n nicht zugeordnete/n Windows-NutzerIn beibehalten werden (Dateisystem-Quoten basieren auf der Unix-UID). Die automatisch erzeugten Unix-UIDs liegen im reservierten Bereich von 0x80000001 bis 0x803FFFFF.

ANMERKUNG: Wenn ein Unix-Standardnutzer konfiguriert ist, können Sie die automatische Zuordnung für Windows-NutzerInnen nicht aktivieren.

Standardnutzernamen

Sie können optional Standardbenutzerkonten für einen NAS-Server konfigurieren, wenn Sie die Freigabeprotokolle des NAS-Servers ändern:

- Das standardmäßige Unix-Benutzerkonto gibt das Unix-Konto an, das für den Zugriff auf das Dateisystem von einem nicht zugeordneten Windows-Konto aus verwendet werden soll. Wenn Sie kein Unix-Standardkonto angeben, kann ein/e nicht zugeordnete/r Windows-NutzerIn nicht auf das System zugreifen. Der Unix-Standardnutzer kann ein gültiger vorhandener Unix-Kontoname sein oder das Format `@uid=xxxx, gid=yyyy@` haben, wobei xxxx die numerischen Dezimalwerte der UID sind und yyyy für die primäre GID steht. Wenn Sie einen Unix-Standardnutzer konfigurieren, beachten Sie Folgendes:
  - Wenn Sie für Windows-NutzerInnen ein Unix-Standardkonto verwenden, werden diese einer UID zugewiesen. Daher wird nur eine Nutzerquote auf all diese NutzerInnen angewendet.

- Durch Festlegen des Standardnutzers auf die UID „0“ oder auf eine/n NutzerIn, der/die in eine UID „0“ aufgelöst wird, wird diesem/dieser NutzerIn vollständiger Stammzugriff gewährt, was aus Sicherheitsgründen jedoch bedenklich sein kann.

- Wenn die Dateisystem-Zugriffs-Policy auf Windows basiert, legt das Windows-Standardkonto fest, welches Windows-Konto für den Dateisystemzugriff von einem nicht zugeordneten Unix-Konto verwendet werden soll. Bei der Windows-Sicherheitsautorisierung werden die Zugangsdaten aus dem Windows-Domain-Controller (DC) und der Datenbank der lokalen Gruppe (LGDB) des SMB-Servers erstellt. Wenn Sie kein Windows-Standardkonto festlegen und der Windows-Standardnutzer nicht im Windows-DC oder in der -LGDB gefunden wird, kann ein/e nicht zugeordnete/r Unix-NutzerIn möglicherweise nicht auf ein Dateisystem mit einer Windows-Zugriffs-Policy zugreifen. Das standardmäßige Windows-Benutzerkonto muss ein vorhandenes Benutzerkonto im AD sein, dem der SMB-Server des NAS-Servers hinzugefügt wird. Hierbei wird zwischen Groß- und Kleinschreibung unterschieden.

Anpassen der Nutzerzuordnungsdatei

Nachdem Sie einen NAS-Server erstellt haben, können Sie optional eine kundenspezifische Nutzerzuordnungsdatei (ntxmap) verwenden, um ein oder mehrere Windows-Nutzerkonten einem oder mehreren Unix-Nutzerkonten bzw. ein oder mehrere Unix-Nutzerkonten einem oder mehreren Windows-Nutzerkonten zuzuordnen (beide Richtungen sind zulässig). Durch das Anpassen der Nutzerzuordnungsdatei können Sie Dateisystemzugriff gewähren, wenn:

- einem Windows-Nutzerkonto kein entsprechendes Unix-Nutzerkonto zugeordnet ist.
- es sich um eine Zugriffs-Policy für ein Windows-Dateisystem handelt und einem Unix-Nutzerkonto kein entsprechendes Windows-Nutzerkonto zugeordnet ist.
- ein Windows-Nutzerkonto und ein Unix-Nutzerkonto vorhanden sind, diese jedoch unterschiedliche Benennungsregeln verwenden. Bei Unix-Nutzernamen muss die Groß- und Kleinschreibung beachtet werden.

Die Nutzerzuordnungsdatei unterstützt die Verwendung von Platzhaltern und Ersatzzeichenfolgen.

