



# Verwalten Sie NFS mit der CLI

ONTAP 9

NetApp  
March 30, 2023

# Inhaltsverzeichnis

- Verwalten Sie NFS mit der CLI . . . . . 1
- NFS-Referenzübersicht . . . . . 1
- NAS-Dateizugriff verstehen . . . . . 1
- Daten-Volumes werden in NAS-Namespaces erstellt und gemanagt . . . . . 9
- Konfigurieren Sie Sicherheitsstile . . . . . 14
- Richten Sie den Dateizugriff über NFS ein . . . . . 19
- Managen Sie den Dateizugriff über NFS . . . . . 57
- Unterstützte NFS-Versionen und -Clients . . . . . 109
- Abhängigkeiten von NFS- und SMB-Dateien und Verzeichnissen . . . . . 113

# Verwalten Sie NFS mit der CLI

## NFS-Referenzübersicht

ONTAP umfasst Dateizugriffsfunktionen, die für das NFS-Protokoll verfügbar sind. Sie können einen NFS-Server aktivieren und Volumes oder qtrees exportieren.

Sie führen diese Schritte unter folgenden Umständen aus:

- Sie möchten mehr über die ONTAP NFS-Protokollfunktionen erfahren?
- Sie möchten weniger häufige Konfigurations- und Wartungsaufgaben ausführen, nicht die einfache NFS-Konfiguration.
- Sie möchten die Befehlszeilenschnittstelle (CLI) verwenden, nicht den System Manager oder ein automatisiertes Scripting Tool.

## NAS-Dateizugriff verstehen

### Namespaces und Verbindungspunkte

#### Übersicht über Namespaces und Verbindungspunkte

Ein NAS *Namespace* ist eine logische Gruppierung von Volumes, die an *Junction Points* zu einer einzigen Filesystem-Hierarchie zusammengeschlossen wurden. Ein Client mit ausreichenden Berechtigungen kann auf Dateien im Namespace zugreifen, ohne den Speicherort der Dateien im Storage anzugeben. Junctioned Volumes können sich überall im Cluster befinden.

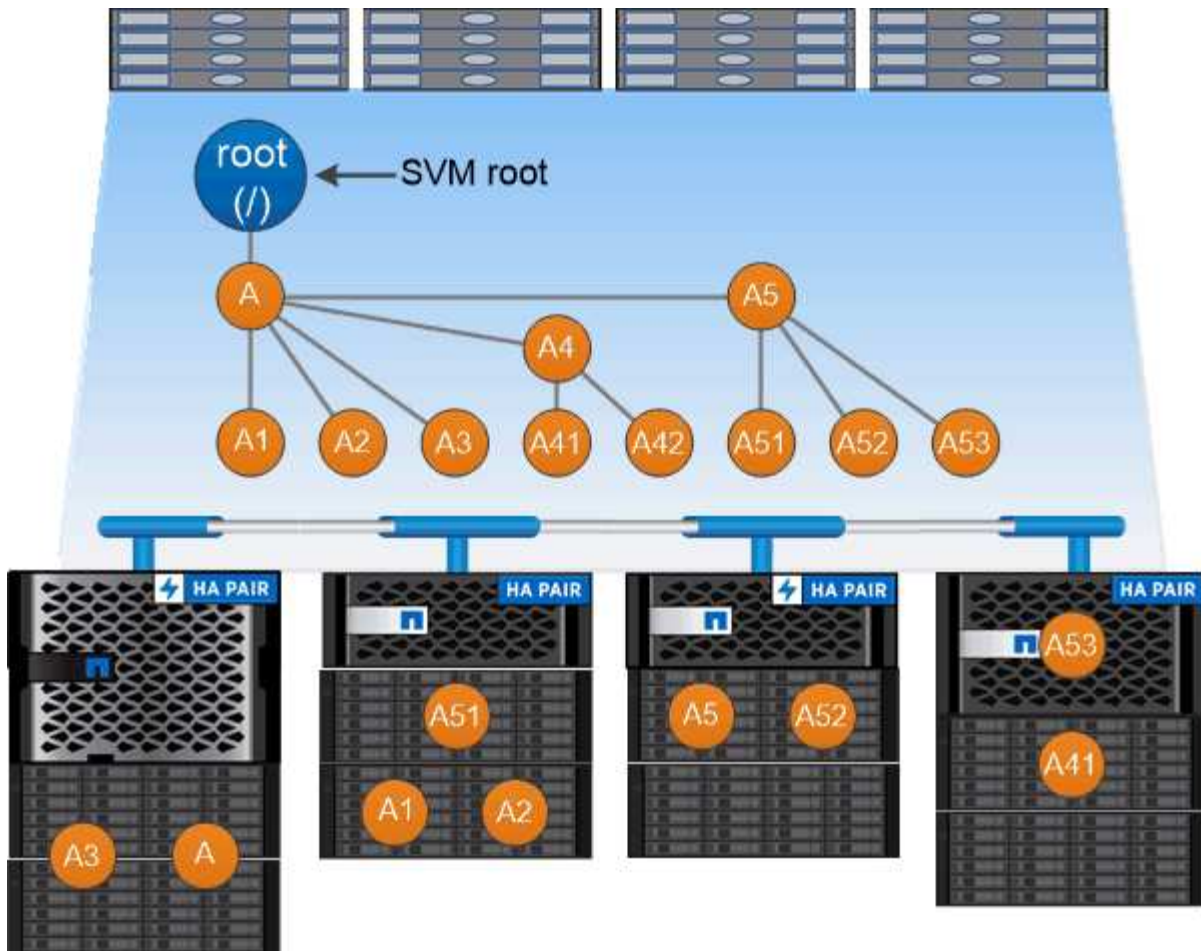
Anstatt jedes Volume mit einer interessanten Datei zu mounten, mounten NAS-Clients einen NFS *Export* oder greifen auf eine SMB *share*. der Export oder Share stellt den gesamten Namespace oder einen Zwischenstandort innerhalb des Namespace dar. Der Client greift nur auf die Volumes zu, die unter seinem Zugriffspunkt gemountet wurden.

Sie können Volumes je nach Bedarf dem Namespace hinzufügen. Sie können Verbindungspunkte direkt unter einer übergeordneten Volume-Verbindung oder in einem Verzeichnis innerhalb eines Volumes erstellen. Möglicherweise ist ein Pfad zu einer Volume-Verbindung für ein Volume mit dem Namen „vol3“ vorhanden /vol1/vol2/vol3, Oder /vol1/dir2/vol3, Oder sogar /dir1/dir2/vol3. Der Pfad wird als *Verbindungspfad bezeichnet*.

Jeder SVM hat einen eindeutigen Namespace. Das SVM-Root-Volume ist der Einstiegspunkt in die Namespace-Hierarchie.



Damit die Daten im Falle eines Node-Ausfalls oder eines Failover weiterhin verfügbar bleiben, sollten Sie eine *Load-Sharing Mirror* Kopie für das SVM Root-Volume erstellen.



*A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.*

### Beispiel

Im folgenden Beispiel wird ein Volume mit dem Namen „home4“ auf der SVM vs1 mit einem Verbindungspfad erstellt /eng/home:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

### Was die typischen NAS Namespace-Architekturen sind

Es gibt verschiedene typische NAS-Namespace-Architekturen, die Sie bei der Erstellung Ihres SVM-Namespaces verwenden können. Sie können die Namespace-Architektur auswählen, die Ihren Business- und Workflow-Anforderungen entspricht.

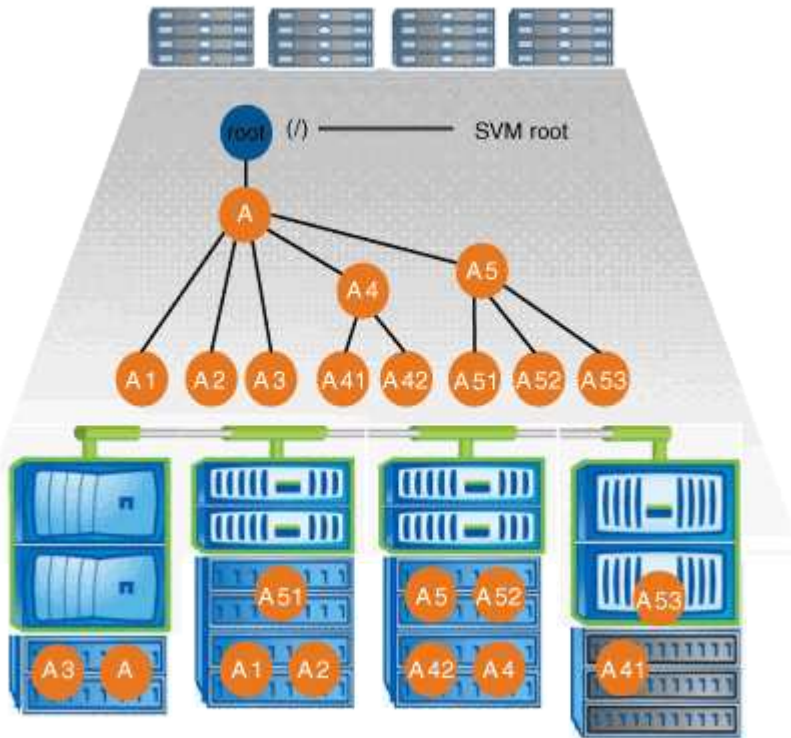
Die Spitze des Namespace ist immer das Root-Volume, das durch einen Schrägstrich (/) dargestellt wird. Die Namespace-Architektur unter der Wurzel lässt sich in drei grundlegende Kategorien einteilen:

- Ein einzelner verzweigter Baum, mit nur einer einzigen Verbindung zum Stammverzeichnis des Namespace

- Mehrere verzweigte Bäume, mit mehreren Verbindungspunkten zum Stammverzeichnis des Namespace
- Mehrere Standalone-Volumes mit jeweils einem separaten Verbindungspunkt zum Root des Namespace

### Namespace mit einem verzweigten Baum

Eine Architektur mit einem einzelnen verzweigten Baum verfügt über einen einzigen Ansatzpunkt zum Root-Verzeichnis des SVM-Namespace. Der einzelne Einfügepunkt kann entweder ein miteinander verbunden Volume oder ein Verzeichnis unter dem Root sein. Alle anderen Volumes werden an Verbindungspunkten unter dem einzelnen Einfügepunkt (ein Volume oder ein Verzeichnis) gemountet.

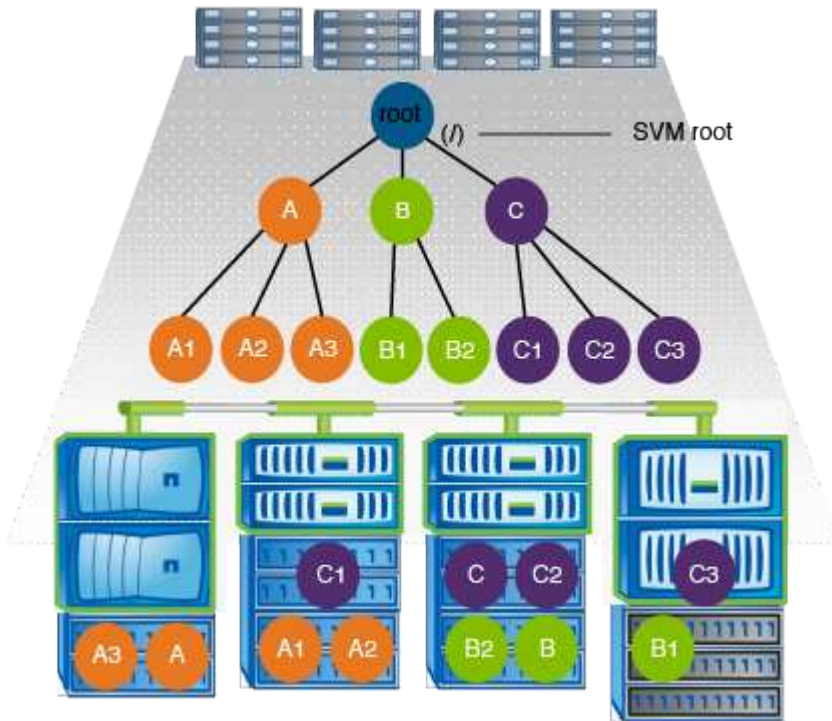


Eine typische Konfiguration für Volume-Verbindungen mit der oben genannten Namespace-Architektur kann beispielsweise wie die folgende Konfiguration aussehen: Alle Volumes werden unter dem einzelnen Einfügepunkt verbunden, ein Verzeichnis mit dem Namen „data“:

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	corp1	true	/data/dir1/corp1	RW_volume
vs1	corp2	true	/data/dir1/corp2	RW_volume
vs1	data1	true	/data/data1	RW_volume
vs1	eng1	true	/data/data1/eng1	RW_volume
vs1	eng2	true	/data/data1/eng2	RW_volume
vs1	sales	true	/data/data1/sales	RW_volume
vs1	vol1	true	/data/vol1	RW_volume
vs1	vol2	true	/data/vol2	RW_volume
vs1	vol3	true	/data/vol3	RW_volume
vs1	vs1_root	-	/	-

## Namespace mit mehreren verzweigten Bäumen

Eine Architektur mit mehreren verzweigten Bäumen verfügt über mehrere Ansatzpunkte zum Root-Verzeichnis des SVM-Namespaces. Die Einfügekpunkte können entweder Volumes oder Verzeichnisse unter dem Root umfassen. Alle anderen Volumes werden an Verbindungspunkten unter den Einfügekpunkten (Volumes oder Verzeichnisse) gemountet.

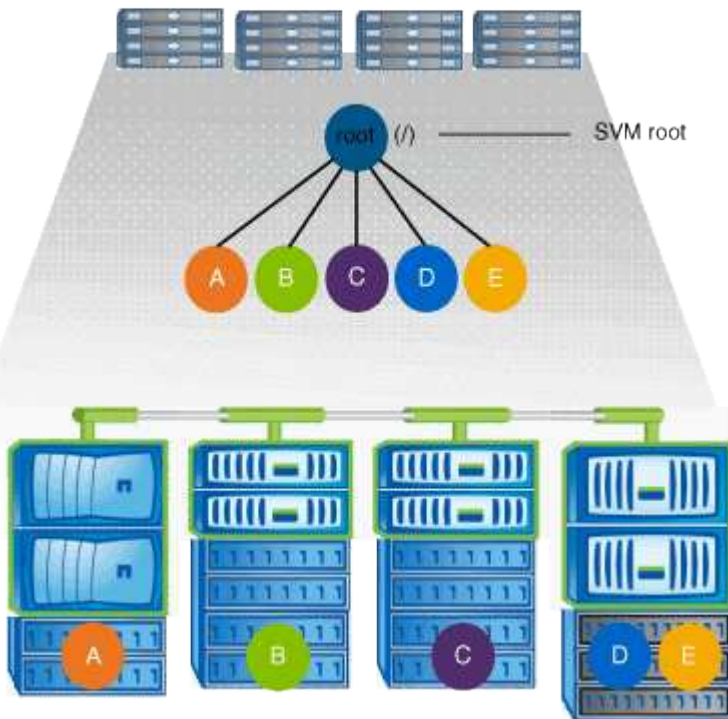


Beispielsweise könnte eine typische Konfiguration für eine Volume-Verbindungsstelle mit der oben genannten Namespace-Architektur wie die folgende Konfiguration aussehen: Es gibt drei Ansatzpunkte für das Root-Volume der SVM. Zwei Einfügekpunkte sind Verzeichnisse mit den Namen "data" und "projects". Ein Einfügekmarkt ist ein mit „Audit“ in Verbindung gefügter Datenträger:

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	audit	true	/audit	RW_volume
vs1	audit_logs1	true	/audit/logs1	RW_volume
vs1	audit_logs2	true	/audit/logs2	RW_volume
vs1	audit_logs3	true	/audit/logs3	RW_volume
vs1	eng	true	/data/eng	RW_volume
vs1	mktg1	true	/data/mktg1	RW_volume
vs1	mktg2	true	/data/mktg2	RW_volume
vs1	project1	true	/projects/project1	RW_volume
vs1	project2	true	/projects/project2	RW_volume
vs1	vs1_root	-	/	-

## Namespace mit mehreren Standalone-Volumes

In einer Architektur mit Standalone Volumes verfügt jedes Volume über einen Ansatzpunkt zum Root-Verzeichnis des SVM Namespace. Das Volume wird jedoch nicht unter einem anderen Volume verbunden. Jedes Volume verfügt über einen eindeutigen Pfad, der entweder direkt unter dem Stammverzeichnis verbunden ist oder unter einem Verzeichnis unter dem Stammverzeichnis verbunden wird.



Beispielsweise kann eine typische Konfiguration für eine Volume-Verbindungsstelle mit der oben genannten Namespace-Architektur wie die folgende Konfiguration aussehen: Es gibt fünf Ansatzpunkte für das Root-Volume der SVM, wobei jeder Einfügepunkt einen Pfad zu einem Volume darstellt.

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	eng	true	/eng	RW_volume
vs1	mktg	true	/vol/mktg	RW_volume
vs1	project1	true	/project1	RW_volume
vs1	project2	true	/project2	RW_volume
vs1	sales	true	/sales	RW_volume
vs1	vs1_root	-	/	-

## Wie ONTAP den Zugriff auf Dateien steuert

### Wie ONTAP den Zugriff auf Dateien steuert, Übersicht

ONTAP steuert den Zugriff auf Dateien gemäß den von Ihnen angegebenen Authentifizierungs- und dateibasierten Einschränkungen.



Wenn ein Client eine Verbindung zum Storage-System herstellt, um auf Dateien zuzugreifen, muss ONTAP zwei Aufgaben erledigen:

- Authentifizierung

ONTAP muss den Client authentifizieren, indem die Identität mit einer vertrauenswürdigen Quelle überprüft wird. Darüber hinaus ist der Authentifizierungstyp des Clients eine Methode, mit der bestimmt werden kann, ob ein Client beim Konfigurieren von Exportrichtlinien auf Daten zugreifen kann (optional für CIFS).

- Autorisierung

ONTAP muss den Benutzer autorisieren, indem er die Anmeldeinformationen des Benutzers mit den in der Datei oder dem Verzeichnis konfigurierten Berechtigungen vergleicht und bestimmt, welche Art von Zugriff, falls vorhanden, zur Verfügung stellt.

Um die Kontrolle über den Dateizugriff ordnungsgemäß zu managen, muss ONTAP mit externen Services wie NIS, LDAP und Active Directory Servern kommunizieren. Um ein Storage-System für Dateizugriff über CIFS oder NFS zu konfigurieren, müssen Sie die entsprechenden Services je nach Ihrer Umgebung in ONTAP einrichten.

### **Authentifizierungsbasierte Einschränkungen**

Bei authentifizierungsbasierten Einschränkungen kann festgelegt werden, welche Client-Machines und welche Benutzer eine Verbindung zur Storage Virtual Machine (SVM) herstellen können.

ONTAP unterstützt Kerberos-Authentisierung von UNIX und Windows Servern.

### **Dateibasierte Einschränkungen**

ONTAP bewertet drei Sicherheitsstufen, um zu ermitteln, ob eine Einheit autorisiert ist, eine angeforderte Aktion für Dateien und Verzeichnisse, die sich auf einer SVM befinden, durchzuführen. Der Zugriff wird durch die effektiven Berechtigungen nach Auswertung der drei Sicherheitsstufen bestimmt.

Jedes Storage-Objekt kann bis zu drei Typen von Sicherheitsebenen enthalten:

- Exportsicherheit (NFS) und Freigabe (SMB)

Die Export- und Share-Sicherheit gilt für den Client-Zugriff auf einen bestimmten NFS-Export oder eine bestimmte SMB-Freigabe. Benutzer mit Administratorrechten können die Sicherheit von Export- und Share-Ebene über SMB- und NFS-Clients managen.