Um eine kundenspezifische Nutzerzuordnungsdatei zu verwenden, wählen Sie **Storage** > **NAS-Server** > **[NAS-Server]** > **Namensservices** > **Lokale Dateien** aus und laden Sie die ntxmap-Dateivorlage herunter. Passen Sie die Datei nach dem Herunterladen an und laden Sie sie wieder in das System hoch.

ANMERKUNG: Die Syntax für die Zuordnungsdatei wird in der Dateivorlage angezeigt.

Ändern von Benutzerzuordnungen bei NAS-Servern

Info über diese Aufgabe

Sie können die Benutzerzuordnungen für Multiprotokoll-NAS-Server ändern.

Schritte

1. Wählen Sie die Optionen **Storage** > **NAS Servers** aus.
2. Wählen Sie den NAS-Server und dann die Registerkarte **Namensservices** aus.
3. Nehmen Sie die gewünschten Änderungen vor, wie in der folgenden Tabelle beschrieben:

Tabelle 8. Nutzerzuordnungen auf NAS-Servern

Aufgabe	Beschreibung
Ordnen Sie Unix-Konten und Windows-Konten mit unterschiedlichen Nutzernamen einander zu.	Mit der ntxmap-Konfigurationsdatei können Sie Unix- und Windows-Konten mit unterschiedlichen Nutzernamen einander zuordnen. Die Syntax für die ntxmap-Datei wird in der Vorlage angezeigt, die Sie mit den folgenden Schritten abrufen: a. Wählen Sie **Lokale Dateien** aus. b. Klicken Sie in der Liste der lokalen Dateien auf das Download-Symbol neben ntxmap, um sie abzurufen. **ANMERKUNG:** Wenn keine kundenspezifische Zuordnungsdatei vorhanden ist, ruft der NAS-Server eine Vorlage für die Konfiguration ab. c. Fügen Sie der Datei mithilfe eines Texteditors Benutzerkontenzuordnungen hinzu oder ändern Sie sie.

Tabelle 8. Nutzerzuordnungen auf NAS-Servern (fortgesetzt)

Aufgabe	Beschreibung
	d. Wählen Sie **Lokale Dateien hochladen** und dann **ntxmap** aus den Dateityp-Optionen aus. e. Verwenden Sie den Browser, um die aktualisierte Datei auszuwählen, und wählen Sie dann **Hochladen** aus.
Erzeugen Sie automatisch eine Unix-UID für jede/n Windows-NutzerIn, der/die keinem Unix-Konto zugeordnet ist.	a. Wählen Sie **Nutzerzuordnung** aus. b. Wählen Sie die Option **Automatische Zuordnung für nicht zugeordnete Windows-Konten/Nutzer aktivieren** aus. Diese Option ist für Umgebungen mit mehreren Protokollen vorgesehen, in denen die meisten Benutzer Windows-Benutzer sind. Wenn Sie diese Option auswählen, erzeugt das System Unix-UIDs für Windows-NutzerInnen, die nicht bereits über einen Verzeichnisdienst (LDAP oder NIS) oder über lokale Dateien Unix-Konten zugeordnet sind. Mit dieser Funktion können Dateisystemquoten für nicht zugeordnete Windows-Benutzer aufbewahrt werden.
Aktivieren oder deaktivieren Sie Standardkonten für nicht zugeordnete Benutzer.	a. Wählen Sie **Nutzerzuordnung** aus. b. Aktivieren oder deaktivieren Sie die Option **Standardkonto für nicht zugeordnete Nutzer aktivieren**. c. Wenn Sie diese Option aktiviert haben, legen Sie den Unix-Standardnutzer (Name oder UID/GID) und den standardmäßigen Windows-Nutzernamen fest. Wenn Sie für nicht zugeordnete NutzerInnen Standardkonten aktivieren, können Sie Unix- und Windows-Standardkonten angeben, die vom System verwendet werden, um nicht zugeordneten NutzerInnen Dateisystemzugriff zu gewähren. Der Unix-Standardnutzer kann ein gültiger vorhandener Unix-Kontoname sein oder das Format `@uid=xxxx,gid=yyyy@` haben, wobei xxxx die numerischen Dezimalwerte der UID sind und yyyy für die primäre GID steht. **ANMERKUNG:** Wenn Sie Standardkonten verwenden, werden die NutzerInnen einer UID zugeordnet und es gilt nur eine Nutzerquote für alle NutzerInnen.