- Sicherheit von Datei- und Verzeichnissebenen auf Storage-Ebene

Die Sicherheit der Storage-Level Access Guard-Lösung gilt für den Zugriff von SMB- und NFS-Clients auf SVM Volumes. Es werden nur NTFS-Zugriffsberechtigungen unterstützt. Damit ONTAP auf UNIX-Benutzern Sicherheitsüberprüfungen für den Zugriff auf Daten auf Volumes durchführen kann, für die der Storage-Level Access Guard angewendet wurde, muss der UNIX-Benutzer einem Windows-Benutzer auf der SVM, der auch Eigentümer des Volumes ist, zuordnen.





Wenn Sie die Sicherheitseinstellungen einer Datei oder eines Verzeichnisses von einem NFS- oder SMB-Client aus anzeigen, wird die Sicherheit des Access Guard auf Storage-Ebene nicht angezeigt. Die Sicherheit des Access Guard auf Storage-Ebene kann nicht von einem Client entzogen werden, selbst wenn ein System-Administrator (Windows oder UNIX) dies durchführt.

- Native Sicherheit auf Dateiebene durch NTFS, UNIX und NFSv4

Die Datei oder das Verzeichnis, die das Storage-Objekt repräsentieren, enthält native Sicherheit auf Dateiebene. Sie können die Sicherheit auf Dateiebene von einem Client aus festlegen. Die Dateiberechtigungen haben unabhängig davon, ob SMB oder NFS für den Zugriff auf die Daten verwendet wird.

## Wie ONTAP die NFS-Client-Authentifizierung verarbeitet

### Überblick über die Handhabung der NFS-Client-Authentifizierung durch ONTAP

NFS-Clients müssen ordnungsgemäß authentifiziert werden, bevor sie auf Daten auf der SVM zugreifen können. ONTAP authentifiziert die Clients, indem ihre UNIX-Anmeldeinformationen auf die von Ihnen konfigurierten Namensdienste überprüft werden.

Wenn ein NFS-Client eine Verbindung zur SVM herstellt, erhält ONTAP die UNIX-Anmeldedaten für den Benutzer, indem er abhängig von der Name-Services-Konfiguration der SVM andere Name-Services überprüft. ONTAP kann die Anmeldedaten für lokale UNIX Accounts, NIS-Domänen und LDAP-Domänen prüfen. Mindestens einer von ihnen muss so konfiguriert werden, dass ONTAP den Benutzer erfolgreich authentifizieren kann. Sie können mehrere Namensdienste und die Reihenfolge angeben, in der ONTAP sie durchsucht.

In einer reinen NFS-Umgebung mit UNIX-Volume-Sicherheitsstil genügt diese Konfiguration zur Authentifizierung und Bereitstellung des richtigen Dateizugriffs für einen Benutzer, der sich von einem NFS-Client aus verbinden lässt.

Bei Verwendung von Sicherheitsstilen für gemischte, NTFS- oder einheitliche Volumes muss ONTAP einen SMB-Benutzernamen für den UNIX-Benutzer zur Authentifizierung mit einem Windows Domain Controller erhalten. Dies kann entweder durch die Zuordnung einzelner Benutzer mithilfe lokaler UNIX-Konten oder LDAP-Domänen oder durch die Verwendung eines standardmäßigen SMB-Benutzers erfolgen. Sie können festlegen, nach welchen Namens-Services ONTAP in welcher Reihenfolge gesucht wird, oder einen standardmäßigen SMB-Benutzer angeben.

### Verwendung von Name Services durch ONTAP

ONTAP bezieht Informationen zu Benutzern und Clients mithilfe von Name Services. ONTAP verwendet diese Informationen, um Benutzer zu authentifizieren, die auf Daten auf dem Storage-System zugreifen, und um Benutzeranmeldeinformationen in einer heterogenen Umgebung zuzuordnen.

Wenn Sie das Speichersystem konfigurieren, müssen Sie angeben, welche Namensdienste ONTAP zum Abrufen von Benutzeranmeldeinformationen zur Authentifizierung verwenden soll. ONTAP unterstützt folgende Namensdienste:

- Lokale Benutzer (Datei)

- Externe NIS-Domänen (NIS)
- Externe LDAP-Domänen (LDAP)

Sie verwenden das `vserver services name-service ns-switch` Produktfamilie konfiguriert SVMs mit den Quellen für die Suche nach Netzwerkinformationen und der Reihenfolge, in der sie durchsucht werden können. Diese Befehle stellen die gleiche Funktionalität des bereit `/etc/nsswitch.conf` File auf UNIX Systemen.

Wenn ein NFS-Client eine Verbindung zur SVM herstellt, überprüft ONTAP die angegebenen Namensservices, um die UNIX-Anmeldedaten für den Benutzer abzurufen. Wenn Namensdienste richtig konfiguriert sind und ONTAP die UNIX-Anmeldedaten erhalten kann, authentifiziert ONTAP den Benutzer erfolgreich.

In einer Umgebung mit unterschiedlichen Sicherheitsstilen muss ONTAP möglicherweise Benutzeranmeldeinformationen zuordnen. Sie müssen Name-Services entsprechend für Ihre Umgebung konfigurieren, damit ONTAP die Benutzeranmeldeinformationen ordnungsgemäß zuordnen kann.

ONTAP verwendet außerdem Namensdienste für die Authentifizierung von SVM-Administratorkonten. Dies müssen Sie beachten, wenn Sie den Namespace-Switch konfigurieren oder ändern, um zu vermeiden, dass die Authentifizierung für SVM-Administratorkonten versehentlich deaktiviert wird. Weitere Informationen zu SVM-Verwaltungsbenutzern finden Sie unter ["Administratorauthentifizierung und RBAC"](#).

### **Wie ONTAP über NFS-Clients SMB-Dateizugriff gewährt**

ONTAP verwendet die Sicherheitssemantik des Windows NT File System (NTFS), um zu ermitteln, ob ein UNIX-Benutzer auf einem NFS-Client Zugriff auf eine Datei mit NTFS-Berechtigungen hat.

ONTAP konvertiert dazu die UNIX-Benutzer-ID (UID) des Benutzers in eine SMB-Berechtigung und überprüft anschließend mit den SMB-Anmeldeinformationen, ob der Benutzer über Zugriffsrechte auf die Datei verfügt. Eine SMB-Berechtigung besteht aus einer primären Sicherheits-ID (SID), in der Regel dem Windows-Benutzernamen des Benutzers und einer oder mehreren Gruppen-SIDs, die den Windows-Gruppen entsprechen, deren Mitglied der Benutzer ist.

Die Zeit, die ONTAP aus der Konvertierung der UNIX UID in eine SMB-Zugangsdaten zieht, kann von Millisekunden in hunderte von Millisekunden betragen, da der Prozess die Kontaktaufnahme mit einem Domain Controller erfordert. ONTAP ordnet die UID den SMB-Anmeldedaten zu und gibt die Zuordnung in einen Anmeldeinformationscache ein, um die durch die Konvertierung verursachte Verifizierungszeit zu reduzieren.

### **Funktionsweise des NFS-Caches für Zugangsdaten**

Wenn ein NFS-Benutzer Zugriff auf NFS-Exporte im Storage-System anfordert, muss ONTAP zur Authentifizierung des Benutzers seine Zugangsdaten entweder von externen Name Servern oder aus lokalen Dateien abrufen. ONTAP speichert diese Zugangsdaten dann in einem internen Cache für Zugangsdaten, um sie später verwenden zu können. Wenn die Funktionsweise der NFS-Caches für Zugangsdaten klar ist, können auch potenzielle Performance- und Zugriffsprobleme vermieden werden.

Ohne den Cache für Zugangsdaten müsste ONTAP jedes Mal, wenn ein NFS-Benutzer Zugriff angefordert hätte, Nameservices abfragen. Auf einem überlasteten Storage-System, auf das viele Benutzer zugreifen, kann dies schnell zu ernsthaften Performance-Problemen führen, was zu unerwünschten Verzögerungen oder gar zum NFS-Client-Zugriff führt.

Im Cache für Zugangsdaten ruft ONTAP die Zugangsdaten ab und speichert sie anschließend für einen vorab festgelegten Zeitraum für den schnellen und einfachen Zugriff, sollte der NFS-Client eine weitere Anforderung senden. Diese Methode bietet die folgenden Vorteile:

- Sie vereinfacht die Belastung des Storage-Systems durch die Verarbeitung von weniger Anfragen an externe Name Server (z. B. NIS oder LDAP).
- Dies vereinfacht die Belastung von externen Name Servern, indem weniger Anfragen an sie gesendet werden.
- Es beschleunigt den Benutzerzugriff, da die Wartezeit für den Erhalt von Anmeldeinformationen von externen Quellen entfällt, bevor der Benutzer authentifiziert werden kann.

ONTAP speichert sowohl positive als auch negative Anmeldeinformationen im Cache für Zugangsdaten. Positive Anmeldeinformationen bedeuten, dass der Benutzer authentifiziert wurde und Zugriff gewährt wurde. Negative Anmeldeinformationen bedeuten, dass der Benutzer nicht authentifiziert wurde und der Zugriff verweigert wurde.

Standardmäßig speichert ONTAP 24 Stunden lang positive Anmeldeinformationen. Das heißt, nach der erstmaligen Authentifizierung eines Benutzers verwendet ONTAP die im Cache gespeicherten Zugangsdaten für alle Zugriffsanfragen dieses Benutzers für 24 Stunden. Wenn der Benutzer nach 24 Stunden Zugriff anfordert, beginnt der Zyklus: ONTAP entnimmt die zwischengespeicherten Anmeldeinformationen und erhält die Anmeldeinformationen erneut aus der entsprechenden Namensdienstquelle. Wenn sich die Anmeldeinformationen auf dem Namensserver während der letzten 24 Stunden geändert haben, speichert ONTAP die aktualisierten Anmeldeinformationen für die nächsten 24 Stunden im Cache.

Standardmäßig speichert ONTAP negative Zugangsdaten für zwei Stunden. Das heißt, nachdem ONTAP den Zugriff zunächst einem Benutzer verweigert hat, werden alle Zugriffsanfragen des Benutzers für zwei Stunden lang verweigert. Wenn der Benutzer nach 2 Stunden Zugriff anfordert, beginnt der Zyklus: ONTAP erhält die Anmeldeinformationen erneut aus der entsprechenden Namensdienstquelle. Wenn sich die Anmeldeinformationen auf dem Namensserver in den letzten zwei Stunden geändert haben, speichert ONTAP die aktualisierten Anmeldeinformationen für die nächsten zwei Stunden im Cache.

## Daten-Volumes werden in NAS-Namespaces erstellt und gemanagt

### Erstellung von Daten-Volumes mit festgelegten Verbindungspunkten

Sie können den Verbindungspunkt bei der Erstellung eines Daten-Volumes angeben. Das resultierende Volume wird automatisch am Verbindungspunkt gemountet und ist für den NAS-Zugriff sofort konfiguriert.

#### Was Sie benötigen

Das Aggregat, in dem Sie das Volume erstellen möchten, muss bereits vorhanden sein.



Folgende Zeichen können nicht im Verbindungspfad verwendet werden: \* # " > < ? \

Darüber hinaus darf die Länge des Verbindungspfades nicht mehr als 255 Zeichen umfassen.

#### Schritte

1. Volume mit einem Verbindungspunkt erstellen:

```
volume create -vserver vserver_name -volume volume_name -aggregate
```

```
aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed} -junction-path junction_path
```

Der Verbindungspfad muss mit dem Root (/) beginnen und kann sowohl Verzeichnisse als auch Volumes enthalten. Der Verbindungspfad muss den Namen des Volumes nicht enthalten. Verbindungspfade sind unabhängig vom Volume-Namen.

Die Angabe eines Volume-Sicherheitsstils ist optional. Wenn Sie keinen Sicherheitsstil angeben, erstellt ONTAP das Volume mit dem gleichen Sicherheitstyp, der auf das Root-Volume der SVM (Storage Virtual Machine) angewendet wird. Der Sicherheitsstil des Root-Volumes ist jedoch möglicherweise nicht der Sicherheitsstil, den Sie auf das von Ihnen erstellte Datenvolumen anwenden möchten. Es wird empfohlen, beim Erstellen des Volumes den Sicherheitsstil festzulegen, um Probleme mit dem Dateizugriff zu minimieren, die sich nur schwer beheben lassen.

Die Groß-/Kleinschreibung des Verbindungspfads wird nicht berücksichtigt. /ENG ist das gleiche wie /eng. Wenn Sie eine CIFS-Freigabe erstellen, behandelt Windows den Verbindungspfad so, als ob die Groß-/Kleinschreibung beachtet wird. Beispiel: Wenn die Verbindung lautet /ENG, Der Pfad einer SMB-Freigabe muss mit beginnen /ENG, Nicht /eng.

Es gibt viele optionale Parameter, mit denen Sie ein Daten-Volume anpassen können. Weitere Informationen dazu finden Sie auf den man-Pages für die `volume create` Befehl.

2. Vergewissern Sie sich, dass das Volume mit dem gewünschten Verbindungspunkt erstellt wurde:

```
volume show -vserver vs1 -volume volume_name -junction
```

### Beispiel

Im folgenden Beispiel wird ein Volume mit dem Namen „home4“ auf der SVM vs1 mit einem Verbindungspfad erstellt /eng/home:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	home4	true	/eng/home	RW_volume

## Erstellung von Daten-Volumes ohne Angabe von Verbindungspunkten

Sie können ein Daten-Volume erstellen, ohne einen Verbindungspunkt anzugeben. Das resultierende Volume wird nicht automatisch gemountet und steht für den NAS-Zugriff nicht zur Verfügung. Sie müssen das Volume mounten, bevor Sie SMB-Freigaben oder NFS-Exporte für dieses Volume konfigurieren können.

### Was Sie benötigen

Das Aggregat, in dem Sie das Volume erstellen möchten, muss bereits vorhanden sein.

## Schritte

1. Um das Volume ohne Verbindungspunkt zu erstellen, verwenden Sie folgenden Befehl:

```
volume create -vserver vserver_name -volume volume_name -aggregate
aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed}
```

Die Angabe eines Volume-Sicherheitsstils ist optional. Wenn Sie keinen Sicherheitsstil angeben, erstellt ONTAP das Volume mit dem gleichen Sicherheitstyp, der auf das Root-Volume der SVM (Storage Virtual Machine) angewendet wird. Der Sicherheitsstil des Root-Volumes ist jedoch möglicherweise nicht der Sicherheitsstil, den Sie auf das Datenvolumen anwenden möchten. Es wird empfohlen, beim Erstellen des Volumes den Sicherheitsstil festzulegen, um Probleme mit dem Dateizugriff zu minimieren, die sich nur schwer beheben lassen.

Es gibt viele optionale Parameter, mit denen Sie ein Daten-Volume anpassen können. Weitere Informationen dazu finden Sie auf den man-Pages für die `volume create` Befehl.

2. Vergewissern Sie sich, dass das Volume ohne Verbindungspunkt erstellt wurde:

```
volume show -vserver vserver_name -volume volume_name -junction
```

## Beispiel

Im folgenden Beispiel wird ein Volume mit dem Namen „sales“ auf der SVM vs1 erstellt, das nicht an einem Verbindungspunkt gemountet ist:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	data	true	/data	RW_volume
vs1	home4	true	/eng/home	RW_volume
vs1	vs1_root	-	/	-
vs1	sales	-	-	-

## Mounten oder Unmounten vorhandener Volumes im NAS Namespace

Ein Volume muss auf dem NAS Namespace gemountet werden, bevor Sie den NAS-Client-Zugriff auf Daten in den Storage Virtual Machine (SVM)-Volumes konfigurieren können. Sie können ein Volume an einen Verbindungspunkt mounten, wenn es derzeit nicht angehängt ist. Sie können auch die Bereitstellung von Volumes aufheben.

### Über diese Aufgabe

Wenn Sie ein Volume unmounten und offline schalten, sind alle Daten innerhalb des Verbindungspunkts, einschließlich Daten in Volumes mit Verbindungspunkten im Namespace des abgehängt Volumes, für NAS-

Clients nicht verfügbar.



Um den NAS-Client-Zugriff auf ein Volume zu beenden, reicht es nicht aus, das Volume einfach zu entmounten. Sie müssen das Volume offline schalten oder andere Schritte Unternehmen, um sicherzustellen, dass Client-seitige Datei-Handle-Caches nicht validiert werden. Weitere Informationen finden Sie im folgenden Knowledge Base-Artikel:

["NFSv3-Clients haben nach Entfernen aus dem Namespace in ONTAP noch Zugriff auf ein Volume"](#)

Wenn Sie ein Volume unmounten und offline schalten, gehen die Daten innerhalb des Volume nicht verloren. Zusätzlich bleiben vorhandene Volume-Exportrichtlinien und SMB-Freigaben, die auf dem Volume oder auf Verzeichnissen und Verbindungspunkten innerhalb des nicht abgehängt Volume erstellt wurden, erhalten. Wenn Sie das nicht abgesetzte Volume erneut mounten, können NAS-Clients mithilfe vorhandener Exportrichtlinien und SMB-Freigaben auf die Daten im Volume zugreifen.

### Schritte

1. Führen Sie die gewünschte Aktion aus:

Ihr Ziel ist	Geben Sie die Befehle ein...
Mounten Sie ein Volume	<pre>volume mount -vserver svm_name -volume volume_name -junction-path junction_path</pre>
Unmount eines Volumes aufheben	<pre>volume unmount -vserver svm_name -volume volume_name volume offline -vserver svm_name -volume volume_name</pre>

2. Vergewissern Sie sich, dass sich das Volume im gewünschten Mount-Status befindet:

```
volume show -vserver vserver_name -volume volume_name -fields state,junction-path,junction-active
```

### Beispiele

Das folgende Beispiel hängt ein Volume mit dem Namen „sales“ auf der SVM vs1 bis zum Verbindungspunkt ab /sales:

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver    volume    state    junction-path    junction-active
-----
vs1        data      online   /data            true
vs1        home4     online   /eng/home        true
vs1        sales     online   /sales           true
```

Im folgenden Beispiel wird ein Volume mit dem Namen „data“ auf SVM vs1 abgehängt und offline gesetzt:

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver    volume      state      junction-path  junction-active
-----
vs1        data        offline    -              -
vs1        home4       online     /eng/home      true
vs1        sales       online     /sales         true
```

## Anzeige von Informationen zu Volume Mount und Verbindungspunkten

Sie können Informationen zu gemounteten Volumes für Storage Virtual Machines (SVMs) und den Verbindungspunkten für die Volumes anzeigen. Sie können auch festlegen, welche Volumes nicht an einem Verbindungspunkt angehängt sind. Anhand dieser Informationen können Sie Ihren SVM-Namespace verstehen und managen.

### Schritt

1. Führen Sie die gewünschte Aktion aus:

Sie möchten Folgendes anzeigen:	Geben Sie den Befehl ein...
Zusammenfassende Informationen über gemountete und abgehängt Volumes auf der SVM	<code>volume show -vserver vserver_name -junction</code>
Detaillierte Informationen zu gemounteten und abgehängt Volumes auf der SVM	<code>volume show -vserver vserver_name -volume volume_name -instance</code>
Spezifische Informationen über gemountete und abgehängt Volumes auf der SVM	<p>a. Bei Bedarf können Sie gültige Felder für das anzeigen <code>-fields</code> Parameter mit dem folgenden Befehl: <code>volume show -fields ?</code></p> <p>b. Zeigen Sie die gewünschten Informationen mit dem an <code>-fields</code> Parameter: <code>volume show -vserver vserver_name -fields fieldname,...</code></p>

### Beispiele

Im folgenden Beispiel werden eine Zusammenfassung der gemounteten und nicht abgehängt Volumes auf SVM vs1 angezeigt:



```
cluster1::> volume show -vserver vs1 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	data	true	/data	RW_volume
vs1	home4	true	/eng/home	RW_volume
vs1	vs1_root	-	/	-
vs1	sales	true	/sales	RW_volume

Im folgenden Beispiel werden Informationen zu den angegebenen Feldern für Volumes in SVM vs2 angezeigt:

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume aggregate size state type security-style junction-path
junction-parent node
-----
```

vserver	volume	aggregate	size	state	type	security-style	junction-path	junction-parent	node
vs2	data1	aggr3	2GB	online	RW	unix	-	-	node3
vs2	data2	aggr3	1GB	online	RW	ntfs	/data2	-	node3
vs2	data2_1	aggr3	8GB	online	RW	ntfs	/data2/d2_1	-	node3
vs2	data2_2	aggr3	8GB	online	RW	ntfs	/data2/d2_2	-	node3
vs2	pubs	aggr1	1GB	online	RW	unix	/publications	-	node1
vs2	images	aggr3	2TB	online	RW	ntfs	/images	-	node3
vs2	logs	aggr1	1GB	online	RW	unix	/logs	-	node1
vs2	vs2_root	aggr3	1GB	online	RW	ntfs	/	-	node3

## Konfigurieren Sie Sicherheitsstile

### Einfluss der Sicherheitsstile auf den Datenzugriff

#### Was die Sicherheitsstile und ihre Auswirkungen sind

Es gibt vier verschiedene Sicherheitsarten: UNIX, NTFS, gemischt und vereinheitlicht. Jeder Sicherheitsstil hat unterschiedliche Auswirkungen auf den Umgang mit Berechtigungen für Daten. Sie müssen die verschiedenen Effekte verstehen, um

sicherzustellen, dass Sie den entsprechenden Sicherheitsstil für Ihre Zwecke auswählen.

Es ist wichtig zu verstehen, dass Sicherheitsstile nicht bestimmen, welche Client-Typen auf Daten zugreifen können oder nicht. Sicherheitsstile bestimmen nur die Art der Berechtigungen, die ONTAP zur Kontrolle des Datenzugriffs verwendet, und welche Clienttypen diese Berechtigungen ändern können.

Wenn ein Volume beispielsweise UNIX-Sicherheitsstil verwendet, können SMB-Clients aufgrund der Multiprotokollart von ONTAP weiterhin auf Daten zugreifen (sofern sie sich ordnungsgemäß authentifizieren und autorisieren). ONTAP verwendet jedoch UNIX-Berechtigungen, die nur UNIX-Clients mit nativen Tools ändern können.

Sicherheitsstil	Clients, die Berechtigungen ändern können	Berechtigungen, die Clients verwenden können	Dadurch effektiver Sicherheitsstil	Clients, die auf Dateien zugreifen können
Unix	NFS	Bits im NFSv3 Modus	Unix	NFS und SMB
		NFSv4.x ACLs		
NTFS	SMB	NTFS-ACLs	NTFS	
Gemischt	NFS oder SMB	Bits im NFSv3 Modus	UNIX	
		NFSv4.ACLs		
		NTFS-ACLs	NTFS	
Unified (nur für Infinite Volumes, in ONTAP 9.4 und älteren Versionen.)	NFS oder SMB	Bits im NFSv3 Modus	Unix	
		NFSv4.1 ACLs		
		NTFS-ACLs	NTFS	

FlexVol Volumes unterstützen UNIX, NTFS und verschiedene Sicherheitsstile. Wenn der Sicherheitsstil gemischt oder vereinheitlicht ist, hängen die effektiven Berechtigungen vom Clienttyp ab, der die Berechtigungen zuletzt geändert hat, da Benutzer den Sicherheitsstil auf individueller Basis festlegen. Wenn der letzte Client, der die Berechtigungen geändert hat, ein NFSv3-Client war, sind die Berechtigungen UNIX NFSv3-Modus-Bits. Wenn der letzte Client ein NFSv4-Client war, sind die Berechtigungen NFSv4 ACLs. Wenn der letzte Client ein SMB-Client war, sind die Berechtigungen Windows NTFS ACLs.

Der Unified Security-Stil ist nur mit Infinite Volumes verfügbar, die in ONTAP 9.5 und neueren Versionen nicht mehr unterstützt werden. Weitere Informationen finden Sie unter [Das Management von FlexGroup Volumes – Überblick](#).

Ab ONTAP 9.2 beginnt der `show-effective-permissions` Parameter für das `vserver security file-directory` Mit Befehl können Sie effektive Berechtigungen anzeigen, die einem Windows- oder UNIX-Benutzer im angegebenen Datei- oder Ordnerpfad gewährt werden. Darüber hinaus der optionale Parameter `-share-name` Ermöglicht Ihnen die Anzeige der effektiven Freigabeberechtigung.



ONTAP legt zunächst einige Standarddateiberechtigungen fest. Standardmäßig ist der effektive Sicherheitsstil auf allen Daten in UNIX-, gemischten und Unified Security-Volumes UNIX und der effektive Berechtigungstyp UNIX Mode Bits (0755, sofern nicht anders angegeben), bis er von einem Client gemäß dem Standardsicherheitsstil konfiguriert wird. Standardmäßig ist der effektive Sicherheitsstil auf allen Daten in NTFS-Sicherheitsstil-Volumes NTFS und hat eine ACL, die allen die vollständige Kontrolle erlaubt.

## Wo und wann Sicherheitsstile eingestellt werden sollen

Sicherheitsstile können auf FlexVol Volumes (Root-Volumes oder Daten-Volumes) und qtrees festgelegt werden. Sicherheitsstile können zum Zeitpunkt der Erstellung manuell eingestellt, automatisch geerbt oder zu einem späteren Zeitpunkt geändert werden.

## Entscheiden Sie, welchen Sicherheitsstil auf SVMs verwendet werden soll

Um zu entscheiden, welchen Sicherheitsstil auf einem Volume verwendet werden soll, sollten Sie zwei Faktoren berücksichtigen. Der Hauptfaktor ist die Art des Administrators, der das Dateisystem verwaltet. Sekundär ist die Art des Benutzers oder Service, der auf die Daten des Volume zugreift.

Wenn Sie den Sicherheitsstil auf einem Volume konfigurieren, sollten Sie die Anforderungen Ihrer Umgebung berücksichtigen, um sicherzustellen, dass Sie den besten Sicherheitsstil wählen und Probleme beim Management von Berechtigungen vermeiden. Die folgenden Überlegungen helfen Ihnen bei der Auswahl:

Sicherheitsstil	Wählen Sie aus, ob...
UNIX	<ul style="list-style-type: none"><li>• Das Dateisystem wird von einem UNIX-Administrator verwaltet.</li><li>• Die Mehrheit der Benutzer sind NFS Clients.</li><li>• Eine Anwendung, die auf die Daten zugreift, verwendet einen UNIX-Benutzer als Dienstkonto.</li></ul>
NTFS	<ul style="list-style-type: none"><li>• Das Dateisystem wird von einem Windows-Administrator verwaltet.</li><li>• Die Mehrheit der Benutzer sind SMB-Clients.</li><li>• Eine Anwendung, die auf die Daten zugreift, verwendet einen Windows-Benutzer als Dienstkonto.</li></ul>
Gemischt	<ul style="list-style-type: none"><li>• Das Filesystem wird sowohl von UNIX- als auch von Windows-Administratoren gemanagt, und die Benutzer bestehen sowohl aus NFS- als auch SMB-Clients.</li></ul>

## Wie funktioniert die Vererbung des Sicherheitsstils

Wenn Sie beim Erstellen eines neuen FlexVol Volumes oder eines qtree nicht den Sicherheitsstil festlegen, übernimmt dieser seinen Sicherheitsstil auf unterschiedliche Weise.

Sicherheitsstile werden auf folgende Weise vererbt:

- Ein FlexVol Volume erbt den Sicherheitsstil des Root-Volumes seiner enthaltenen SVM.

- Ein qtree übernimmt den Sicherheitsstil seines enthaltenen FlexVol Volume.
- Eine Datei oder ein Verzeichnis erbt den Sicherheitsstil, den sie FlexVol Volume oder qtree enthält.

### **Wie ONTAP UNIX-Berechtigungen bewahrt**

Wenn Dateien in einem FlexVol-Volume mit derzeit UNIX-Berechtigungen von Windows-Anwendungen bearbeitet und gespeichert werden, kann ONTAP die UNIX-Berechtigungen beibehalten.

Wenn Anwendungen auf Windows-Clients Dateien bearbeiten und speichern, lesen sie die Sicherheitseinstellungen der Datei, erstellen eine neue temporäre Datei, wenden diese Eigenschaften auf die temporäre Datei an und geben der temporären Datei dann den ursprünglichen Dateinamen an.

Wenn Windows-Clients eine Abfrage für die Sicherheitseigenschaften durchführen, erhalten sie eine konstruierte ACL, die genau die UNIX-Berechtigungen repräsentiert. Der einzige Zweck dieser aufgebauten ACL besteht darin, die UNIX-Berechtigungen der Datei beizubehalten, da Dateien von Windows-Anwendungen aktualisiert werden, um sicherzustellen, dass die resultierenden Dateien dieselben UNIX-Berechtigungen haben. ONTAP legt keine NTFS-ACLs mithilfe der konstruierten ACL fest.

### **Verwalten Sie UNIX-Berechtigungen über die Registerkarte Windows-Sicherheit**

Wenn Sie UNIX-Berechtigungen von Dateien oder Ordnern in gemischten Volumes oder qtrees auf SVMs manipulieren möchten, können Sie auf Windows-Clients die Registerkarte „Sicherheit“ verwenden. Alternativ können Sie Anwendungen verwenden, die Windows ACLs abfragen und festlegen können.

- Ändern der UNIX-Berechtigungen

Mithilfe der Registerkarte Windows Security können Sie UNIX Berechtigungen für ein Volume oder einen qtree im gemischten Sicherheitsstil anzeigen und ändern. Wenn Sie die Windows-Hauptregisterkarte verwenden, um UNIX-Berechtigungen zu ändern, müssen Sie zuerst den vorhandenen ACE entfernen, den Sie bearbeiten möchten (dadurch werden die Modusbits auf 0 gesetzt), bevor Sie Ihre Änderungen vornehmen. Alternativ können Sie den erweiterten Editor verwenden, um Berechtigungen zu ändern.

Bei Verwendung von Modusberechtigungen können Sie die Modusberechtigungen für die angegebene UID, GID und andere (alle anderen mit einem Konto auf dem Computer) direkt ändern. Wenn die angezeigte UID beispielsweise r-x-Berechtigungen hat, können Sie die UID-Berechtigungen in rwx ändern.

- Ändern der UNIX-Berechtigungen in NTFS-Berechtigungen

Sie können die Registerkarte Windows Security verwenden, um UNIX Sicherheitsobjekte durch Windows-Sicherheitsobjekte auf einem Volume mit gemischtem Sicherheitsstil oder qtree zu ersetzen, wobei die Dateien und Ordner einen effektiven UNIX-Sicherheitsstil haben.

Sie müssen zuerst alle aufgeführten UNIX-Berechtigungseinträge entfernen, bevor Sie sie durch die gewünschten Windows-Benutzer- und Gruppenobjekte ersetzen können. Anschließend können Sie NTFS-basierte ACLs auf den Windows-Benutzerobjekten konfigurieren. Indem Sie alle UNIX-Sicherheitsobjekte entfernen und nur Windows-Benutzer und -Gruppen zu einer Datei oder einem Ordner in einem gemischten Volume oder qtree hinzufügen, ändern Sie den effektiven Sicherheitsstil auf der Datei oder dem Ordner von UNIX auf NTFS.

Wenn Sie die Berechtigungen für einen Ordner ändern, ist das Windows-Standardverhalten, diese Änderungen auf alle Unterordner und Dateien zu übertragen. Daher müssen Sie die

Ausbreitungsmöglichkeit auf die gewünschte Einstellung ändern, wenn Sie keine Änderung des Sicherheitsstils auf alle untergeordneten Ordner, Unterordner und Dateien übertragen möchten.

## Sicherheitsstile für SVM-Root-Volumes konfigurieren

Sie konfigurieren den Sicherheitsstil des Root-Volumes der Storage Virtual Machine (SVM), um die Art der Berechtigungen zu ermitteln, die für Daten im Root-Volume der SVM verwendet werden.

### Schritte

1. Verwenden Sie die `vserver create` Befehl mit dem `-rootvolume-security-style` Parameter zum Definieren des Sicherheitsstils.

Mögliche Optionen für die Sicherheit im Root-Volume sind `unix`, `ntfs`, Oder `mixed`.

2. Anzeigen und Überprüfen der Konfiguration, einschließlich des Root-Volume-Sicherheitsstils der erstellten SVM:

```
vserver show -vserver vserver_name
```

## Konfigurieren Sie Sicherheitsstile auf FlexVol Volumes

Sie konfigurieren den Sicherheitsstil des FlexVol Volume, um die Art der Berechtigungen zu bestimmen, die für Daten in FlexVol-Volumes der Storage Virtual Machine (SVM) verwendet werden.

### Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn das FlexVol Volume...	Verwenden Sie den Befehl...
Ist noch nicht vorhanden	<code>volume create</code> Und nehmen Sie die auf <code>-security-style</code> Parameter, um den Sicherheitsstil anzugeben.
Ist bereits vorhanden	<code>volume modify</code> Und nehmen Sie die auf <code>-security-style</code> Parameter, um den Sicherheitsstil anzugeben.

Mögliche Optionen für den FlexVol Volume Security Stil sind `unix`, `ntfs`, Oder `mixed`.

Wenn Sie beim Erstellen eines FlexVol-Volumes keinen Sicherheitsstil festlegen, erbt das Volume den Sicherheitsstil des Root-Volumes.

Weitere Informationen zum `volume create` Oder `volume modify` Befehle, siehe "[Logisches Storage-Management](#)".

2. Um die Konfiguration anzuzeigen, einschließlich des Sicherheitsstils des erstellten FlexVol-Volumes, geben Sie den folgenden Befehl ein:

```
volume show -volume volume_name -instance
```

## Security Styles auf qtrees konfigurieren

Sie konfigurieren den Sicherheitsstil des qtree Volume, um die Art der Berechtigungen zu bestimmen, die für Daten in qtrees verwendet werden.

### Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn der qtree...	Verwenden Sie den Befehl...
Ist noch nicht vorhanden	<code>volume qtree create</code> Und nehmen Sie die auf <code>-security-style</code> Parameter, um den Sicherheitsstil anzugeben.
Ist bereits vorhanden	<code>volume qtree modify</code> Und nehmen Sie die auf <code>-security-style</code> Parameter, um den Sicherheitsstil anzugeben.

Die möglichen Optionen für den qtree-Sicherheitsstil sind `unix`, `ntfs`, Oder `mixed`.

Wenn Sie beim Erstellen eines qtree keinen Sicherheitsstil angeben, wird der Standardsicherheitsstil festgelegt `mixed`.

Weitere Informationen zum `volume qtree create` Oder `volume qtree modify` Befehle, siehe "[Logisches Storage-Management](#)".

2. Geben Sie zum Anzeigen der Konfiguration, einschließlich des Sicherheitsstils des erstellten qtree, den folgenden Befehl ein: `volume qtree show -qtree qtree_name -instance`

## Richten Sie den Dateizugriff über NFS ein

### Richten Sie den Dateizugriff über NFS Overview ein

Sie müssen eine Reihe von Schritten durchführen, um Clients über NFS den Zugriff auf Dateien auf Storage Virtual Machines (SVMs) zu erlauben. Abhängig von der aktuellen Konfiguration Ihrer Umgebung sind einige zusätzliche Schritte optional.

Damit Clients über NFS auf Dateien auf SVMs zugreifen können, müssen Sie die folgenden Aufgaben durchführen:

1. Aktivieren des NFS-Protokolls auf der SVM

Sie müssen die SVM konfigurieren, um den Datenzugriff von Clients über NFS zu ermöglichen.

2. Erstellen eines NFS-Servers auf der SVM

Ein NFS-Server ist eine logische Einheit auf der SVM, über die die SVM Dateien über NFS bereitstellen kann. Sie müssen den NFS-Server erstellen und die NFS-Protokollversionen angeben, die zugelassen werden sollen.

3. Exportrichtlinien für die SVM konfigurieren

Sie müssen Exportrichtlinien konfigurieren, um Volumes und qtrees für Clients verfügbar zu machen.

4. Konfigurieren Sie den NFS-Server je nach Netzwerk- und Storage-Umgebung mit entsprechenden Sicherheits- und anderen Einstellungen.

Dieser Schritt kann die Konfiguration von Kerberos, LDAP, NIS, Namenszuordnungen und lokalen Benutzern umfassen.

## Sicherer NFS-Zugriff über Exportrichtlinien

### Wie Exportrichtlinien den Client-Zugriff auf Volumes oder qtrees steuern

Exportrichtlinien enthalten mindestens eine *Exportregel*, die jede Clientzugriffsanforderung verarbeitet. Das Ergebnis des Prozesses legt fest, ob der Client-Zugriff verweigert oder gewährt wird und welche Zugriffsstufe. Auf der Storage Virtual Machine (SVM) muss eine Exportrichtlinie mit Exportregeln vorhanden sein, damit Clients auf Daten zugreifen können.

Sie verknüpfen jedem Volume oder qtree exakt eine Exportrichtlinie, um den Client-Zugriff auf das Volume oder qtree zu konfigurieren. Die SVM kann mehrere Exportrichtlinien enthalten. Dies ermöglicht Ihnen die folgenden Aktionen für SVMs mit mehreren Volumes oder qtrees:

- Jedem Volume oder qtree der SVM müssen für jedes Volume oder qtree verschiedene Exportrichtlinien zugewiesen werden, um für jedes Volume oder qtree in der SVM individuelle Zugriffskontrollen zu ermöglichen.
- Weisen Sie für eine identische Client-Zugriffskontrolle dieselbe Exportrichtlinie mehreren Volumes oder qtrees der SVM zu, ohne dass für jedes Volume oder qtree eine neue Exportrichtlinie erstellt werden muss.

Wenn ein Client eine Zugriffsanforderung stellt, die von der entsprechenden Exportrichtlinie nicht zulässig ist, schlägt die Anforderung mit einer Nachricht, die eine Berechtigung verweigert hat, fehl. Wenn ein Client keine Regel in der Exportrichtlinie enthält, wird der Zugriff verweigert. Wenn eine Exportrichtlinie leer ist, werden alle Zugriffe implizit verweigert.

Sie können eine Exportrichtlinie auf einem System, auf dem ONTAP ausgeführt wird, dynamisch ändern.

### Standardmäßige Exportrichtlinie für SVMs

Jede SVM verfügt über eine standardmäßige Exportrichtlinie, die keine Regeln enthält. Bevor Clients auf Daten auf der SVM zugreifen können, muss eine Exportrichtlinie mit Regeln vorhanden sein. Jedes FlexVol Volume in der SVM muss einer Exportrichtlinie zugeordnet werden.

Wenn Sie eine SVM erstellen, erstellt das Storage-System automatisch eine Standard-Exportrichtlinie mit dem Namen `default` für das Root-Volume der SVM. Sie müssen eine oder mehrere Regeln für die Standard-Exportrichtlinie erstellen, bevor Clients auf Daten auf der SVM zugreifen können. Alternativ können Sie auch eine benutzerdefinierte Exportrichtlinie mit Regeln erstellen. Sie können die Standard-Exportrichtlinie ändern und umbenennen, aber Sie können die standardmäßige Exportrichtlinie nicht löschen.

Wenn Sie ein FlexVol Volume mit SVM erstellen, erstellt das Storage-System das Volume und ordnet das Volume der standardmäßigen Exportrichtlinie für das Root-Volume der SVM zu. Standardmäßig ist jedes in der SVM erstellte Volume der standardmäßigen Exportrichtlinie für das Root-Volume zugeordnet. Sie können die Standard-Exportrichtlinie für alle Volumes in der SVM verwenden oder für jedes Volume eine eindeutige Exportrichtlinie erstellen. Sie können mehrere Volumes derselben Exportrichtlinie zuordnen.



## Wie Exportregeln funktionieren

Exportregeln sind die funktionalen Elemente einer Exportrichtlinie. Exportregeln stimmen die Client-Zugriffsanforderungen auf ein Volume ab. Dabei werden bestimmte Parameter verwendet, die Sie konfigurieren, um zu bestimmen, wie die Clientzugriffsanforderungen verarbeitet werden sollen.