4

Konfigurieren eines Dateisystems für die Multiprotokoll-Dateifreigabe

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Erstellen eines Dateisystems

Voraussetzungen

- Ein NAS-Server, der für die Unterstützung von SMB- und NFS-Protokollen konfiguriert ist

Schritte

1. Wählen Sie die Optionen **Storage** > **File Systems** aus.
2. Klicken Sie auf **Erstellen**, um den Assistenten **Erstellen eines NAS-Servers** zu öffnen.
3. Konfigurieren Sie das Dateisystem gemäß den Schritten im Assistenten:

Option	Beschreibung
Typ auswählen	Wählen Sie **Allgemein** als Dateisystemtyp aus.
Wählen Sie den NAS-Server aus.	Wählen Sie einen SMB- und NFS-fähigen NAS-Server aus. Optional können Sie die erweiterten SMB-Einstellungen festlegen. Weitere Informationen finden Sie unter Erweiterte Dateisystemeinstellungen für SMB.
Details des Dateisystems	Geben Sie den Namen, die Beschreibung (optional) 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. Beispiel: Nach der Erstellung eines 100-GB-Thin-Dateisystems zeigt das PowerStore T-Modell sofort 1,5 GB an, die verwendet werden. Wenn das Dateisystem auf einem Host gemountet ist, werden 98,5 GB nutzbare Kapazität angezeigt. Dies ist darauf zurückzuführen, dass der Metadatenspeicherplatz in der nutzbaren Dateisystemkapazität reserviert wird.
Aufbewahrung auf Dateiebene	Wählen Sie einen Aufbewahrungstyp auf Dateiebene aus: • Aus – Es wird keine Aufbewahrung auf Dateiebene festgelegt. • Enterprise (FLR-E) – Schützt Inhalte vor Änderungen, die von NutzerInnen über SMB, 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 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:** Der FLR-Status und Dateiaufbewahrungstyp werden bei der Dateisystemerstellung festgelegt und können nicht geändert werden. Legen Sie die Aufbewahrungszeiträume fest:

Option	Beschreibung
	• 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. Der Wert ist unbegrenzt. • Maximum: Gibt den längsten Zeitraum an, für den Dateien gesperrt werden können. Der Wert ist unbegrenzt.
NFS-Export (optional)	Konfigurieren Sie einen Namen und eine Beschreibung für den ersten Export des Dateisystems. Nach der ersten Dateisystemkonfiguration können Sie Exporte zum Dateisystem hinzufügen.
Zugriffskonfiguration	Fügen Sie Hosts hinzu.

SMB-Freigabe (optional)	Konfigurieren Sie die erste SMB-Freigabe:
	ANMERKUNG: Sie können dem Dateisystem nach der anfänglichen Dateisystemkonfiguration Freigaben hinzufügen.
	• Name
	• Beschreibung (optional)
	• Offlineverfügbarkeit: Legt die Client-seitige Zwischenspeicherung von Offlinedateien fest.
	  ○ Keine: Die Client-seitige Zwischenspeicherung von Offlinedateien ist nicht konfiguriert.
	  ○ Manuell: Dateien werden nur dann zwischengespeichert und sind offline verfügbar, wenn dies ausdrücklich angefordert wird.
	  ○ Programme: Ausführbare Dateien, die zuvor lokal zwischengespeichert wurden, werden von der zwischengespeicherten Kopie statt der Kopie auf der Freigabe ausgeführt.
	  ○ Dokumente: Wann immer ein/e Nutzerln über eine Freigabe auf eine Datei oder ein Programm zugreift, wird dieser Inhalt automatisch zwischengespeichert, damit er offline verfügbar ist. Zwischengespeicherte Inhalte werden kontinuierlich mit der Version auf dem Server synchronisiert.
	Konfigurieren Sie optional die erweiterte SMB-Einstellungen für SMB-Freigaben. Weitere Informationen finden Sie unter Erweiterte Eigenschaften für SMB-Freigaben.
	• **Kontinuierliche Verfügbarkeit**
	• **Protokollverschlüsselung**
	• **Access Based Enumeration**
	• **Branch Cache aktiviert**

Schutz-Policy (optional)	Geben Sie optional eine Schutz-Policy für das Dateisystem an. PowerStore unterstützt Snapshots und Replikation für Datei-Storage-Schutz.
Datei-QoS-Policy (optional)	Geben Sie optional eine QoS-Policy für das Dateisystem an. **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 bei Bedarf zurück, um Änderungen vorzunehmen.