Eine Exportrichtlinie muss mindestens eine Exportregel enthalten, um den Zugriff auf Clients zu ermöglichen. Wenn eine Exportrichtlinie mehrere Regeln enthält, werden die Regeln in der Reihenfolge verarbeitet, in der sie in der Exportrichtlinie angezeigt werden. Die Regelreihenfolge wird durch die Indexnummer der Regel vorgegeben. Stimmt eine Regel mit einem Client überein, werden die Berechtigungen dieser Regel verwendet und keine weiteren Regeln verarbeitet. Stimmen keine Regeln überein, wird dem Client der Zugriff verweigert.

Sie können Exportregeln konfigurieren, um Clientzugriffsberechtigungen anhand der folgenden Kriterien zu ermitteln:

- Das Dateizugriffsprotokoll, das vom Client verwendet wird, der die Anforderung sendet, z. B. NFSv4 oder SMB.
- Eine Client-ID, z. B. Hostname oder IP-Adresse.

Die maximale Größe für die `-clientmatch` Das Feld darf 4096 Zeichen enthalten.

- Der vom Client zum Authentifizieren verwendete Sicherheitstyp, z. B. Kerberos v5, NTLM oder AUTH\_SYS.

Wenn in einer Regel mehrere Kriterien angegeben sind, muss der Client alle Kriterien erfüllen, damit die Regel angewendet werden kann.



Ab ONTAP 9.3 können Sie die Überprüfung der Konfiguration der Exportrichtlinie als Hintergrundjob aktivieren, der Regelverletzungen in einer Fehlerregelliste aufzeichnet. Der `vserver export-policy config-checker` Befehle rufen den Checker auf und zeigen Ergebnisse an, mit denen Sie Ihre Konfiguration überprüfen und fehlerhafte Regeln aus der Richtlinie löschen können.

Die Befehle validieren lediglich die Exportkonfiguration für Hostnamen, Netzwerkgruppen und anonyme Benutzer.

### Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

Die Client-Zugriffsanforderung wird mithilfe des NFSv3-Protokolls versendet, und der Client hat die IP-Adresse 10.1.17.37.

Obwohl das Client-Zugriffsprotokoll übereinstimmt, befindet sich die IP-Adresse des Clients in einem anderen Subnetz als dem in der Exportregel angegebenen. Daher schlägt die Clientabgleich fehl, und diese Regel gilt nicht für diesen Client.

## Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

Die Client-Zugriffsanforderung wird mit dem NFSv4-Protokoll gesendet, und der Client hat die IP-Adresse 10.1.16.54.

Das Client-Zugriffsprotokoll stimmt überein, und die IP-Adresse des Clients befindet sich im angegebenen Subnetz. Daher ist die Clientabgleich erfolgreich, und diese Regel gilt für diesen Client. Der Client erhält unabhängig vom Sicherheitstyp Lese-/Schreibzugriff.

## Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

Client #1 hat die IP-Adresse 10.1.16.207, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit Kerberos v5.

Client #2 hat die IP-Adresse 10.1.16.211, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit AUTH\_SYS.

Das Client-Zugriffsprotokoll und die IP-Adresse stimmen für beide Clients überein. Der schreibgeschützte Parameter ermöglicht den schreibgeschützten Zugriff auf alle Clients unabhängig vom Sicherheitstyp, mit dem sie authentifiziert wurden. Daher erhalten beide Clients nur Lesezugriff. Allerdings erhält nur Client #1 Lese-Schreib-Zugriff, weil er den genehmigten Sicherheitstyp Kerberos v5 zur Authentifizierung verwendet hat. Client #2 erhält keinen Lese-/Schreibzugriff.

## Verwalten von Clients mit einem nicht aufgelisteten Sicherheitstyp

Wenn ein Client sich mit einem Sicherheitstyp präsentiert, der nicht in einem Zugriffsparameter einer Exportregel aufgeführt ist, haben Sie die Wahl, entweder den Zugriff auf den Client zu verweigern oder ihn stattdessen der anonymen Benutzer-ID zuzuordnen, indem Sie die Option verwenden `none` Im Zugriffsparameter.

Ein Client kann sich mit einem Sicherheitstyp präsentieren, der nicht in einem Zugriffsparameter aufgeführt ist, da er mit einem anderen Sicherheitstyp authentifiziert wurde oder überhaupt nicht authentifiziert wurde (Sicherheitstyp AUTH\_NONE). Standardmäßig wird dem Client automatisch der Zugriff auf diese Ebene verweigert. Sie können die Option jedoch hinzufügen `none` Zum Zugriffsparameter. Als Ergebnis werden Clients mit einem nicht aufgelisteten Sicherheitsstil stattdessen der anonymen Benutzer-ID zugeordnet. Der `-anon` Parameter legt fest, welche Benutzer-ID diesen Clients zugewiesen ist. Die für das angegebene Benutzer-ID `-anon` Der Parameter muss ein gültiger Benutzer sein, der mit Berechtigungen konfiguriert ist, die

Sie für den anonymen Benutzer als geeignet erachten.

Gültige Werte für das `-anon` Parameterbereich von 0 Bis 65535.

Benutzer-ID zugewiesen zu <code>-anon</code>	Die sich daraus ergebende Bearbeitung von Client-Zugriffsanfragen
0 - 65533	Die Clientzugriffsanforderung wird der anonymen Benutzer-ID zugeordnet und erhält je nach den für diesen Benutzer konfigurierten Berechtigungen Zugriff.
65534	Die Client-Zugriffsanforderung ist dem Benutzer niemand zugeordnet und erhält je nach den für diesen Benutzer konfigurierten Berechtigungen Zugriff. Dies ist die Standardeinstellung.
65535	Die Zugriffsanforderung eines beliebigen Clients wird verweigert, wenn diese ID zugeordnet ist, und der Client stellt sich mit dem Sicherheitstyp <code>AUTH_NONE</code> vor. Die Zugriffsanforderung von Clients mit Benutzer-ID 0 wird verweigert, wenn sie dieser ID zugeordnet sind und der Client sich mit jedem anderen Sicherheitstyp präsentiert.

Wenn Sie die Option verwenden `none`, Es ist wichtig zu beachten, dass der schreibgeschützte Parameter zuerst verarbeitet wird. Beachten Sie die folgenden Richtlinien, wenn Sie Exportregeln für Clients mit nicht aufgeführten Sicherheitstypen konfigurieren:

Read-Only umfasst <code>none</code>	Lese-Schreib-enthält <code>none</code>	Dadurch wird Zugriff für Clients mit nicht aufgelisteten Sicherheitstypen gewährleistet
Nein	Nein	Abgelehnt
Nein	Ja.	Abgelehnt, da schreibgeschützt zuerst verarbeitet wird
Ja.	Nein	Schreibgeschützt als anonym
Ja.	Ja.	Lese-Schreib als anonym

### Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`

- `-rwrule any`
- `-anon 70`

Client #1 hat die IP-Adresse 10.1.16.207, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit Kerberos v5.

Client #2 hat die IP-Adresse 10.1.16.211, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit AUTH\_SYS.

Client #3 hat die IP-Adresse 10.1.16.234, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert sich nicht (was bedeutet Sicherheitstyp AUTH\_NONE).

Das Client-Zugriffsprotokoll und die IP-Adresse stimmen für alle drei Clients überein. Der schreibgeschützte Parameter ermöglicht den schreibgeschützten Zugriff auf Clients mit eigener Benutzer-ID, die mit AUTH\_SYS authentifiziert wurde. Der schreibgeschützte Parameter ermöglicht schreibgeschützten Zugriff als anonymer Benutzer mit Benutzer-ID 70 auf Clients, die mit anderen Sicherheitstypen authentifiziert wurden. Der Lese-Schreib-Parameter erlaubt Lese-Schreib-Zugriff auf jeden Sicherheitstyp, gilt in diesem Fall jedoch nur für Clients, die bereits durch die schreibgeschützte Regel gefiltert sind.

Clients #1 und #3 erhalten daher Lese-/Schreibzugriff nur als anonymer Benutzer mit Benutzer-ID 70. Client #2 erhält Lese-/Schreibzugriff mit einer eigenen Benutzer-ID.

### Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys, none`
- `-rwrule none`
- `-anon 70`

Client #1 hat die IP-Adresse 10.1.16.207, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit Kerberos v5.

Client #2 hat die IP-Adresse 10.1.16.211, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit AUTH\_SYS.

Client #3 hat die IP-Adresse 10.1.16.234, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert sich nicht (was bedeutet Sicherheitstyp AUTH\_NONE).

Das Client-Zugriffsprotokoll und die IP-Adresse stimmen für alle drei Clients überein. Der schreibgeschützte Parameter ermöglicht den schreibgeschützten Zugriff auf Clients mit eigener Benutzer-ID, die mit AUTH\_SYS authentifiziert wurde. Der schreibgeschützte Parameter ermöglicht schreibgeschützten Zugriff als anonymer Benutzer mit Benutzer-ID 70 auf Clients, die mit anderen Sicherheitstypen authentifiziert wurden. Der Lese-Schreib-Parameter erlaubt den Lese-Schreib-Zugriff nur als anonymer Benutzer.

Client #1 und Client #3 erhalten daher nur Lese-/Schreibzugriff als anonymer Benutzer mit Benutzer-ID 70. Client #2 erhält schreibgeschützten Zugriff mit einer eigenen Benutzer-ID, wird aber Lese-Schreib-Zugriff verweigert.

## Wie Sicherheitstypen die Client-Zugriffsebenen bestimmen

Der Sicherheitstyp, mit dem der Client authentifiziert wurde, spielt eine besondere Rolle in den Exportregeln. Sie müssen verstehen, wie der Sicherheitstyp die Zugriffsebenen bestimmt, die der Client zu einem Volume oder qtree erhält.

Die drei möglichen Zugriffsebenen sind wie folgt:

1. Schreibgeschützt
2. Lesen und schreiben
3. Superuser (für Clients mit Benutzer-ID 0)

Da die Zugriffsebene nach Sicherheitstyp in dieser Reihenfolge ausgewertet wird, müssen Sie beim Erstellen von Parametern auf Zugriffsebene in Exportregeln folgende Regeln beachten:

Damit ein Client die Zugriffsebene abrufen kann...	Diese Zugriffsparameter müssen dem Sicherheitstyp des Clients entsprechen...
Normaler Benutzer schreibgeschützt	Schreibgeschützt ( <code>-rorule</code> )
Normaler Benutzer Lese-/Schreibzugriff	Schreibgeschützt ( <code>-rorule</code> ) Und lesen-schreiben ( <code>-rwrule</code> )
Schreibgeschützt für Superuser	Schreibgeschützt ( <code>-rorule</code> ) Und <code>-superuser</code>
Superuser lesen und schreiben	Schreibgeschützt ( <code>-rorule</code> ) Und lesen-schreiben ( <code>-rwrule</code> ) Und <code>-superuser</code>

Die folgenden Sicherheitstypen sind für jeden der folgenden drei Zugriffsparameter gültig:

- `any`
- `none`
- `never`

Dieser Sicherheitstyp ist für die Verwendung mit dem nicht gültig `-superuser` Parameter.

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`
- `sys`

Beim Abgleich des Sicherheitstyps eines Clients mit jedem der drei Zugriffsparameter gibt es drei mögliche Ergebnisse:

Falls der Sicherheitstyp des Clients...	Dann der Client...
Stimmt mit dem im Zugriffsparameter angegebenen überein.	Erhält Zugriff auf dieses Level mit eigener Benutzer-ID.
Stimmt nicht mit dem angegebenen überein, der Zugriffsparameter enthält jedoch die Option <code>none</code> .	Ruft Zugriff auf diese Ebene, jedoch als anonymer Benutzer mit der von angegebenen Benutzer-ID ab <code>-anon</code> Parameter.
Stimmt nicht mit dem angegebenen überein und der Zugriffsparameter enthält die Option nicht <code>none</code> .	Für diese Ebene wird kein Zugriff erhalten. Dies gilt nicht für die <code>-superuser</code> Parameter, da er immer enthält <code>none</code> Auch wenn sie nicht angegeben werden.

### Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule sys, krb5`
- `-superuser krb5`

Client #1 hat die IP-Adresse 10.1.16.207, hat Benutzer-ID 0, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit Kerberos v5.

Client #2 hat die IP-Adresse 10.1.16.211, hat Benutzer-ID 0, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit AUTH\_SYS.

Client #3 hat die IP-Adresse 10.1.16.234, hat Benutzer-ID 0, sendet eine Zugriffsanforderung über das NFSv3-Protokoll und authentifiziert nicht (AUTH\_NONE).

Das Client-Zugriffsprotokoll und die IP-Adresse stimmen mit allen drei Clients überein. Der schreibgeschützte Parameter ermöglicht den schreibgeschützten Zugriff auf alle Clients unabhängig vom Sicherheitstyp. Der Lese-Schreib-Parameter ermöglicht den Lese-Schreib-Zugriff auf Clients mit eigener Benutzer-ID, die mit AUTH\_SYS oder Kerberos v5 authentifiziert wurden. Der Superuser-Parameter ermöglicht Superuser-Zugriff auf Clients mit Benutzer-ID 0, die mit Kerberos v5 authentifiziert wurden.

Client #1 erhält daher Lese-/Schreibzugriff für Superuser, da er alle drei Zugriffsparameter einordnet. Client #2 erhält Lese-/Schreibzugriff, aber keinen Superuser-Zugriff. Client #3 erhält nur Lesezugriff, aber keinen Superuser-Zugriff.

### Management von Zugriffsanfragen durch Superbenutzer

Wenn Sie Exportrichtlinien konfigurieren, müssen Sie berücksichtigen, was Sie tun möchten, wenn das Storage-System eine Client-Zugriffsanfrage mit Benutzer-ID 0 erhält, also als Superuser, und Ihre Exportregeln entsprechend festlegen.

In der UNIX-Welt wird ein Benutzer mit der Benutzer-ID 0 als Superuser bezeichnet, der normalerweise root genannt wird, der unbegrenzte Zugriffsrechte auf einem System besitzt. Die Verwendung von Superuser-

Berechtigungen kann aus verschiedenen Gründen gefährlich sein, einschließlich Verletzung des Systems und der Datensicherheit.

Standardmäßig ordnet ONTAP Clients, die mit der Benutzer-ID 0 angezeigt werden, dem anonymen Benutzer zu. Sie können jedoch die angeben `-superuser` Parameter in Exportregeln, um zu bestimmen, wie Clients, die je nach Sicherheitstyp mit Benutzer-ID 0 angegeben werden, behandelt werden. Die folgenden Optionen sind gültig für die `-superuser` Parameter:

- any
- none

Dies ist die Standardeinstellung, wenn Sie den nicht angeben `-superuser` Parameter.

- krb5
- ntlm
- sys

Es gibt zwei verschiedene Arten, wie Clients, die mit der Benutzer-ID 0 angezeigt werden, je nach behandelt werden `-superuser` Parameterkonfiguration:

Wenn der <code>-superuser</code> Parameter und der Sicherheitstyp des Clients...	Dann der Client...
Übereinstimmung	Erhält Superuser-Zugriff mit Benutzer-ID 0.
Stimmen Sie nicht überein	Ruft als anonymen Benutzer mit der vom angegebenen Benutzer-ID auf <code>-anon</code> Parameter und seine zugewiesenen Berechtigungen. Dies ist unabhängig davon, ob der Parameter schreibgeschützt oder Lesen/Schreiben die Option angibt <code>none</code> .

Wenn ein Client mit der Benutzer-ID 0 angezeigt wird, um auf ein Volume mit dem NTFS-Sicherheitsstil und dem zuzugreifen `-superuser` Parameter ist auf festgelegt `none`, ONTAP verwendet die Namenszuweisung für den anonymen Benutzer, um die richtigen Anmeldedaten zu erhalten.

### Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-anon 127`

Client #1 hat die IP-Adresse 10.1.16.207, hat Benutzer-ID 746, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit Kerberos v5.



Client #2 hat die IP-Adresse 10.1.16.211, hat Benutzer-ID 0, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit AUTH\_SYS.

Das Client-Zugriffsprotokoll und die IP-Adresse stimmen für beide Clients überein. Der schreibgeschützte Parameter ermöglicht den schreibgeschützten Zugriff auf alle Clients unabhängig vom Sicherheitstyp, mit dem sie authentifiziert wurden. Allerdings erhält nur Client #1 Lese-Schreib-Zugriff, weil er den genehmigten Sicherheitstyp Kerberos v5 zur Authentifizierung verwendet hat.

Client #2 erhält keinen Superuser-Zugriff. Stattdessen wird sie anonym zugeordnet, weil die `-superuser` Parameter wurde nicht angegeben. Das bedeutet, dass es standardmäßig eingestellt ist `none` Und ordnet die Benutzer-ID 0 automatisch anonym zu. Client #2 erhält auch nur schreibgeschützten Zugriff, da sein Sicherheitstyp nicht mit dem Parameter Read-Write übereinstimmt.

### Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

Client #1 hat die IP-Adresse 10.1.16.207, hat Benutzer-ID 0, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit Kerberos v5.

Client #2 hat die IP-Adresse 10.1.16.211, hat Benutzer-ID 0, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit AUTH\_SYS.

Das Client-Zugriffsprotokoll und die IP-Adresse stimmen für beide Clients überein. Der schreibgeschützte Parameter ermöglicht den schreibgeschützten Zugriff auf alle Clients unabhängig vom Sicherheitstyp, mit dem sie authentifiziert wurden. Allerdings erhält nur Client #1 Lese-Schreib-Zugriff, weil er den genehmigten Sicherheitstyp Kerberos v5 zur Authentifizierung verwendet hat. Client #2 erhält keinen Lese-/Schreibzugriff.

Die Exportregel erlaubt Superuser-Zugriff für Clients mit Benutzer-ID 0. Client #1 erhält Superuser-Zugriff, da er mit der Benutzer-ID und dem Sicherheitstyp für den schreibgeschützten und übereinstimmt `-superuser` Parameter. Client #2 erhält keinen Lese-/Schreib- oder Superuser-Zugriff, da sein Sicherheitstyp nicht mit dem Lese-Schreib-Parameter oder dem übereinstimmt `-superuser` Parameter. Stattdessen wird Client #2 dem anonymen Benutzer zugeordnet, der in diesem Fall die Benutzer-ID 0 hat.

### So nutzt ONTAP Exportrichtlinien-Caches

Zur Verbesserung der Systemperformance verwendet ONTAP lokale Caches zum Speichern von Informationen wie Hostnamen und Netzwerkgruppen. So kann ONTAP die Regeln für Exportrichtlinien schneller verarbeiten als die Informationen aus externen Quellen abzurufen. Informationen über die Caches und ihre Maßnahmen können Ihnen bei der Fehlerbehebung bei Problemen mit dem Client-Zugriff helfen.

Sie konfigurieren Exportrichtlinien, um den Client-Zugriff auf NFS-Exporte zu steuern. Jede Exportrichtlinie enthält Regeln, und jede Regel enthält Parameter, die der Regel entsprechen, die Clients, die Zugriff

anfordern, anfordert. Bei einigen dieser Parameter muss ONTAP eine externe Quelle kontaktieren, z. B. DNS- oder NIS-Server, um Objekte wie Domain-Namen, Host-Namen oder Netzwerkgruppen zu lösen.

Diese Kommunikation mit externen Quellen nimmt eine kleine Menge Zeit in Anspruch. Um die Performance zu steigern, reduziert ONTAP die benötigte Zeit zur Auflösung von Objekten für Exportregelungen, indem Informationen lokal auf jedem Node in mehreren Caches gespeichert werden.