4. Klicken Sie auf **Create File System**.
Das Dateisystem wird in der Liste der Dateisysteme angezeigt. Wenn Sie einen NFS-Export oder eine SMB-Freigabe erstellt haben, werden diese in der entsprechenden Liste angezeigt.

Erweiterte Dateisystemeinstellungen für SMB

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

Tabelle 9. 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

Tabelle 9. Erweiterte Dateisystemeinstellungen für SMB (fortgesetzt)

Einstellung	Beschreibung
	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. Die Option für synchrone Schreibvorgänge 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	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 ermöglicht 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.

5

Konfigurieren von Freigaben

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Freigeben und Exportieren von lokalen Pfaden und Exportpfaden

In der folgenden Tabelle sind die Pfadeinstellungen für Freigaben und Exporte enthalten:

Tabelle 10. Pfadeinstellungen für Freigaben und Exporte

Einstellung	Beschreibung
Lokaler Pfad	Der Pfad zur Dateisystem-Storage-Ressource im Storage-System. Dieser Pfad gibt den eindeutigen Speicherort der Freigabe oder des Exports im Storage-System an. ● SMB-Shares ○ In einem SMB-Dateisystem können mehrere Freigaben mit demselben lokalen Pfad erstellt werden. In diesen Fällen können Sie unterschiedliche hostseitige Zugriffskontrollen für unterschiedliche NutzerInnen festlegen, die Freigaben innerhalb des Dateisystems greifen jedoch alle 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-Freigaben über die Microsoft Management Console erstellen und managen. ● NFS-Exporte ○ Jeder NFS-Export muss über einen eigenen eindeutigen lokalen Pfad verfügen. PowerStore weist diesen Pfad automatisch der ursprünglichen Freigabe zu, die in einem neuen Dateisystem erstellt wurde. Der Name des lokalen Pfads basiert auf dem Namen des Dateisystems. ○ Bevor Sie zusätzliche Freigaben innerhalb eines NFS-Dateisystems erstellen können, müssen Sie ein Verzeichnis erstellen, das von einem Linux-/UNIX-Host aus freigegeben werden kann, das mit dem Dateisystem verbunden ist. Dann können Sie einen Export aus PowerStore heraus erstellen und die Zugriffsberechtigungen entsprechend festlegen.
Exportpfad	Der vom Host für die Verbindung mit der Freigabe oder dem Export verwendete Pfad. PowerStore erstellt den Exportpfad anhand des Namens der Freigabe oder des Exports und des

Tabelle 10. Pfadeinstellungen für Freigaben und Exporte (fortgesetzt)

Einstellung	Beschreibung
	Namens des Dateisystems, in dem diese sich befinden. Hosts verwenden entweder den Exportnamen oder den Exportpfad zum Einhängen oder Zuordnen der Freigabe oder des Exports von einem Netzwerkhost aus. Dieses Verhalten wird mithilfe von NFS-Aliasse für Freigaben aktiviert.

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-Freigabes** aus.
2. Klicken Sie auf **Create** und führen Sie die Schritte des Assistenten **SMB-Freigabe erstellen** aus.