Cache-Name	Art der gespeicherten Informationen
Datenzugriff	Zuordnung von Clients zu entsprechenden Exportrichtlinien
Name	Zuordnungen von UNIX-Benutzernamen zu entsprechenden UNIX-Benutzer-IDs
ID	Zuordnungen von UNIX-Benutzer-IDs zu entsprechenden UNIX-Benutzer-IDs und erweiterten UNIX-Gruppen-IDs
Host	Zuordnung von Hostnamen zu entsprechenden IP-Adressen
Netzgruppe	Zuordnung von Netzgruppen zu entsprechenden IP-Adressen der Mitglieder
Showmount	Liste der exportierten Verzeichnisse aus SVM Namespace

Wenn Sie nach dem Abrufen und Speichern von ONTAP Daten über die externen Nameserver in Ihrer Umgebung ändern, können die Caches nun veraltete Informationen enthalten. Auch wenn ONTAP Cache-Aktualisierungen nach bestimmten Zeiträumen automatisch aktualisiert, haben verschiedene Caches unterschiedliche Ablaufdaten, Aktualisierungszeiten und Algorithmen.

Ein weiterer möglicher Grund, warum Caches veraltete Informationen enthalten, ist, wenn ONTAP versucht, zwischengespeicherte Informationen zu aktualisieren, aber beim Versuch, mit Name-Servern zu kommunizieren, einen Fehler auftritt. Sollte dies der Fall sein, verwendet ONTAP die derzeit in den lokalen Caches gespeicherten Informationen weiter, um eine Client-Unterbrechung zu vermeiden.

Dadurch können Clientzugriffsanforderungen, die erfolgreich ausgeführt werden sollen, fehlschlagen, und Clientzugriffsanfragen, die fehlschlagen sollen, können erfolgreich ausgeführt werden. Sie können einige der Caches für Exportrichtlinien anzeigen und manuell bereinigen, wenn Sie solche Probleme mit dem Clientzugriff beheben.

### So funktioniert der Zugriffs-Cache

ONTAP verwendet einen Zugriffs-Cache, um die Ergebnisse der Bewertung von Exportrichtlinien für Client-Zugriffsoperationen auf ein Volume oder einen qtree zu speichern. Das führt zu Performance-Verbesserungen, da die Informationen viel schneller aus dem Zugriffs-Cache abgerufen werden können als jedes Mal, wenn ein Client eine I/O-Anforderung sendet, den Auswertungsprozess für die Richtlinie für den Export durchzugehen.

Sobald ein NFS-Client eine I/O-Anforderung für den Zugriff auf Daten eines Volume oder qtree sendet, muss ONTAP jede I/O-Anfrage bewerten, um zu ermitteln, ob die I/O-Anforderung erteilt oder abgelehnt werden soll. Diese Bewertung beinhaltet die Überprüfung jeder Regel für die Exportrichtlinie, die mit dem Volume oder qtree verknüpft ist. Wenn der Pfad zum Volume oder qtree einen oder mehrere Verbindungspunkte überschreiten muss, muss diese Prüfung möglicherweise für mehrere Exportrichtlinien entlang des Pfads durchgeführt werden.

Beachten Sie, dass diese Bewertung für jede von einem NFS-Client gesendete I/O-Anfrage, z. B. Lesen, Schreiben, Liste, Kopieren und andere Vorgänge, nicht nur für anfängliche Mount-Anforderungen durchgeführt wird.

Nachdem ONTAP die geltenden Regeln für die Exportrichtlinie ermittelt und entschieden hat, ob die Anfrage zugelassen werden soll oder abgelehnt wird, erstellt ONTAP dann zum Speichern dieser Informationen einen Eintrag im Zugriffs-Cache.

Wenn ein NFS-Client eine I/O-Anfrage sendet, nimmt ONTAP die IP-Adresse des Clients, die ID der SVM und die dem Ziel-Volume oder qtree zugeordnete Exportrichtlinie zur Kenntnis. Außerdem überprüft er zuerst den Zugriffs-Cache auf einen entsprechenden Eintrag. Wenn im Zugriffs-Cache ein übereinstimmender Eintrag vorhanden ist, verwendet ONTAP die gespeicherten Informationen, um die I/O-Anforderung zuzulassen oder abzulehnen. Wenn kein übereinstimmender Eintrag vorhanden ist, durchläuft ONTAP den normalen Prozess der Auswertung aller anwendbaren Richtlinienregeln, wie oben erläutert.

Einträge im Zugriffs-Cache, die nicht aktiv genutzt werden, werden nicht aktualisiert. Dies reduziert unnötige und verschwenderische Kommunikation mit externen Namen.

Das Abrufen der Informationen aus dem Zugriffs-Cache ist wesentlich schneller als das Auswertungsprozess für die gesamte Exportrichtlinie für jede I/O-Anforderung. Daher verbessert die Nutzung des Zugriffs-Cache die Performance immens, indem der Overhead von Client-Zugriffsprüfungen verringert wird.

### **Funktionsweise von Zugriffsparametern im Cache**

Mehrere Parameter steuern die Aktualisierungszeiträume für Einträge im Zugriffs-Cache. Wenn Sie die Funktionsweise dieser Parameter verstehen, können Sie sie ändern, um den Zugriffs-Cache zu optimieren und die Performance mit den neuesten gespeicherten Informationen abzustimmen.

Im Zugriffs-Cache werden Einträge gespeichert, die aus einer oder mehreren Exportregeln bestehen, die für Clients gelten, die auf Volumes oder qtrees zugreifen möchten. Diese Einträge werden für eine bestimmte Zeit gespeichert, bevor sie aktualisiert werden. Die Aktualisierungszeit wird durch Parameter des Zugriffs-Caches bestimmt und hängt vom Typ des Eintrags aus dem Zugriffs-Cache ab.

Sie können Parameter für den Zugriffs-Cache für einzelne SVMs festlegen. Dadurch können die Parameter entsprechend den SVM-Zugriffsanforderungen variieren. Nicht aktiv verwendete Zugriffs-Cache-Einträge werden nicht aktualisiert, was die unnötige und verschwenderische Kommunikation mit externen Namen reduziert.

Eintragstyp für den Zugriffs-Cache	Beschreibung	Aktualisierung innerhalb von Sekunden
------------------------------------	--------------	---------------------------------------

Positive Beiträge	Einträge im Zugriffs-Cache, die nicht zu einem Denial-Access-Zugriff auf Clients geführt haben.	Minimum: 300 Maximal 86,400 Standard: 3,600
Negative Einträge	Einträge im Zugriffs-Cache, die zu einem Denial-Access-Zugriff auf Clients geführt haben.	Minimum: 60 Maximal 86,400 Standard: 3,600

### Beispiel

Ein NFS-Client versucht, auf ein Volume in einem Cluster zuzugreifen. ONTAP stimmt den Client mit einer Regel für die Exportrichtlinie ab und legt fest, dass der Client basierend auf der Konfiguration der Regel für die Exportrichtlinie auf Zugriff erhält. Als positiver Eintrag speichert ONTAP die Regel für die Exportrichtlinie im Zugriffs-Cache. Standardmäßig behält ONTAP den positiven Eintrag im Zugriffs-Cache eine Stunde (3,600 Sekunden) bei und aktualisiert den Eintrag automatisch, um die Informationen auf dem aktuellen Stand zu halten.

Um zu verhindern, dass der Zugriffs-Cache unnötig auffüllt wird, gibt es einen zusätzlichen Parameter, um vorhandene Einträge aus dem Zugriffs-Cache zu löschen, die für einen bestimmten Zeitraum nicht verwendet wurden, um den Client-Zugriff zu bestimmen. Das `-harvest-timeout` Der zulässige Bereich für den Parameter beträgt 60 bis 2,592,000 Sekunden und die Standardeinstellung 86,400 Sekunden.

### Entfernen Sie eine Exportrichtlinie von einem qtree

Wenn Sie sich entscheiden, dass einer bestimmten Exportrichtlinie einem qtree nicht mehr zugewiesen wird, können Sie die Exportrichtlinie entfernen, indem Sie den qtree ändern, um die Exportrichtlinie des enthaltenden Volumes stattdessen zu übernehmen. Dies können Sie mit dem `tun volume qtree modify` Befehl mit dem `-export -policy` Parameter und eine leere Namenszeichenfolge („").

### Schritte

1. Geben Sie den folgenden Befehl ein, um eine Exportrichtlinie von einem qtree zu entfernen:

```
volume qtree modify -vserver vserver_name -qtree-path
/vol/volume_name/qtree_name -export-policy ""
```

2. Vergewissern Sie sich, dass der qtree entsprechend geändert wurde:

```
volume qtree show -qtree qtree_name -fields export-policy
```

### Qtree IDs für qtree-Dateivorgänge validieren

ONTAP kann eine zusätzliche Validierung von qtree IDs optional durchführen. Diese Validierung stellt sicher, dass Anforderungen der Client-Dateioperationen eine gültige qtree ID verwenden und dass Clients Dateien nur innerhalb desselben qtree verschieben können. Sie können diese Validierung aktivieren oder deaktivieren, indem Sie den ändern

`-validate-qtrees-export` Parameter. Dieser Parameter ist standardmäßig aktiviert.

### Über diese Aufgabe

Dieser Parameter ist nur dann effektiv, wenn Sie einer oder mehreren qtrees auf der Storage Virtual Machine (SVM) eine Exportrichtlinie direkt zugewiesen haben.

### Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Führen Sie eine der folgenden Aktionen aus:

Wenn die qtrees ID-Validierung gewünscht wird...	Geben Sie den folgenden Befehl ein...
Aktiviert	<pre>vserver nfs modify -vserver vserver_name -validate-qtrees-export enabled</pre>
Deaktiviert	<pre>vserver nfs modify -vserver vserver_name -validate-qtrees-export disabled</pre>

3. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

### Einschränkungen der Exportrichtlinien und verschachtelte Verbindungen für FlexVol Volumes

Wenn Sie Exportrichtlinien so konfiguriert haben, dass eine weniger restriktive Richtlinie für eine verschachtelte Verbindung festgelegt wird, jedoch eine restriktivere Richtlinie für eine Verbindung höherer Ebene, kann der Zugriff auf die untere Ebene fehlschlagen.

Sie sollten sicherstellen, dass Verbindungen auf höherer Ebene weniger restriktive Exportrichtlinien aufweisen als Verbindungen auf niedrigerer Ebene.

### Hohe Sicherheit durch Kerberos mit NFS

#### ONTAP-Unterstützung für Kerberos

Kerberos bietet eine starke, sichere Authentifizierung für Client-/Server-Applikationen. Authentifizierung ermöglicht die Überprüfung von Benutzer- und Prozessidentitäten auf einem Server. In der ONTAP Umgebung bietet Kerberos die Authentifizierung zwischen Storage Virtual Machines (SVMs) und NFS-Clients.

In ONTAP 9 wird die folgende Kerberos-Funktion unterstützt:

- Kerberos 5-Authentifizierung mit Integritätsprüfung (krb5i)

Krb5i verwendet Prüfsummen, um die Integrität jeder NFS-Nachricht, die zwischen Client und Server

übertragen wurde, zu überprüfen. Dies ist sowohl aus Sicherheitsgründen (um sicherzustellen, dass Daten nicht manipuliert werden) als auch aus Gründen der Datenintegrität (zum Beispiel zur Vermeidung von Datenkorruption bei der Nutzung von NFS über unzuverlässige Netzwerke) nützlich.

- Kerberos 5-Authentifizierung mit Datenschutzprüfung (krb5p)

Krb5p verwendet Prüfsummen, um den gesamten Verkehr zwischen Client und Server zu verschlüsseln. Dies ist sicherer und führt zu einer höheren Belastung.

- 128-Bit- und 256-Bit-AES-Verschlüsselung

Advanced Encryption Standard (AES) ist ein Verschlüsselungsalgorithmus zur Sicherung elektronischer Daten. ONTAP unterstützt jetzt AES mit 128-Bit-Schlüsseln (AES-128) und AES mit 256-Bit-Verschlüsselung (AES-256) für Kerberos für eine höhere Sicherheit.

- Kerberos-Bereichskonfigurationen auf SVM-Ebene

SVM-Administratoren können jetzt Kerberos-Bereichskonfigurationen auf SVM-Ebene erstellen. Das bedeutet, dass SVM-Administratoren sich bei der Konfiguration von Kerberos-Bereich nicht mehr auf den Cluster-Administrator verlassen müssen und in einer mandantenfähigen Umgebung einzelne Kerberos-Bereichskonfigurationen erstellen können.

## Anforderungen für die Konfiguration von Kerberos mit NFS

Bevor Sie Kerberos mit NFS auf Ihrem System konfigurieren, müssen Sie sicherstellen, dass bestimmte Elemente in Ihrer Netzwerk- und Speicherumgebung ordnungsgemäß konfiguriert sind.



Die Schritte zur Konfiguration Ihrer Umgebung hängen davon ab, welche Version und Art von Clientbetriebssystem, Domänencontroller, Kerberos, DNS usw. Sie verwenden. Die Dokumentation all dieser Variablen übersteigt den Rahmen dieses Dokuments. Weitere Informationen finden Sie in der entsprechenden Dokumentation zu den einzelnen Komponenten.

Ein detailliertes Beispiel, wie man ONTAP und Kerberos 5 mit NFSv3 und NFSv4 in einer Umgebung mit Windows Server 2008 R2 Active Directory und Linux Hosts einrichtet, finden Sie im technischen Bericht 4073.

Die folgenden Elemente sollten zuerst konfiguriert werden:

### Anforderungen an die Netzwerkkumgebung

- Kerberos

Sie müssen über ein funktionierendes Kerberos-Setup mit einem Key Distribution Center (KDC) verfügen, z. B. mit Windows Active Directory-basierten Kerberos oder mit Kerberos.

NFS-Server müssen sie verwenden `nfs` Als Hauptkomponente ihres Maschinentranchials.

- Verzeichnisdienst

Sie müssen einen sicheren Verzeichnisdienst in Ihrer Umgebung verwenden, z. B. Active Directory oder OpenLDAP, der für die Verwendung von LDAP über SSL/TLS konfiguriert ist.

- NTP

Sie müssen über einen Arbeitszeitserver verfügen, auf dem NTP ausgeführt wird. Dies ist notwendig, um ein Versagen der Kerberos-Authentifizierung aufgrund von Zeitverzerrung zu verhindern.

- DNS (Domain Name Resolution)

Jeder UNIX-Client und jede SVM-LIF müssen über einen entsprechenden Service-Datensatz (SRV) verfügen, der beim KDC unter „Forward and Reverse Lookup Zones“ registriert ist. Alle Teilnehmer müssen über DNS richtig lösbar sein.

- Benutzerkonten

Jeder Client muss über ein Benutzerkonto im Kerberos-Bereich verfügen. NFS-Server müssen „nfs“ als primäre Komponente ihres Machine-Principal verwenden.

### Anforderungen des NFS-Clients

- NFS

Jeder Client muss ordnungsgemäß konfiguriert sein, um mit NFSv3 oder NFSv4 über das Netzwerk zu kommunizieren.

Die Clients müssen RFC1964 und RFC2203 unterstützen.

- Kerberos

Jeder Client muss richtig konfiguriert sein, um Kerberos-Authentifizierung zu verwenden, einschließlich der folgenden Details:

- Die Verschlüsselung für TGS-Kommunikation ist aktiviert.

AES-256 für höchste Sicherheit.

- Der sicherste Verschlüsselungstyp für die TGT-Kommunikation ist aktiviert.
- Der Kerberos-Bereich und die Domäne sind korrekt konfiguriert.
- GSS ist aktiviert.

Bei Verwendung von Geräteanmeldeinformationen:

- Nicht ausführen `gssd` Mit dem `-n` Parameter.
- Nicht ausführen `kinit` Als Root-Benutzer.

- Jeder Client muss die neueste und aktualisierte Betriebssystemversion verwenden.

Dies bietet die beste Kompatibilität und Zuverlässigkeit für AES-Verschlüsselung mit Kerberos.

- DNS

Jeder Client muss richtig konfiguriert sein, damit DNS für die richtige Namensauflösung verwendet wird.

- NTP

Jeder Client muss mit dem NTP-Server synchronisiert werden.

- Host- und Domain-Informationen

Jedem Kunden `/etc/hosts` Und `/etc/resolv.conf` Dateien müssen den richtigen Host-Namen bzw. die richtigen DNS-Informationen enthalten.

- Keytab-Dateien

Jeder Client muss über eine Keytab-Datei aus dem KDC verfügen. Der Bereich muss in Großbuchstaben liegen. Der Verschlüsselungstyp muss AES-256 sein, um höchste Sicherheit zu gewährleisten.

- Optional: Für eine optimale Leistung profitieren Kunden von mindestens zwei Netzwerkschnittstellen: Eine für die Kommunikation mit dem lokalen Netzwerk und eine für die Kommunikation mit dem Speichernetzwerk.

### **Storage-Systemanforderungen**

- NFS-Lizenz

Auf dem Speichersystem muss eine gültige NFS-Lizenz installiert sein.

- CIFS-Lizenz

Die CIFS-Lizenz ist optional. Sie ist nur zum Überprüfen der Windows-Anmeldeinformationen erforderlich, wenn die Multiprotokoll-Namenszuweisung verwendet wird. In einer strikten, ausschließlich auf UNIX ausgesetzten Umgebung ist dies nicht erforderlich.

- SVM

Auf dem System muss mindestens eine SVM konfiguriert sein.

- DNS auf der SVM

Sie müssen DNS für jede SVM konfiguriert haben.

- NFS-Server

Sie müssen NFS auf der SVM konfiguriert haben.

- AES-Verschlüsselung

Für eine starke Sicherheit müssen Sie den NFS-Server so konfigurieren, dass nur AES-256-Verschlüsselung für Kerberos zugelassen ist.

- SMB Server

Falls Sie eine Multi-Protokoll-Umgebung ausführen, müssen Sie SMB für die SVM konfiguriert haben. Der SMB-Server ist für die Multiprotokoll-Namenszuweisung erforderlich.

- Volumes

Sie müssen über ein Root-Volume und mindestens ein Daten-Volume verfügen, das für die Verwendung durch die SVM konfiguriert ist.

- Root-Volume

Das Root-Volume der SVM muss über folgende Konfiguration verfügen:



Name	Einstellung
Sicherheitsstil	UNIX
UID	Root oder ID 0
GID	Root oder ID 0
UNIX-Berechtigungen	777

Im Gegensatz zum Root-Volume kann bei Daten-Volumes entweder der Sicherheitsstil genutzt werden.

- UNIX-Gruppen

Die SVM muss über die folgenden UNIX-Gruppen konfiguriert sein:

Gruppenname	Gruppen-ID
Dämon	1
Stamm	0
Pcuser	65534 (wird automatisch von ONTAP beim Erstellen der SVM erstellt)

- UNIX-Benutzer

Die SVM muss über die folgenden UNIX-Benutzer konfiguriert sein:

Benutzername	Benutzer-ID	ID der primären Gruppe	Kommentar
nfs	500	0	Erforderlich für die GSS INIT-Phase wird die erste Komponente des NFS-Client-Benutzers SPN als Benutzer verwendet.
Pcuser	65534	65534	Erforderlich für die Verwendung von NFS- und CIFS-Protokollen, die von ONTAP erstellt und der pcuser-Gruppe automatisch hinzugefügt werden, wenn Sie die SVM erstellen.
Stamm	0	0	Zur Montage erforderlich

Der nfs-Benutzer ist nicht erforderlich, wenn eine Kerberos-UNIX Namenszuweisung für das SPN des

NFS-Client-Benutzers besteht.

- Exportrichtlinien und Regeln

Sie müssen Exportrichtlinien mit den erforderlichen Exportregeln für das Root-Medium und die Daten-Volumes und qtrees konfiguriert haben. Wenn über Kerberos auf alle Volumes der SVM zugegriffen wird, können Sie die Optionen für die Exportregel festlegen `-rorule`, `-rwrule`, und `-superuser` Für das Root-Volume zu `krb5`, `krb5i`, Oder `krb5p`.

- Kerberos-UNIX-Namenszuweisung

Wenn der vom NFS-Client-Benutzer SPN identifizierte Benutzer über Root-Berechtigungen verfügen soll, müssen Sie eine Namenszuweisung zum Root erstellen.