Seite	Description
Dateisystem auswählen	Wählen Sie ein Dateisystem aus, das für SMB aktiviert wurde.
Snapshot auswählen (optional)	Wählen Sie einen der Dateisystem-Snapshots aus, auf dem die Freigabe erstellt werden soll.
Details zur SMB-Freigabe	Geben Sie einen Namen, eine Beschreibung 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-Freigaben über die Microsoft Management Console erstellen und managen. PowerStore zeigt auch den SMB-Freigabepfad an, über den der Host eine Verbindung mit der Freigabe herstellt. Beim Freigabepfad handelt es sich um die IP-Adresse oder den Namen des NAS-Servers und den Namen der Freigabe. Hosts verwenden Freigabepfad zum Mounten oder Zuordnen der Freigabe von einem Netzwerkhost aus.
Erweiterte Einstellungen für die SMB-Freigabe	Aktivieren Sie eine oder mehrere der erweiterten SMB-Einstellungen: ● Kontinuierliche Verfügbarkeit ● Protokollverschlüsselung ● Access-based Enumeration ● Branch Cache aktiviert ● Offlineverfügbarkeit (Standardeinstellung – keine) ● Umask (Standard – 022)

Nächste Schritte

Wenn Sie eine Freigabe erstellen, 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-Freigabe** 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 11. 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 RejectUnencryptedAccess-Registrierungsschlüssel auf dem NAS-Server konfigurieren. 1 (Standardwert) lehnt nicht verschlüsselten 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.
Distributed File System (DFS)	(Schreibgeschützt) Ermöglicht Ihnen das Gruppieren von Dateien auf verschiedenen Freigaben, indem sie transparent in einem oder mehreren DFS-Namespaces verbunden werden. Dadurch wird der Prozess der Verschiebung von Daten von einer Share in eine andere vereinfacht. Diese Option ist in Unisphere schreibgeschützt, da Sie DFS über Microsoft-Hosts managen. Weitere Informationen finden Sie in der Dokumentation zum Microsoft Distributed File System.
Offlineverfügbarkeit	Konfiguriert die clientseitige Zwischenspeicherung von Offlinedateien: • **Manuel**: Dateien werden nur zwischengespeichert und sind offline verfügbar, wenn dies ausdrücklich angefordert wird. • **Von Nutzern geöffnete Programme und Dateien**: Alle Dateien, die von den Clients aus der Freigabe geöffnet werden, werden automatisch zwischengespeichert und offline zur Verfügung gestellt. Clients öffnen diese Dateien von der Share, wenn sie mit ihr verbunden sind. Diese Option wird für Dateien mit gemeinsamer Arbeit empfohlen. • **Von Nutzern geöffnete Programme und Dateien, für Performance optimiert**: Alle Dateien, die von den Clients aus der Freigabe geöffnet werden, werden automatisch zwischengespeichert und offline zur Verfügung gestellt. Clients öffnen diese Dateien aus dem lokalen Cache der Share, wenn möglich, selbst dann, wenn sie mit dem Netzwerk verbunden sind. Diese Option wird für ausführbare Programme empfohlen. • **Keine**: Das clientseitige Zwischenspeichern von Offlinedateien ist nicht konfiguriert.
UMASK	(Gilt für SMB-Freigaben eines Dateisystems, das Multiprotokollzugriff mit einer UNIX- oder einer nativen Zugriffs-Policy unterstützt.) Eine Bitmask, die zeigt, welche UNIX-Berechtigungen für die auf der Freigabe erstellten Dateien ausgeschlossen sind. Die Standardberechtigungen sind: • 666 für Dateien, die allen Nutzern Lese- und Schreibberechtigungen gewährt. • 777 für Verzeichnisse, die allen Nutzern Lese-, Schreib- und Ausführungsberechtigungen gewährt. Wenn UMASK auf 022 festgelegt ist, werden die folgenden Berechtigungen erteilt: • 644 für Dateien, die dem Dateiinhaber Lese- und Schreibberechtigungen und allen anderen Nutzern Leseberechtigungen erteilt.

Tabelle 11. Advanced SMB Properties (fortgesetzt)

Option	Beschreibung
	• 755 für Verzeichnisse, die den Verzeichnisinhabern Lese-, Schreib- und Ausführungsberechtigungen und allen anderen Nutzern Lese- und Ausführungsberechtigungen erteilt. **ANMERKUNG:** Wenn eine NFSv4-ACL-Vererbung vorhanden ist, hat sie Vorrang vor der UMASK-Einstellung. • Um die ausgeschlossenen Berechtigungen zu ändern, klicken Sie auf **Ändern** und aktivieren oder deaktivieren Sie dann Berechtigungen. • Um die Bitmask auf den Standardwert (022) festzulegen, klicken Sie auf **Standard festlegen**. Wenn der Wert 022 festgelegt ist, können nur Sie Daten schreiben und alle anderen Benutzer Daten lesen. Weitere Informationen finden Sie in der UNIX-Dokumentation.

Erstellen eines NFS-Exports

Sie können einen NFS-Export in einem Dateisystem erstellen.

Schritte

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.

6

Aktivieren der Multiprotokoll-Dateifreigabe auf einem vorhandenen NAS-Server

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Aktivieren der Multiprotokoll-Dateifreigabe auf einem vorhandenen NFS-fähigen NAS-Server

Info über diese Aufgabe

Wenn Sie die Multiprotokoll-Dateifreigabe konfigurieren, wird für alle vorhandenen Dateisysteme die native Sicherheitszugriffs-Policy aktiviert.

Schritte

1. Wählen Sie die Optionen **Storage** > **NAS Servers** aus.
2. Wählen Sie den entsprechenden NAS-Server und dann die Registerkarte **Namensservices** aus.
3. Konfigurieren Sie einen der folgenden Verzeichnisdienste, wenn noch kein Unix-Verzeichnisdienst (Unix Directory Service, UDS) für den NAS-Server konfiguriert wurde bzw. keine lokalen Dateien konfiguriert wurden:
   - NIS
   - LDAP
   - Lokale Dateien
   - Lokale Dateien und NIS oder LDAP

   Sie können LDAP für die Verwendung von anonymer, einfacher und Kerberos-Authentifizierung konfigurieren. Sie können LDAP auch mit SSL (LDAP Secure) konfigurieren und die Verwendung eines Zertifikats von einer Zertifizierungsstelle bei der Authentifizierung durchsetzen.
4. Wählen Sie die Registerkarte **Nutzerzuordnung** aus und konfigurieren Sie die Suchreihenfolge. Die Verzeichnisdienste, die Sie zuvor konfiguriert haben, können im Drop-down-Menü ausgewählt werden.
5. Wählen Sie die Registerkarte **Nutzerzuordnung** aus und aktivieren Sie die automatische Zuordnung oder das Standardkonto für nicht zugeordnete NutzerInnen. Wenn Sie das Standardkonto aktiviert haben, geben Sie die Windows- und Unix-Standardkonten an. Sie können auch **`ntxmap`** (auf der Registerkarte **Lokale Dateien**) verwenden, um Windows- und Unix-NutzerInnen zuzuordnen.
6. Wählen Sie die Seite **Freigabeprotokolle** und dann **SMB-Server** aus.
7. Führen Sie auf der Registerkarte **SMB-Server** die folgenden Schritte aus:
   - Aktivieren Sie den SMB-Server.
   - Fügen Sie den NAS-Server zur AD-Domäne (Active Directory) hinzu.
   - Wählen Sie optional **Erweitert** aus, um den NetBIOS-Namen und die Organisationseinheit anzugeben. Der NetBIOS-Name besteht standardmäßig aus den ersten 15 Zeichen des SMB-Servernamens. Die Organisationseinheit lautet standardmäßig „CN=Computers“.

Aktivieren der Multiprotokoll-Dateifreigabe auf einem vorhandenen SMB-fähigen NAS-Server

Info über diese Aufgabe

Die folgenden Überlegungen gelten für die Aktivierung der Multiprotokoll-Dateifreigabe auf einem vorhandenen SMB-fähigen NAS-Server:

- Wenn Sie die Multiprotokoll-Dateifreigabe konfigurieren, wird für alle vorhandenen Dateisysteme die native Sicherheitszugriffs-Policy aktiviert. Mit dieser Policy wird die Windows-Sicherheit für NFS- und SMB-Zugriff auf die Dateien verwendet. Diese Policy verwendet für alle Protokolle native Windows-Zugangsdaten und erzwingt für alle Protokolle nur die SMB-ACLs. Darüber hinaus aktualisiert das System automatisch die Eigentumsrechte aller Dateien mit den Unix-UID-Informationen. Der Aktualisierungsprozess kann einige Zeit dauern, die Daten bleiben jedoch zugänglich. Falls erforderlich, können Sie diese Zugriffs-Policy ändern.
- Für Clients mit falschen Zuordnungen wird die Meldung „Zugriff verweigert“ angezeigt, bis die Zuordnungskonfiguration korrigiert wurde.