## Verwandte Informationen

["Technischer Bericht 4073 von NetApp: Sichere einheitliche Authentifizierung"](#)

["NetApp Interoperabilitäts-Matrix-Tool"](#)

["Systemadministration"](#)

["Logisches Storage-Management"](#)

## Geben Sie die Benutzer-ID-Domäne für NFSv4 an

Um die Benutzer-ID-Domäne anzugeben, können Sie die festlegen `-v4-id-domain` Option.

### Über diese Aufgabe

Standardmäßig verwendet ONTAP die NIS-Domäne für die Zuordnung der NFSv4-Benutzer-ID, wenn eine festgelegt ist. Wenn keine NIS-Domäne festgelegt ist, wird die DNS-Domäne verwendet. Möglicherweise müssen Sie die Benutzer-ID-Domäne festlegen, wenn Sie beispielsweise mehrere Benutzer-ID-Domänen haben. Der Domänenname muss mit der Domänenkonfiguration auf dem Domänencontroller übereinstimmen. Es ist nicht für NFSv3 erforderlich.

### Schritt

1. Geben Sie den folgenden Befehl ein:

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

## Konfigurieren Sie Name Services

### Funktionsweise der Switch-Konfiguration für den ONTAP Name Service

ONTAP speichert Informationen zur Service-Konfiguration in einer Tabelle, die dem Äquivalent von entspricht `/etc/nsswitch.conf` File auf UNIX Systemen. Sie müssen die Funktion der Tabelle und deren Verwendung durch ONTAP kennen, damit Sie sie für Ihre Umgebung entsprechend konfigurieren können.

Die Switch-Tabelle für den ONTAP-Namensdienst legt fest, welche Namensdienstquellen ONTAP konsultiert, um Informationen für bestimmte Arten von Namensdienstinformationen abzurufen. Für jede SVM verwaltet

ONTAP eine separate Name-Service-Switch-Tabelle.

### Datenbanktypen

Die Tabelle enthält eine separate Namensdienstliste für jeden der folgenden Datenbanktypen:

Datenbanktyp	Definiert Namensdienstquellen für...	Gültige Quellen sind...
Hosts	Hostnamen in IP-Adressen werden konvertiert	Dateien, dns
Gruppieren	Benutzergruppeninformationen werden gesucht	Dateien, nis, ldap
Passwd	Benutzerinformationen werden gesucht	Dateien, nis, ldap
Netzgruppe	Netzgruppeninformationen werden gesucht	Dateien, nis, ldap
Namemap	Zuordnen von Benutzernamen	Dateien, ldap

### Quellentypen

Die Quellen geben an, welche Namensdienstquelle zum Abrufen der entsprechenden Informationen verwendet werden soll.

Typ der Quelle angeben...	Um Informationen zu suchen in...	Verwaltet durch die Befehlsfamilien...
Dateien	Lokale Quelldateien	<pre>vserver services name- service unix-user vserver services name-service unix-group  vserver services name- service netgroup  vserver services name- service dns hosts</pre>
nis	Externe NIS-Server, wie in der NIS-Domain-Konfiguration der SVM angegeben	<pre>vserver services name- service nis-domain</pre>
ldap	Externe LDAP-Server, wie in der LDAP-Client-Konfiguration der SVM angegeben	<pre>vserver services name- service ldap</pre>

Typ der Quelle angeben...	Um Informationen zu suchen in...	Verwaltet durch die Befehlsfamilien...
dns	Externe DNS-Server, die in der DNS-Konfiguration der SVM angegeben sind	vserver services name-service dns

Selbst wenn Sie NIS oder LDAP sowohl für den Datenzugriff als auch zur SVM-Administration-Authentifizierung verwenden möchten, sollten Sie weiterhin einschließen `files` und konfigurieren Sie lokale Benutzer als Fallback, falls die NIS- oder LDAP-Authentifizierung fehlschlägt.

#### Protokolle für den Zugriff auf externe Quellen

Für den Zugriff auf die Server für externe Quellen verwendet ONTAP die folgenden Protokolle:

Externe Servicequelle	Für den Zugriff verwendetes Protokoll
NIS	UDP
DNS	UDP
LDAP	TCP

#### Beispiel

Im folgenden Beispiel wird die Switch-Konfiguration für den Namensservice für die SVM `svm_1` angezeigt:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
          Source
Vserver   Database   Order
-----
svm_1     hosts           files,
          dns
svm_1     group           files
svm_1     passwd          files
svm_1     netgroup        nis,
          files
```

Um IP-Adressen für Hosts zu suchen, konsultiert ONTAP First lokale Quelldateien. Wenn die Abfrage keine Ergebnisse liefert, werden DNS-Server als nächstes überprüft.

Um Benutzer- oder Gruppeninformationen zu suchen, konsultiert ONTAP nur lokale Quelldateien. Wenn die Abfrage keine Ergebnisse liefert, schlägt die Suche fehl.

Um Informationen zu Netzgruppen zu suchen, konsultiert ONTAP First externe NIS-Server. Wenn die Abfrage keine Ergebnisse liefert, wird die lokale Netzgruppedatei als nächstes geprüft.

In der Tabelle für `svm_1` sind keine Namensdiensteinträge für die Namenszuweisung vorhanden. Daher konsultiert ONTAP standardmäßig nur lokale Quelldateien.

## Verwandte Informationen

["NetApp Technical Report 4668: Name Services Best Practices Guide"](#)

## LDAP verwenden

### LDAP – Übersicht

Ein LDAP-Server (Lightweight Directory Access Protocol) ermöglicht die zentrale Verwaltung von Benutzerinformationen. Wenn Sie Ihre Benutzerdatenbank auf einem LDAP-Server in Ihrer Umgebung speichern, können Sie Ihr Speichersystem so konfigurieren, dass Benutzerinformationen in Ihrer bestehenden LDAP-Datenbank angezeigt werden.

- Bevor Sie LDAP für ONTAP konfigurieren, sollten Sie überprüfen, ob die Standortbereitstellung die Best Practices für die LDAP-Server- und Client-Konfiguration erfüllt. Insbesondere sind folgende Voraussetzungen zu erfüllen:
  - Der Domänenname des LDAP-Servers muss mit dem Eintrag auf dem LDAP-Client übereinstimmen.
  - Die vom LDAP-Server unterstützten LDAP-Benutzerpasswort-Hash-Typen müssen die von ONTAP unterstützten LDAP-Benutzerpasswort-Typen enthalten:
    - CRYPT (alle Typen) und SHA-1 (SHA, SSHA).
    - Beginnend mit ONTAP 9.8, SHA-2-Hashes (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384 und SSHA-512) werden ebenfalls unterstützt.
  - Wenn für den LDAP-Server Sitzungssicherheitsmaßnahmen erforderlich sind, müssen Sie diese im LDAP-Client konfigurieren.

Folgende Sicherheitsoptionen sind verfügbar:

- LDAP-Signatur (bietet Datenintegritätsprüfung) und LDAP-Signing and Sealing (bietet Datenintegritätsprüfung und -Verschlüsselung)
- STARTEN SIE TLS
- LDAPS (LDAP über TLS oder SSL)
- Um signierte und versiegelte LDAP-Abfragen zu aktivieren, müssen die folgenden Dienste konfiguriert sein:
  - LDAP-Server müssen den GSSAPI (Kerberos) SASL-Mechanismus unterstützen.
  - LDAP-Server müssen DNS-A/AAAA-Datensätze sowie PTR-Datensätze auf dem DNS-Server eingerichtet haben.
  - Kerberos-Server müssen über SRV-Datensätze auf dem DNS-Server verfügen.
- Um TLS ODER LDAPS ZU STARTEN, sollten die folgenden Punkte berücksichtigt werden.
  - Es handelt sich hierbei um eine NetApp Best Practice, Start TLS statt LDAPS zu verwenden.
  - Bei Verwendung von LDAPS muss der LDAP-Server für TLS oder für SSL in ONTAP 9.5 und höher aktiviert sein. SSL wird in ONTAP 9.0-9.4 nicht unterstützt.
  - Ein Zertifikatsserver muss bereits in der Domäne konfiguriert sein.
- Um LDAP-Verweisungsjagd zu ermöglichen (in ONTAP 9.5 und höher), müssen die folgenden Bedingungen erfüllt sein:
  - Beide Domänen sollten mit einer der folgenden Vertrauensbeziehungen konfiguriert werden:

- Zwei-Wege
- Eine Möglichkeit, bei der der primäre vertraut auf die Empfehlungsdomäne
- Elternteil-Kind
- DNS muss so konfiguriert sein, dass alle genannten Servernamen aufgelöst werden.
- Domänenpasswörter sollten für die Authentifizierung identisch sein, wenn `--bind-as-cifs-server` Auf „true“ setzen.

Die folgenden Konfigurationen werden mit LDAP-Referenznachverfolgungsjagd nicht unterstützt.



- Für alle ONTAP-Versionen:
- LDAP-Clients auf einer Administrator-SVM
- Für ONTAP 9.8 und frühere Versionen (unterstützt ab 9.9.1):
- LDAP-Signing and Sealing (das `-session-security` Option)
- Verschlüsselte TLS-Verbindungen (das `-use-start-tls` Option)
- Kommunikation über LDAPS-Port 636 (der `-use-ldaps-for-ad-ldap` Option)

- Ab ONTAP 9.11.1 können Sie dies nutzen "[LDAP fast bind für nsswitch-Authentifizierung.](#)"
- Sie müssen beim Konfigurieren des LDAP-Clients auf der SVM ein LDAP-Schema eingeben.

In den meisten Fällen ist eines der Standard-ONTAP-Schemas angemessen. Wenn sich das LDAP-Schema in Ihrer Umgebung jedoch von diesen unterscheidet, müssen Sie ein neues LDAP-Client-Schema für ONTAP erstellen, bevor Sie den LDAP-Client erstellen. Wenden Sie sich an Ihren LDAP-Administrator, um die Anforderungen Ihrer Umgebung zu besprechen.

- Die Verwendung von LDAP für die Auflösung des Hostnamens wird nicht unterstützt.

Weitere Informationen finden Sie unter "[Technischer Bericht von NetApp 4835: Konfigurieren von LDAP in ONTAP](#)".

### LDAP-Signing- und Sealing-Konzepte

Ab ONTAP 9 können Sie Signing and Sealing konfigurieren, um die LDAP-Sitzungssicherheit bei Anfragen an einen Active Directory-Server (AD) zu aktivieren. Sie müssen die Sicherheitseinstellungen des NFS-Servers auf der Storage Virtual Machine (SVM) so konfigurieren, dass sie den auf dem LDAP-Server entsprechen.

Das Signieren bestätigt die Integrität der LDAP-Nutzlastdaten mithilfe der Geheimschlüsseltechnologie. Das Sealing verschlüsselt die LDAP-Nutzlastdaten, um das Übertragen sensibler Informationen als unverschlüsselten Text zu vermeiden. Die Option *LDAP Security Level* gibt an, ob der LDAP-Datenverkehr signiert, signiert und versiegelt werden muss oder nicht. Die Standardeinstellung lautet `none`. Test

Das LDAP-Signing and Sealing für SMB-Datenverkehr wird auf der SVM mit dem aktiviert `-session-security-for-ad-ldap` Option für die `vserver cifs security modify` Befehl.

### LDAPS-Konzepte

Sie müssen bestimmte Begriffe und Konzepte verstehen, wie ONTAP die LDAP-

Kommunikation sichert. ONTAP kann TLS ODER LDAPS STARTEN, um authentifizierte Sitzungen zwischen Active Directory-integrierten LDAP-Servern oder UNIX-basierten LDAP-Servern einzurichten.

## Terminologie

Es gibt bestimmte Begriffe, die Sie verstehen sollten, wie ONTAP LDAPS verwendet, um LDAP-Kommunikation zu sichern.

- **LDAP**

(Lightweight Directory Access Protocol) Ein Protokoll für den Zugriff auf und das Management von Informationsverzeichnissen. LDAP wird als Informationsverzeichnis zum Speichern von Objekten wie Benutzern, Gruppen und Netzwerkgruppen verwendet. LDAP bietet außerdem Verzeichnisdienste, die diese Objekte verwalten und LDAP-Anforderungen von LDAP-Clients erfüllen.

- \* SSL \*

(Secure Sockets Layer) Ein Protokoll, das zum sicheren Versenden von Informationen über das Internet entwickelt wurde. Es wurde zugunsten von TLS abgelehnt. SSL wird in ONTAP 9.0-9.4 nicht unterstützt.

- **TLS**

(Transport Layer Security) ein IETF-Standards-Protokoll, das auf den früheren SSL-Spezifikationen basiert. Es ist der Nachfolger von SSL.

- **LDAPS (LDAP über SSL oder TLS)**

Ein Protokoll, das TLS oder SSL zur sicheren Kommunikation zwischen LDAP-Clients und LDAP-Servern verwendet. Die Begriffe *LDAP über SSL* und *LDAP über TLS* werden manchmal synonym verwendet; TLS wird von ONTAP 9 und höher unterstützt, SSL wird von ONTAP 9.5 und höher unterstützt.

- In ONTAP 9.5-9.8 kann LDAPS nur auf Port 636 aktiviert werden. Verwenden Sie dazu den `-use -ldaps-for-ad-ldap` Parameter mit `vserver cifs security modify` Befehl.
- Ab ONTAP 9.9 kann LDAPS auf jedem Port aktiviert werden, obwohl Port 636 weiterhin der Standard bleibt. Stellen Sie dazu den ein `-ldaps-enabled` Parameter an `true` Und geben Sie die gewünschte an `-port` Parameter. Weitere Informationen finden Sie im `vserver services name-service ldap client create` Man-Page



Es handelt sich hierbei um eine NetApp Best Practice, Start TLS statt LDAPS zu verwenden.

- **TLS starten**

(Auch bekannt als *Start\_tls*, *STARTTLS* und *StartTLS*) Ein Mechanismus zur sicheren Kommunikation mittels TLS-Protokollen.

ONTAP verwendet STARTTLS zur Sicherung der LDAP-Kommunikation und verwendet den Standard-LDAP-Port (389) zur Kommunikation mit dem LDAP-Server. Der LDAP-Server muss so konfiguriert sein, dass Verbindungen über den LDAP-Port 389 zuzulassen. Andernfalls schlagen LDAP-TLS-Verbindungen von der SVM zum LDAP-Server fehl.

## So nutzt ONTAP LDAPS

ONTAP unterstützt die TLS-Serverauthentifizierung, sodass der SVM-LDAP-Client die Identität des LDAP-Servers während des Bindungsvorgangs bestätigen kann. TLS-fähige LDAP-Clients können mithilfe von Standardverfahren für Public-Key-Kryptografie überprüfen, ob das Zertifikat und die öffentliche ID eines Servers gültig sind und von einer Zertifizierungsstelle ausgestellt wurden, die in der Liste vertrauenswürdiger CAS des Clients aufgeführt ist.

LDAP unterstützt STARTTLS zur Verschlüsselung der Kommunikation mit TLS. STARTTLS beginnt als Klartext-Verbindung über den Standard-LDAP-Port (389) und wird dann auf TLS aktualisiert.

ONTAP unterstützt Folgendes:

- LDAPS für SMB-bezogenen Datenverkehr zwischen den durch Active Directory integrierten LDAP-Servern und der SVM
- LDAPS für LDAP-Datenverkehr für Namenszuweisung und andere UNIX-Informationen

Entweder in Active Directory integrierte LDAP-Server oder UNIX-basierte LDAP-Server können zum Speichern von Informationen für die LDAP-Namenszuweisung und andere UNIX-Informationen verwendet werden, z. B. Benutzer, Gruppen und Netzwerkgruppen.

- Selbstsignierte Root-CA-Zertifikate

Bei Verwendung eines in Active Directory integrierten LDAP wird das selbstsignierte Stammzertifikat generiert, wenn der Windows Server Certificate Service in der Domäne installiert wird. Bei Verwendung eines UNIX-basierten LDAP-Servers zur LDAP-Namenszuweisung wird das selbstsignierte Stammzertifikat generiert und unter Verwendung der für diese LDAP-Anwendung geeigneten Mittel gespeichert.

LDAPS ist standardmäßig deaktiviert.

### Aktivieren Sie die LDAP RFC2307bis-Unterstützung

Wenn Sie LDAP verwenden möchten und die zusätzliche Funktion benötigen, um geschachtelte Gruppenmitgliedschaften zu verwenden, können Sie ONTAP so konfigurieren, dass LDAP RFC2307bis Unterstützung aktiviert wird.

### Was Sie benötigen

Sie müssen eine Kopie eines der Standard-LDAP-Client-Schemas erstellt haben, die Sie verwenden möchten.

### Über diese Aufgabe

In LDAP-Client-Schemata verwenden Gruppenobjekte das Attribut `memberUid`. Dieses Attribut kann mehrere Werte enthalten und listet die Namen der Benutzer auf, die zu dieser Gruppe gehören. In RFC2307bis aktivierten LDAP-Client-Schemas verwenden Gruppenobjekte das Attribut `uniqueMember`. Dieses Attribut kann den vollständigen Distinguished Name (DN) eines anderen Objekts im LDAP-Verzeichnis enthalten. Damit können Sie verschachtelte Gruppen verwenden, da Gruppen andere Gruppen als Mitglieder haben können.

Der Benutzer darf nicht Mitglied von mehr als 256 Gruppen einschließlich verschachtelter Gruppen sein. ONTAP ignoriert alle Gruppen über das 256 Gruppenlimit.

Standardmäßig ist die Unterstützung von RFC2307bis deaktiviert.





Die Unterstützung von RFC2307bis wird in ONTAP automatisch aktiviert, wenn ein LDAP-Client mit dem MS-AD-bis-Schema erstellt wird.

Weitere Informationen finden Sie unter ["Technischer Bericht von NetApp 4835: Konfigurieren von LDAP in ONTAP"](#).

### Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Ändern Sie das kopierte RFC2307 LDAP-Client-Schema, um die Unterstützung von RFC2307bis zu aktivieren:

```
vserver services name-service ldap client schema modify -vserver vserver_name  
-schema schema-name -enable-rfc2307bis true
```

3. Ändern Sie das Schema so, dass es mit der im LDAP-Server unterstützten Objektklasse übereinstimmt:

```
vserver services name-service ldap client schema modify -vserver vserver-name  
-schema schema_name -group-of-unique-names-object-class object_class
```

4. Ändern Sie das Schema so, dass es mit dem im LDAP-Server unterstützten Attributnamen übereinstimmt:

```
vserver services name-service ldap client schema modify -vserver vserver-name  
-schema schema_name -unique-member-attribute attribute_name
```

5. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

### Konfigurationsoptionen für LDAP-Verzechnissuches

Sie können LDAP-Verzechnissuches, einschließlich Benutzer-, Gruppen- und Netzwerkgruppeninformationen, optimieren, indem Sie den ONTAP LDAP-Client so konfigurieren, dass eine Verbindung zu LDAP-Servern auf die für Ihre Umgebung am besten geeignete Weise hergestellt wird. Sie müssen wissen, wann die Standard-LDAP-Basis- und Bereichssuche ausreichen und welche Parameter angegeben werden sollen, wenn benutzerdefinierte Werte besser geeignet sind.

LDAP-Client-Suchoptionen für Benutzer-, Gruppen- und Netzwerkgruppeninformationen können dazu beitragen, fehlerhafte LDAP-Abfragen zu vermeiden, und damit einen fehlgeschlagenen Client-Zugriff auf Speichersysteme. Sie tragen außerdem dazu bei, dass die Suchvorgänge so effizient wie möglich sind, um Probleme mit der Client-Performance zu vermeiden.

### Standardwerte für die Basis- und Bereichssuche

Die LDAP-Basis ist der Standard-Basis-DN, den der LDAP-Client zur Durchführung von LDAP-Abfragen verwendet. Alle Suchvorgänge, einschließlich Benutzer-, Gruppen- und Netgroup-Suchen, werden mit dem Basis-DN durchgeführt. Diese Option ist geeignet, wenn Ihr LDAP-Verzeichnis relativ klein ist und alle relevanten Einträge im selben DN liegen.

Wenn Sie keinen benutzerdefinierten Basis-DN angeben, ist die Standardeinstellung `root`. Das bedeutet, dass jede Abfrage das gesamte Verzeichnis durchsucht. Dies maximiert zwar die Erfolgsaussichten der LDAP-Abfrage, kann aber ineffizient sein und bei großen LDAP-Verzeichnissen zu einer deutlich geringeren Leistung führen.

Der Umfang der LDAP-Basis ist der Standard-Suchumfang, den der LDAP-Client zur Durchführung von LDAP-Abfragen verwendet. Alle Suchvorgänge, einschließlich Benutzer-, Gruppen- und Netgroup-Suchen, werden mit dem Basisumfang durchgeführt. Es legt fest, ob die LDAP-Abfrage nur den benannten Eintrag durchsucht, eine Ebene unterhalb des DN eingibt oder die gesamte Unterstruktur unter dem DN.

Wenn Sie keinen benutzerdefinierten Basisbereich angeben, wird der Standardwert verwendet `subtree`. Das bedeutet, dass jede Abfrage die gesamte Unterstruktur unter dem DN durchsucht. Dies maximiert zwar die Erfolgsaussichten der LDAP-Abfrage, kann aber ineffizient sein und bei großen LDAP-Verzeichnissen zu einer deutlich geringeren Leistung führen.

### Benutzerdefinierte Basis- und Bereichssuche

Optional können Sie separate Basis- und Bereichswerte für Benutzer-, Gruppen- und Netzgruppensuchen festlegen. Eine Begrenzung der Such-Basis und des Umfangs von Abfragen auf diese Weise kann die Leistung erheblich verbessern, da die Suche auf einen kleineren Unterabschnitt des LDAP-Verzeichnisses beschränkt wird.

Wenn Sie benutzerdefinierte Basis- und Bereichswerte angeben, überschreiben sie die allgemeine Standardsuchbasis und den Umfang für Benutzer-, Gruppen- und Netzgruppensuchen. Die Parameter zum Festlegen benutzerdefinierter Basis- und Bereichswerte sind auf der erweiterten Berechtigungsebene verfügbar.

LDAP-Client-Parameter...	Gibt Benutzerdefiniert an...
<code>-base-dn</code>	Basis-DN für alle LDAP-Suche bei Bedarf können mehrere Werte eingegeben werden (z. B. wenn LDAP-Weiterleitung in ONTAP 9.5 und späteren Versionen aktiviert ist).
<code>-base-scope</code>	Basisumfang für alle LDAP-Suchvorgänge
<code>-user-dn</code>	Basis-DNS für alle LDAP-Benutzersuche Dieser Parameter gilt auch für die Suche nach Benutzernamen.
<code>-user-scope</code>	Basisumfang für alle LDAP-Benutzersuchen dieser Parameter gilt auch für die Suche nach dem User Name-Mapping.
<code>-group-dn</code>	Basis-DNS für alle LDAP-Gruppensuchen
<code>-group-scope</code>	Basisumfang für alle LDAP-Gruppensuchen
<code>-netgroup-dn</code>	Basis-DNS für alle LDAP-Netzgruppensuche
<code>-netgroup-scope</code>	Basisumfang für alle LDAP-Netzgruppensuche

## Mehrere benutzerdefinierte Basis-DN-Werte

Wenn Ihre LDAP-Verzeichnisstruktur komplexer ist, ist es möglicherweise erforderlich, dass Sie mehrere Basis-DNS angeben, um mehrere Teile Ihres LDAP-Verzeichnisses nach bestimmten Informationen zu durchsuchen. Sie können mehrere DNS für die DN-Parameter Benutzer, Gruppen und Netzwerkgruppen festlegen, indem Sie diese mit einem Semikolon (;) trennen und die gesamte DN-Suchliste mit doppelten Anführungszeichen (") schließen. Wenn ein DN ein Semikolon enthält, müssen Sie unmittelbar vor dem Semikolon im DN ein Escape-Zeichen (\) hinzufügen.

Der Umfang gilt für die gesamte für den entsprechenden Parameter angegebene DNS-Liste. Wenn Sie beispielsweise eine Liste mit drei verschiedenen Benutzer-DNS und Unterstrukturen für den Benutzerbereich angeben, sucht der LDAP-Benutzer die gesamte Unterstruktur für jedes der drei angegebenen DNS.

Ab ONTAP 9.5 können Sie auch LDAP *Referral Chasing* angeben, wodurch der ONTAP LDAP-Client Look-up-Anfragen an andere LDAP-Server weiterleiten kann, wenn keine LDAP-Referral-Antwort vom primären LDAP-Server zurückgegeben wird. Der Client verwendet diese Verweisdaten, um das Zielobjekt vom in den Empfehlungsdaten beschriebenen Server abzurufen. Um nach Objekten zu suchen, die in den genannten LDAP-Servern vorhanden sind, kann der Basis-dn der genannten Objekte im Rahmen der LDAP-Client-Konfiguration dem Basis-dn hinzugefügt werden. Referenzobjekte werden jedoch nur dann gesucht, wenn die Verweisungsjagd aktiviert ist (mit dem `-referral-enabled true` Option) während der Erstellung oder Änderung von LDAP-Clients.

## Verbesserung der Performance von LDAP-Verzeichnis Netzgroup-by-Host-Suchen

Wenn Ihre LDAP-Umgebung so konfiguriert ist, dass sie Netgroup-by-Host-Suchen zuzulassen, können Sie ONTAP so konfigurieren, dass sie dies nutzt und Netgroup-by-Host-Suchen durchführen. Dies kann die Netgroup-Suche erheblich beschleunigen und mögliche Probleme beim NFS-Client-Zugriff aufgrund der Latenz bei der Suche in einer Netzgruppe verringern.

### Was Sie benötigen

Ihr LDAP-Verzeichnis muss ein enthalten `netgroup.byhost` Zuordnen:

Ihre DNS-Server sollten sowohl vorwärts (A) als auch rückwärts (PTR) Suchdatensätze für NFS-Clients enthalten.

Wenn Sie IPv6-Adressen in Netzgruppen angeben, müssen Sie jede Adresse wie in RFC 5952 angeben kürzen und komprimieren.

### Über diese Aufgabe

NIS-Server speichern Netzwerkgruppeninformationen in drei separaten, so genannten Zuordnungen `netgroup`, `netgroup.byuser`, und `netgroup.byhost`. Der Zweck des `netgroup.byuser` Und `netgroup.byhost` Karten sollen die Suche in Netzgruppen beschleunigen. ONTAP führt Netgroup-by-Host-Suchen auf NIS Servern durch und verbessert so die Mount-Reaktionszeiten.

LDAP-Verzeichnisse verfügen standardmäßig nicht über eine solche `netgroup.byhost` Zuordnung wie NIS-Server Es ist jedoch möglich, mit Hilfe von Drittanbieter-Tools einen NIS zu importieren `netgroup.byhost` In LDAP-Verzeichnissen zuordnen, um schnelle netzgruppenspezifische Suche zu ermöglichen. Wenn Sie Ihre LDAP-Umgebung so konfiguriert haben, dass sie Netgroup-by-Host-Suchen zulässt, können Sie den ONTAP LDAP-Client mit dem konfigurieren `netgroup.byhost` Kartenname, DN und Suchumfang für schnellere Suche nach Netzgruppen nach Host.

Wenn ONTAP die Ergebnisse für netzgruppenspezifische Host-Suchen schneller erhalten, kann Exportregeln

schneller verarbeiten, wenn NFS-Clients Zugriff auf Exporte anfordern. Dies verringert die Wahrscheinlichkeit eines verzögerten Zugriffs aufgrund von Latenzproblemen bei der netgroup-Suche.

## Schritte

1. Holen Sie sich den genauen vollständigen Distinguished Name des NIS netgroup.byhost Zuordnung, die Sie in Ihr LDAP-Verzeichnis importiert haben.

Der map-DN kann je nach dem Werkzeug eines Drittanbieters variieren, das Sie für den Import verwendet haben. Um eine optimale Leistung zu erzielen, sollten Sie den genauen MAP-DN angeben.

2. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
3. Aktivieren von netgroup-by-Host-Suchen in der LDAP-Client-Konfiguration der Storage Virtual Machine (SVM): `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost -dn netgroup-by-host_map_distinguished_name -netgroup-byhost-scope netgroup-by-host_search_scope`

`-is-netgroup-byhost-enabled {true false}` Aktiviert oder deaktiviert die netgroup-by-Host-Suche nach LDAP-Verzeichnissen. Die Standardeinstellung lautet `false`.

`-netgroup-byhost-dn netgroup-by-host_map_distinguished_name` Gibt den Distinguished Name des an netgroup.byhost Zuordnung im LDAP-Verzeichnis Es überschreibt den Basis-DN für Netgroup-by-Host-Suchen. Wenn Sie diesen Parameter nicht angeben, verwendet ONTAP stattdessen den Basis-DN.

`-netgroup-byhost-scope {base|onelevel subtree}` Gibt den Suchumfang für Netgroup-by-Host-Suchen an. Wenn Sie diesen Parameter nicht angeben, wird der Standardwert verwendet `subtree`.

Wenn die LDAP-Client-Konfiguration noch nicht vorhanden ist, können Sie Netgroup-by-Host-Suchen aktivieren, indem Sie diese Parameter angeben, wenn Sie eine neue LDAP-Client-Konfiguration mit dem erstellen `vserver services name-service ldap client create` Befehl.



Ab ONTAP 9.2 Field Portal `-ldap-servers` Ersetzt das Feld `-servers`. Dieses neue Feld kann entweder einen Hostnamen oder eine IP-Adresse für den LDAP-Server verwenden.

4. Zurück zur Administratorberechtigungsebene: `set -privilege admin`

## Beispiel

Mit dem folgenden Befehl wird die vorhandene LDAP-Client-Konfiguration „ldap\_corp“ geändert, um netgroup-by-Host-Suchen mit dem zu aktivieren netgroup.byhost Zuordnung mit dem Namen „nisMapName=„netgroup.byhost“,dc=corp,dc=example,dc=com“ und Standardsuchumfang subtree:

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

## Nachdem Sie fertig sind

Der netgroup.byhost Und netgroup Karten im Verzeichnis müssen stets synchron gehalten werden, um Clientzugriffsprobleme zu vermeiden.

## Verwandte Informationen

["IETF RFC 5952: Eine Empfehlung für die IPv6-Adresstext-Darstellung"](#)

### Verwenden Sie LDAP fast bind für die nswitch-Authentifizierung

Ab ONTAP 9.11.1 können Sie die LDAP *fast BIND*-Funktionalität (auch bekannt als *Concurrent BIND*) für schnellere und einfachere Clientauthentifizierungsanforderungen nutzen. Um diese Funktion nutzen zu können, muss der LDAP-Server die Funktion für schnelles Binden unterstützen.

### Über diese Aufgabe

Ohne schnelle Bindung verwendet ONTAP eine einfache LDAP-Bindung, um Administratorbenutzer mit dem LDAP-Server zu authentifizieren. Mit dieser Authentifizierungsmethode sendet ONTAP einen Benutzer- oder Gruppennamen an den LDAP-Server, empfängt das gespeicherte Hash-Passwort und vergleicht den Server-Hash-Code mit dem lokal aus dem Benutzerpasswort generierten Hash-Passcode. Sind sie identisch, gewährt ONTAP eine Anmeldegenehmigung.

Mit der F.A.S.T. BIND-Funktion sendet ONTAP über eine sichere Verbindung nur Benutzeranmeldeinformationen (Benutzername und Passwort) an den LDAP-Server. Der LDAP-Server validiert diese Anmeldedaten dann und weist ONTAP an, die Anmeldeberechtigungen zu erteilen.

Ein Vorteil von fast bind besteht darin, dass ONTAP nicht jeden neuen Hashing-Algorithmus unterstützt, der von LDAP-Servern unterstützt wird, unterstützen muss, da das Passwort-Hashing vom LDAP-Server durchgeführt wird.

["Erfahren Sie mehr über die Verwendung von fast Bind."](#)

Vorhandene LDAP-Clientkonfigurationen können für LDAP fast Binding verwendet werden. Es wird jedoch dringend empfohlen, den LDAP-Client für TLS oder LDAPS zu konfigurieren; andernfalls wird das Passwort im Klartext über das Kabel gesendet.

Zur Aktivierung der LDAP-F.A.S.T.-Bindung in einer ONTAP-Umgebung müssen Sie folgende Anforderungen erfüllen:

- ONTAP-Admin-Benutzer müssen auf einem LDAP-Server konfiguriert werden, der schnelle Bindungen unterstützt.
- Die ONTAP SVM muss für LDAP in der Name Services Switch (nswitch)-Datenbank konfiguriert sein.
- ONTAP-Admin-Benutzer- und Gruppenkonten müssen für nswitch-Authentifizierung mit fast-BIND konfiguriert werden.

### Schritte

1. Bestätigen Sie mit Ihrem LDAP-Administrator, dass LDAP fast BIND auf dem LDAP-Server unterstützt wird.
2. Stellen Sie sicher, dass die Anmeldedaten für ONTAP-Admin-Benutzer auf dem LDAP-Server konfiguriert sind.
3. Vergewissern Sie sich, dass der Administrator oder die Daten-SVM für LDAP fast bind richtig konfiguriert sind.
  - a. Um zu bestätigen, dass der LDAP fast BIND-Server in der LDAP-Client-Konfiguration aufgeführt ist, geben Sie Folgendes ein:

```
vserver services name-service ldap client show
```

["Weitere Informationen zur LDAP-Client-Konfiguration."](#)

- b. Um das zu bestätigen `ldap` ist eine der konfigurierten Quellen für den `nswitch passwd` Datenbank, geben Sie ein:

```
vserver services name-service ns-switch show
```

["Weitere Informationen zur nswitch-Konfiguration."](#)

4. Stellen Sie sicher, dass Administratorbenutzer mit `nswitch` authentifizieren und die LDAP-Authentifizierung für die schnelle Bindung in ihren Konten aktiviert ist.
  - Geben Sie für bestehende Benutzer ein `security login modify` Und überprüfen Sie die folgenden Parametereinstellungen:

```
-authentication-method nswitch
```

```
-is-ldap-fastbind true
```

- Informationen zu neuen Admin-Benutzern finden Sie unter ["Aktivieren Sie den LDAP- oder NIS-Kontozugriff."](#)

#### **Zeigt LDAP-Statistiken an**

Ab ONTAP 9.2 können Sie LDAP-Statistiken für Storage Virtual Machines (SVMs) auf einem Storage-System anzeigen, um die Performance zu überwachen und Probleme zu diagnostizieren.

#### **Was Sie benötigen**

- Sie müssen einen LDAP-Client auf der SVM konfiguriert haben.
- Sie müssen LDAP-Objekte identifiziert haben, von denen Sie Daten anzeigen können.

#### **Schritt**

1. Performance-Daten für Zählerobjekte anzeigen:

```
statistics show
```

#### **Beispiele**

Das folgende Beispiel zeigt die Performance-Daten für das Objekt `secd_external_service_op`:

```
cluster::*> statistics show -vserver vserverName -object
secd_external_service_op -instance "vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1"
```