Schritte

1. Wählen Sie die Optionen **Storage** > **NAS Servers** aus.
2. Wählen Sie den entsprechenden NAS-Server und dann die Registerkarte **Namensservices** aus.
3. Konfigurieren Sie einen der folgenden Verzeichnisdienste:
   - NIS
   - LDAP
   - Lokale Dateien
   - Lokale Dateien und NIS oder LDAP

   Sie können LDAP für die Verwendung von anonymer, einfacher und Kerberos-Authentifizierung konfigurieren. Sie können LDAP auch mit SSL (LDAP Secure) konfigurieren und die Verwendung eines Zertifikats von einer Zertifizierungsstelle bei der Authentifizierung durchsetzen.
4. Wählen Sie die Registerkarte **Nutzerzuordnung** aus und konfigurieren Sie die Suchreihenfolge. Die Verzeichnisdienste, die Sie zuvor konfiguriert haben, können im Drop-down-Menü ausgewählt werden.
5. Legen Sie auf der Registerkarte **Nutzerzuordnung** den Zuordnungsmodus für nicht zugeordnete NutzerInnen fest. Wenn Sie automatische UID-Zuweisungen wünschen, aktivieren Sie die Option **Automatische Zuordnung für nicht zugeordnete Windows-Konten/Nutzer aktivieren**. Eine weitere Möglichkeit ist die Aktivierung der Option **Standardkonto für nicht zugeordnete Nutzer aktivieren**. Geben Sie in diesem Fall die Windows- und Unix-Standardkonten an.

7

Konfigurieren von verteilten Dateisystemen und Widelinks

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Übersicht über verteilte Dateisysteme

Mit Microsoft Distributed File System (DFS) können Sie Dateisysteme (freigegebene Ordner), die sich auf verschiedenen Servern befinden, in einem logischen DFS-Namespace gruppieren. Ein DFS-Namespace ist eine virtuelle Ansicht dieser Dateisysteme, die in einer Verzeichnisstruktur dargestellt wird. Mithilfe von DFS können Sie Dateisysteme in einem logischen DFS-Namespace gruppieren und Ordner, die über mehrere Server verteilt sind, für NutzerInnen so anzeigen, als befänden sie sich an einem einzigen Speicherort im Netzwerk. NutzerInnen können durch den Namespace navigieren, ohne die Servernamen oder die Dateisysteme kennen zu müssen, auf denen die Daten gehostet werden.

Jede DFS-Baumstruktur verfügt über ein Stammziel, d. h. den Hostserver, auf dem der DFS-Service ausgeführt wird und der den Namespace hostet. Ein DFS-Stamm enthält DFS-Links, die zu den Dateisystemen (einer Freigabe und allen darunter liegenden Verzeichnissen im Netzwerk) führen. Die Dateisysteme werden als DFS-Ziele betrachtet. Microsoft bietet sowohl eigenständige als auch domänenbasierte DFS-Stammserver an. Der domänenbasierte DFS-Server speichert die DFS-Hierarchie im AD. Der eigenständige DFS-Stammserver speichert die DFS-Hierarchie lokal. PowerStore bietet die gleiche Funktionalität wie ein eigenständiger Windows 2000- oder Windows Server 2003-DFS-Stammserver.

Konfigurieren von DFS-Stämmen

Sie können in PowerStore DFS-Stämme (Distributed Filesystem Support) auf einer SMB-Freigabe konfigurieren. Führen Sie die folgenden Aufgaben aus, bevor Sie einen DFS-Stamm auf einer SMB-Freigabe konfigurieren:

1. Konfigurieren Sie einen NAS-Server, der SMB unterstützt.
2. Konfigurieren Sie auf dem neu erstellten NAS-Server ein Dateisystem, auf dem der DFS-Stamm erstellt werden soll.

ANMERKUNG: Richten Sie keinen DFS-Stamm auf einem Dateisystemobjekt mit einer Zugriffsüberprüfungs-Policy von Unix ein, da keine der DFS-Linkkomponenten mit Unix-Rechten erstellt wurde.

Es gibt zwei Möglichkeiten, einen DFS-Stamm auf einer SMB-Freigabe zu erstellen:

- Erstellen eines DFS-Stamms mithilfe von dfsutil.exe
- Erstellen eines eigenständigen DFS-Stamms mithilfe von DFS MMC

Weitere Informationen zur Konfiguration von DFS finden Sie in der entsprechenden Dokumentation von Microsoft.

Informationen zu Widelinks

Widelinks machen herkömmliche symbolische Unix-Links in Nutzerdateisystemen für SMB-Clients nutzbar. Wenn ein NFS-Client einen symbolischen Link in einem Dateisystem findet, löst er das Ziel des Links selbst auf. Die Herausforderung liegt darin, dass der Zielpfad des symbolischen Links zwar für NFS-Clients aussagekräftig, für SMB-Clients jedoch höchstwahrscheinlich nicht von Nutzen ist. Diese Herausforderung wird durch die Konfiguration eines lokalen Microsoft Windows-DFS-Stamms auf dem NAS-Server bewältigt, der die Nutzerdateisysteme hostet, die symbolische Unix-Links enthalten, die für SMB-Clients übersetzt werden müssen. Dem DFS-Stamm werden Einträge hinzugefügt, damit der NAS-Server die Unix-Pfade übersetzen kann.

Beispielsweise sieht widelink1 für einen NFS-Client wie folgt aus:

```
$ ls -l widelink1
lrwxr-xr-x 1 cstacey ENG\Domain Users 30 23 JUS 17:33
widelink1 -> /net/nfsserver42/export1/target1
```

$ ls -l widelink1

Daher sollte der Eintrag im DFS-Stammverzeichnis wie folgt lauten:

```
net/nfsserver42/export1/target1 ->
\\nfsserver42\<share-name>\<path-to-target1>
```

8

Troubleshooting einer Multiprotokollkonfiguration

Dieses Kapitel enthält die folgenden Informationen:

Themen:

Servicebefehle für das Troubleshooting einer Multiprotokollkonfiguration

Die folgenden Servicebefehle sind hilfreich für das Troubleshooting von Zugriffsproblemen bei einer Multiprotokollkonfiguration. Weitere Informationen zu den Servicebefehlen finden Sie in *Technische Hinweise zu Servicebefehlen*.

Tabelle 12. Servicebefehle für das Troubleshooting einer Multiprotokollkonfiguration

Anwendungsbeispiel	Servicebefehl
Abrufen von Informationen zur Netzwerkverbindung zu Domain Controllern, zu Zugriffsrechten, Zugangsdaten, Zugriffsprotokollen usw.	`svc_nas_cifssupport --server <NAS_Server_Name>`
Überprüfen der aktuellen Verbindung zwischen dem SMB-Client und dem Domain Controller	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-builtinclient"`
Ausführen interner Konfigurationstests, um die Ursache für mögliche Konfigurations- oder Umgebungsfehler zu ermitteln	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-checkup"`
Troubleshooting der Nutzerzugriffskontrolle durch Auflistung der Nutzerzugangsdaten aus dem SMB-Servercache	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-cred"`
Abrufen der Informationen zu den globalen Policy-Objekten, die auf den SMB-Server angewendet wurden	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-gpo"`
Aktivieren eines Protokolls mit Anmeldeversuchen von NutzerInnen oder Computern	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-logontrace"`
Überprüfen der Authentifizierung eines/einer bestimmten NutzerIn bei einem SMB-Server	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-lsarpc"`
Testen der Netzwerkanmeldung bei einem SMB-Server	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-nltest"`
Anzeigen der Domain-Controller-Informationen für einen bestimmten SMB-Server	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-pdcdump"`
Versuchen, von einem bestimmten SMB-Server aus eine Verbindung zum SMB-Domain-Controller herzustellen	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-pingdc"`
Abrufen der Gruppenmitgliedschaft eines/einer bestimmten NutzerIn vom SMB-Domain-Controller	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-samr"`
Zugreifen auf die sichere Zuordnungsdatenbank, die als Cachemechanismus für die Zuordnung von Windows-SIDs zu Unix-UIDs fungiert	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-secmap"`