```
Object: secd_external_service_op
Instance: vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1
Start-time: 4/13/2016 22:15:38
End-time: 4/13/2016 22:15:38
Scope: vserverName
```

Counter	Value
instance_name	vserverName:LDAP (NIS & Name Mapping):GetUserInfoFromName: 1.1.1.1
last_modified_time	1460610787
node_name	nodeName
num_not_found_responses	1
num_request_failures	1
num_requests_sent	1
num_responses_received	1
num_successful_responses	0
num_timeouts	0
operation	GetUserInfoFromName
process_name	secd
request_latency	52131us

## Konfigurieren Sie Namenszuordnungen

### Übersicht über Namenszuordnungen konfigurieren

ONTAP verwendet Namenszuweisung, um SMB-Identitäten UNIX-Identitäten, Kerberos-Identitäten und UNIX-Identitäten den SMB-Identitäten zuzuordnen. Die IT benötigt diese Informationen, um Benutzeranmeldeinformationen zu erhalten und ordnungsgemäßen Dateizugriff bereitzustellen, unabhängig davon, ob sie eine Verbindung von einem NFS-Client oder einem SMB-Client herstellen.

Es gibt zwei Ausnahmen, in denen Sie keine Namenszuweisung verwenden müssen:

- Sie konfigurieren eine reine UNIX-Umgebung und planen keinen SMB-Zugriff oder NTFS-Sicherheitsstil auf Volumes.
- Sie konfigurieren stattdessen den Standardbenutzer für die Verwendung.

In diesem Szenario ist keine Namenszuweisung erforderlich, da anstelle der Zuordnung aller einzelnen Client-Anmeldeinformationen alle Client-Anmeldeinformationen demselben Standardbenutzer zugeordnet werden.

Beachten Sie, dass Sie die Namenszuordnung nur für Benutzer und nicht für Gruppen verwenden können.

Sie können jedoch einem bestimmten Benutzer eine Gruppe von einzelnen Benutzern zuordnen. Sie können beispielsweise alle AD-Benutzer, die mit DEM Wort „VERTRIEB“ beginnen oder enden, einem bestimmten UNIX-Benutzer und der UID des Benutzers zuordnen.

### **Funktionsweise der Namenszuweisung**

Wenn ONTAP Anmeldeinformationen für einen Benutzer zuordnen muss, überprüft er zunächst die Datenbank für die Zuordnung von lokalen Namen und den LDAP-Server auf eine vorhandene Zuordnung. Überprüft wird, ob ein oder beide Einstellungen überprüft werden und in welcher Reihenfolge durch die Name-Service-Konfiguration der SVM bestimmt wird.

- Für die Zuordnung von Windows zu UNIX

Wenn keine Zuordnung gefunden wird, überprüft ONTAP, ob der kleine Windows-Benutzername ein gültiger Benutzername in der UNIX-Domäne ist. Wenn dies nicht funktioniert, wird der Standard-UNIX-Benutzer verwendet, sofern er konfiguriert ist. Wenn der standardmäßige UNIX-Benutzer nicht konfiguriert ist und ONTAP auf diese Weise keine Zuordnung erhalten kann, schlägt die Zuordnung fehl und es wird ein Fehler zurückgegeben.

- Für die Zuordnung von UNIX zu Windows

Wenn keine Zuordnung gefunden wird, versucht ONTAP, ein Windows-Konto zu finden, das dem UNIX-Namen in der SMB-Domäne entspricht. Wenn dies nicht funktioniert, wird der SMB-Standardbenutzer verwendet, vorausgesetzt, er ist konfiguriert. Wenn der SMB-Standardbenutzer nicht konfiguriert ist und ONTAP auch keine Zuordnung auf diese Weise erhalten kann, schlägt die Zuordnung fehl und es wird ein Fehler zurückgegeben.

Computerkonten sind standardmäßig dem angegebenen UNIX-Standardbenutzer zugeordnet. Wenn kein UNIX-Standardbenutzer angegeben ist, schlägt die Zuordnung des Computerkontos fehl.

- Ab ONTAP 9.5 können Sie Computerkonten anderen Benutzern als dem standardmäßigen UNIX-Benutzer zuordnen.
- In ONTAP 9.4 und früher können Sie Computerkonten nicht anderen Benutzern zuordnen.

Auch wenn Namenszuordnungen für Computerkonten definiert sind, werden die Zuordnungen ignoriert.

### **Multidomain sucht nach Zuordnungen von UNIX-Benutzern zu Windows-Benutzernamen**

ONTAP unterstützt Multidomain-Suchen beim Zuordnen von UNIX-Benutzern zu Windows-Benutzern. Alle erkannten vertrauenswürdigen Domänen werden nach Übereinstimmungen mit dem Ersatzmuster gesucht, bis ein passendes Ergebnis zurückgegeben wird. Alternativ können Sie eine Liste der bevorzugten vertrauenswürdigen Domänen konfigurieren, die anstelle der Liste der erkannten vertrauenswürdigen Domänen verwendet wird und bis zur Rückgabe eines übereinstimmenden Ergebnisses durchsucht wird.



## Wie Domain Trusts sich auf UNIX-Benutzer bei der Suche nach der Windows-User Name Mapping auswirken

Um zu verstehen, wie die Zuordnung von Benutzernamen mit mehreren Domänen funktioniert, müssen Sie verstehen, wie Domain Trusts mit ONTAP arbeiten. Active Directory-Vertrauensbeziehungen mit der Home-Domain des SMB-Servers können ein bidirektionales Vertrauen sein oder eine von zwei Arten von unidirektionalen Trusts sein, entweder ein eingehendes Vertrauen oder ein ausgehendes Vertrauen. Die Home-Domäne ist die Domäne, zu der der SMB-Server der SVM gehört.

- *Bidirektionales Vertrauen*

Bei bidirektionalen Trusts vertrauen sich beide Domänen gegenseitig. Wenn die Home-Domain des SMB-Servers bidirektional mit einer anderen Domain vertraut ist, kann die Home-Domain einen Benutzer authentifizieren und autorisieren, der der vertrauenswürdigen Domain angehört, und umgekehrt.

Die Suche nach der Zuordnung von UNIX-Benutzern zu Windows-Benutzernamen kann nur auf Domänen mit bidirektionalen Vertrauensstellungen zwischen der Home-Domain und der anderen Domain ausgeführt werden.

- *Outbound Trust*

Mit einem ausgehenden Vertrauen vertraut die Home Domain der anderen Domain. In diesem Fall kann die Home-Domain einen Benutzer authentifizieren und autorisieren, der der vertrauenswürdigen Outbound-Domäne angehört.

Eine Domäne mit einem abgehenden Vertrauen in die Home-Domäne wird beim Durchführen der Suche nach UNIX-Benutzern zu Windows-Benutzernamenzuordnung *not* durchsucht.

- *Inbound Trust*


Mit einem eingehenden Vertrauen vertraut die andere Domäne auf die Home Domain des SMB-Servers. In diesem Fall kann die Home-Domäne einen Benutzer der eingehenden vertrauenswürdigen Domäne nicht authentifizieren oder autorisieren.

Eine Domäne mit einem eingehenden Vertrauen in die Home-Domäne wird beim Durchführen der Suche nach UNIX-Benutzern bei der Zuordnung von Windows-Benutzernamen *Not* durchsucht.

## Wie Platzhalter (\*) zum Konfigurieren von Mehrfachdomain-Suchen für das Namenszuordnungen verwendet werden

Suchvorgänge für die Zuordnung von Mehrfachdomänen werden durch die Verwendung von Wildcards im Domain-Bereich des Windows-Benutzernamens erleichtert. In der folgenden Tabelle wird veranschaulicht, wie Wildcards im Domain-Teil eines Namenszuordnungseintrags verwendet werden, um Mehrfachdomain-Suchen zu ermöglichen:

Muster	Austausch	Ergebnis
Stamm	{Sternchen}{umgekehrter Schrägstrich}Administrator	Der UNIX-Benutzer „root“ ist dem Benutzer „Administrator“ zugeordnet. Alle vertrauenswürdigen Domains werden so lange durchsucht, bis der erste übereinstimmende Benutzer namens „Administrator“ gefunden wurde.

Muster	Austausch	Ergebnis
*	{Sternchen}{umgekehrter Schrägstrich}\{Sternchen}	<p>Gültige UNIX-Benutzer werden den entsprechenden Windows-Benutzern zugeordnet. Alle vertrauenswürdigen Domänen werden so lange durchsucht, bis der erste übereinstimmende Benutzer mit diesem Namen gefunden wurde.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>Das Muster <code>*\*</code> ist nur für die Namenszuweisung von UNIX zu Windows gültig, nicht umgekehrt.</p> </div>

### Durchführen von Suchvorgängen mit mehreren Domänen

Sie können eine von zwei Methoden wählen, um die Liste der vertrauenswürdigen Domänen zu bestimmen, die für die Suche nach Namen mehrerer Domänen verwendet werden:

- Verwenden Sie die automatisch erkannte bidirektionale Vertrauensliste, die von ONTAP erstellt wurde
- Verwenden Sie die Liste der bevorzugten vertrauenswürdigen Domänen, die Sie kompilieren

Wenn ein UNIX-Benutzer einem Windows-Benutzer mit einem Platzhalter zugeordnet ist, der für den Domain-Abschnitt des Benutzernamens verwendet wird, wird der Windows-Benutzer in allen vertrauenswürdigen Domänen wie folgt angezeigt:

- Wenn eine bevorzugte Liste der vertrauenswürdigen Domäne konfiguriert ist, wird der zugeordnete Windows-Benutzer nur in dieser Suchliste in der entsprechenden Reihenfolge angezeigt.
- Wenn eine bevorzugte Liste der vertrauenswürdigen Domänen nicht konfiguriert ist, wird der Windows-Benutzer in allen bidirektionalen vertrauenswürdigen Domänen der Home-Domäne gesucht.
- Wenn es keine bidirektional vertrauenswürdigen Domänen für die Home-Domain gibt, wird der Benutzer in der Home-Domain angezeigt.

Wenn ein UNIX-Benutzer einem Windows-Benutzer ohne Domain-Abschnitt im Benutzernamen zugeordnet ist, wird der Windows-Benutzer in der Home-Domain angezeigt.

### Konvertierungsregeln für Namenszuordnungen

Ein ONTAP System behält eine Reihe von Konversionsregeln für jede SVM bei. Jede Regel besteht aus zwei Teilen: Einem *pattern* und einem *Replacement*. Konvertierungen beginnen am Anfang der entsprechenden Liste und führen eine Substitution basierend auf der ersten übereinstimmenden Regel durch. Das Muster ist ein normaler Ausdruck im UNIX-Stil. Der Ersatz ist eine Zeichenkette, die Escape-Sequenzen enthält, die Unterausdrücke aus dem Muster darstellen, wie im UNIX `sed` Programm.

## Erstellen einer Namenszuweisung

Sie können das verwenden `vserver name-mapping create` Befehl zum Erstellen einer Namenszuweisung. Sie verwenden Namenszuordnungen, um Windows-Benutzern den Zugriff auf UNIX-Sicherheitsstil-Volumes zu ermöglichen und umgekehrt.

### Über diese Aufgabe

Für jede SVM unterstützt ONTAP bis zu 12,500 Namenszuordnungen für jede Richtung.

### Schritt

1. Erstellen einer Namenszuweisung:

```
vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-unix|unix-win} -position integer -pattern text -replacement text
```



Der `-pattern` Und `-replacement` Aussagen können als reguläre Ausdrücke formuliert werden. Sie können auch die verwenden `-replacement` Anweisung, eine Zuordnung zum Benutzer durch Verwendung der leeren Ersatzzeichenfolge explizit zu verweigern " " (Das Leerzeichen). Siehe `vserver name-mapping create` Man-Page für Details.

Beim Erstellen von Windows-zu-UNIX-Zuordnungen müssen sich alle SMB-Clients, die zum Zeitpunkt der Erstellung der neuen Zuordnungen offene Verbindungen zum ONTAP System haben, abmelden und zurück anmelden, um die neuen Zuordnungen zu sehen.

### Beispiele

Mit dem folgenden Befehl wird eine Namenszuweisung auf der SVM mit dem Namen `vs1` erstellt. Die Zuordnung ist eine Zuordnung von UNIX zu Windows an Position 1 in der Prioritätenliste. Das Mapping ordnet den UNIX-Benutzer `john` dem Windows-Benutzer `eng\JohnDoe` zu.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern john
-replacement "ENG\\JohnDoe"
```

Mit dem folgenden Befehl wird eine weitere Namenszuweisung auf der SVM mit dem Namen `vs1` erstellt. Die Zuordnung ist eine Zuordnung von Windows zu UNIX an Position 1 in der Prioritätenliste. Hier sind Muster und Ersatz enthalten reguläre Ausdrücke. Das Mapping ordnet jedem CIFS-Benutzer in der Domäne `eng` Benutzern in der mit der SVM verknüpften LDAP-Domäne zu.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\\1"
```

Mit dem folgenden Befehl wird eine weitere Namenszuweisung auf der SVM mit dem Namen `vs1` erstellt. Hier enthält das Muster „`€“ als Element im Windows-Benutzernamen, das entkommen sein muss. Das Mapping ordnet den Windows-Benutzer `eng\john€3ps` dem UNIX-Benutzer `john OPS` zu.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

## Konfigurieren Sie den Standardbenutzer

Sie können einen Standardbenutzer so konfigurieren, dass er verwendet wird, wenn alle anderen Zuordnungsversuche für einen Benutzer fehlschlagen oder wenn Sie nicht einzelne Benutzer zwischen UNIX und Windows zuordnen möchten. Wenn die Authentifizierung von nicht zugeordneten Benutzern fehlschlägt, sollten Sie keinen Standardbenutzer konfigurieren.

### Über diese Aufgabe

Wenn Sie bei der CIFS-Authentifizierung nicht jeden Windows-Benutzer einem einzelnen UNIX-Benutzer zuordnen möchten, können Sie stattdessen einen standardmäßigen UNIX-Benutzer festlegen.

Wenn Sie bei der NFS-Authentifizierung nicht jeden UNIX-Benutzer einem einzelnen Windows-Benutzer zuordnen möchten, können Sie stattdessen einen standardmäßigen Windows-Benutzer festlegen.

### Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den folgenden Befehl ein...
Konfigurieren Sie den UNIX-Standardbenutzer	<code>vserver cifs options modify -default-unix-user user_name</code>
Konfigurieren Sie den Windows-Standardbenutzer	<code>vserver nfs modify -default-win-user user_name</code>

## Befehle zum Verwalten von Name-Zuordnungen

Zum Verwalten von Name-Zuordnungen gibt es bestimmte ONTAP-Befehle.

Ihr Ziel ist	Befehl
Erstellen einer Namenszuweisung	<code>vserver name-mapping create</code>
Eine Namenszuordnung an einer bestimmten Position einfügen	<code>vserver name-mapping insert</code>
Namenszuordnungen anzeigen	<code>vserver name-mapping show</code>

Tauschen Sie die Position zweier Namenszuordnungen AUS HINWEIS: Ein Austausch ist nicht zulässig, wenn das Namenszuordnungen mit einem ip-Qualifier-Eintrag konfiguriert ist.	<code>vserver name-mapping swap</code>
Ändern einer Namenszuweisung	<code>vserver name-mapping modify</code>
Löschen einer Namenszuweisung	<code>vserver name-mapping delete</code>
Überprüfen Sie die richtige Namenszuweisung	<code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code>

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

## Zugriff für Windows NFS-Clients aktivieren

ONTAP unterstützt Dateizugriff über Windows NFSv3-Clients. Das bedeutet, dass Clients, die Windows Betriebssysteme mit NFSv3 Unterstützung ausführen, jetzt auf Dateien von NFSv3 Exports auf dem Cluster zugreifen können. Um diese Funktion erfolgreich zu nutzen, müssen Sie die Storage Virtual Machine (SVM) richtig konfigurieren und bestimmte Anforderungen und Einschränkungen beachten.

### Was Sie benötigen

NFSv3 muss auf der SVM aktiviert sein.

### Über diese Aufgabe

Standardmäßig ist die Unterstützung für Windows NFSv3-Clients deaktiviert.

Windows-NFSv3-Clients unterstützen das NSM-Protokoll (Network Status Monitor) nicht. Aus diesem Grund können Windows NFSv3-Client-Sessions u. U. Unterbrechungen beim Storage Failover und bei der Verschiebung von Volumes auftreten.

### Schritte

1. Unterstützung für Windows NFSv3-Clients aktivieren:

```
vserver nfs modify -vserver vserver_name -v3-ms-dos-client enabled
```

2. Deaktivieren Sie auf allen SVMs, die Windows NFSv3-Clients unterstützen, das `-enable-ejukebox` Und `-v3-connection-drop` Parameter: `vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection-drop disabled`

Windows NFSv3-Clients können nun Exporte im Storage-System mounten.

3. Stellen Sie sicher, dass jeder Windows NFSv3-Client harte Mounts verwendet, indem Sie den angeben `-o mtype=hard` Option.

Dies ist erforderlich, um zuverlässige Halterungen zu gewährleisten.

```
mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
```

## Aktivieren Sie die Anzeige von NFS-Exporten auf NFS-Clients

NFS Clients können die verwenden `showmount -e` Befehl, um eine Liste der Exporte anzuzeigen, die von einem ONTAP-NFS-Server verfügbar sind. Dies kann Benutzern helfen, das Dateisystem zu identifizieren, das sie mounten möchten.

Ab ONTAP 9.2 können NFS-Clients über ONTAP standardmäßig die Exportliste anzeigen. In früheren Versionen, der `showmount` Option des `vserver nfs modify` Befehl muss explizit aktiviert sein. Zum Anzeigen der Exportliste sollte NFSv3 auf der SVM aktiviert sein.

### Beispiel

Mit dem folgenden Befehl wird die Showmount-Funktion auf der SVM namens vs1 angezeigt:

```
cluster1 : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
-----
vs1      enabled
```

Mit dem folgenden Befehl, der auf einem NFS-Client ausgeführt wird, wird die Liste der Exporte auf einem NFS-Server mit der IP-Adresse 10.63.21.9 angezeigt:

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix      (everyone)
/unix/unix1 (everyone)
/unix/unix2 (everyone)
/          (everyone)
```

## Managen Sie den Dateizugriff über NFS

### Aktivieren oder deaktivieren Sie NFSv3

Sie können NFSv3 aktivieren oder deaktivieren, indem Sie den ändern `-v3` Option. So ist der Dateizugriff über das NFSv3-Protokoll für Clients möglich. Standardmäßig ist NFSv3 aktiviert.

### Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein...

Aktivieren Sie NFSv3	<code>vserver nfs modify -vserver vserver_name -v3 enabled</code>
Deaktivieren Sie NFSv3	<code>vserver nfs modify -vserver vserver_name -v3 disabled</code>

## Aktivieren oder deaktivieren Sie NFSv4.0

Sie können NFSv4.0 aktivieren oder deaktivieren, indem Sie den ändern `-v4.0` Option. Dadurch können Clients über das NFSv4.0-Protokoll auf Dateien zugreifen. In ONTAP 9.9 ist NFSv4.0 standardmäßig aktiviert; in früheren Versionen ist dieser Dienst standardmäßig deaktiviert.

### Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den folgenden Befehl ein...
Aktivieren Sie NFSv4.0	<code>vserver nfs modify -vserver vserver_name -v4.0 enabled</code>
Deaktivieren Sie NFSv4.0	<code>vserver nfs modify -vserver vserver_name -v4.0 disabled</code>

## Aktivieren oder deaktivieren Sie NFSv4.1

Sie können NFSv4.1 aktivieren oder deaktivieren, indem Sie den ändern `-v4.1` Option. So ist der Dateizugriff für Clients möglich, die das NFSv4.1-Protokoll verwenden. In ONTAP 9.9 ist NFSv4.1 standardmäßig aktiviert; in früheren Versionen ist er standardmäßig deaktiviert.

### Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den folgenden Befehl ein...
Aktivieren Sie NFSv4.1	<code>vserver nfs modify -vserver vserver_name -v4.1 enabled</code>
Deaktivieren Sie NFSv4.1	<code>vserver nfs modify -vserver vserver_name -v4.1 disabled</code>

## Aktivieren oder deaktivieren Sie pNFS

pNFS verbessert die Performance, da NFS-Clients Lese-/Schreibvorgänge direkt und parallel auf Storage-Geräten durchführen können. Dadurch wird der NFS-Server als möglicher Engpass vermieden. Zum Aktivieren oder Deaktivieren von pNFS (Parallel NFS) können Sie das ändern `-v4.1-pnfs` Option.

ONTAP Release:	Der pNFS-Standard lautet...
9.8 oder höher	Deaktiviert
9.7 oder früher	Aktiviert

### Was Sie benötigen

Zur Verwendung von pNFS ist die Unterstützung für NFSv4.1 erforderlich.

Wenn Sie pNFS aktivieren möchten, müssen Sie zuerst die NFS-Empfehlungen deaktivieren. Beide können nicht gleichzeitig aktiviert werden.

Wenn Sie pNFS mit Kerberos auf SVMs verwenden, müssen Sie Kerberos auf jeder LIF auf der SVM aktivieren.

### Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein...
Aktivieren Sie pNFS	<pre>vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled</pre>
Deaktivieren Sie pNFS	<pre>vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled</pre>

## Kontrollieren Sie den NFS-Zugriff über TCP und UDP

Sie können den NFS-Zugriff auf Storage Virtual Machines (SVMs) über TCP und UDP aktivieren oder deaktivieren, indem Sie die ändern `-tcp` und `-udp` Parameter. So können Sie kontrollieren, ob NFS-Clients in Ihrer Umgebung über TCP oder UDP auf Daten zugreifen können.

### Über diese Aufgabe

Diese Parameter gelten nur für NFS. Sie wirken sich nicht auf Hilfsprotokolle aus. Wenn beispielsweise NFS über TCP deaktiviert ist, sind die Mount-Vorgänge über TCP immer noch erfolgreich. Um TCP- oder UDP-Datenverkehr vollständig zu blockieren, können Sie die Regeln für die Exportrichtlinie verwenden.



Sie müssen den SnapDiff RPC Server deaktivieren, bevor Sie TCP für NFS deaktivieren, um einen Fehler bei Befehlsfehlern zu vermeiden. Sie können TCP mit dem Befehl deaktivieren `vserver snapdiff-rpc-server off -vserver vserver name`.



## Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn NFS-Zugriff sein soll...	Geben Sie den Befehl ein...
Aktiviert über TCP	<code>vserver nfs modify -vserver vserver_name -tcp enabled</code>
Über TCP deaktiviert	<code>vserver nfs modify -vserver vserver_name -tcp disabled</code>
Aktiviert über UDP	<code>vserver nfs modify -vserver vserver_name -udp enabled</code>
Über UDP deaktiviert	<code>vserver nfs modify -vserver vserver_name -udp disabled</code>

## Kontrollieren Sie NFS-Anforderungen von nicht reservierten Ports

Sie können NFS-Mount-Anforderungen von nicht reservierten Ports ablehnen, indem Sie den aktivieren `-mount-rootonly` Option. Um alle NFS-Anforderungen von nicht reservierten Ports abzulehnen, können Sie den aktivieren `-nfs-rootonly` Option.

### Über diese Aufgabe

Standardmäßig ist die Option `-mount-rootonly` ist enabled.

Standardmäßig ist die Option `-nfs-rootonly` ist disabled.

Diese Optionen gelten nicht für das Null-Verfahren.

## Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein...
Zulassen von NFS-Mount-Anforderungen von nicht reservierten Ports	<code>vserver nfs modify -vserver vserver_name -mount-rootonly disabled</code>
NFS-Mount-Anforderungen von nicht reservierten Ports ablehnen	<code>vserver nfs modify -vserver vserver_name -mount-rootonly enabled</code>
Erlauben Sie alle NFS-Anfragen von nicht reservierten Ports	<code>vserver nfs modify -vserver vserver_name -nfs-rootonly disabled</code>
Alle NFS-Anfragen von nicht reservierten Ports ablehnen	<code>vserver nfs modify -vserver vserver_name -nfs-rootonly enabled</code>

## Bearbeiten Sie den NFS-Zugriff auf NTFS-Volumes oder qtrees für unbekannte UNIX-Benutzer

Wenn ONTAP UNIX-Benutzer, die eine Verbindung zu Volumes oder qtrees mit NTFS-Sicherheitsstil herstellen möchten, nicht identifizieren kann, kann er den Benutzer daher nicht explizit einem Windows-Benutzer zuordnen. Sie können ONTAP so konfigurieren, dass diese Benutzer entweder den Zugriff auf eine strengere Sicherheit verweigern oder sie einem Windows-Standardbenutzer zuordnen, um einen Mindestzugriff für alle Benutzer zu gewährleisten.

### Was Sie benötigen

Ein Windows-Standardbenutzer muss konfiguriert werden, wenn Sie diese Option aktivieren möchten.

### Über diese Aufgabe

Wenn ein UNIX-Benutzer versucht, auf Volumes oder qtrees mit NTFS-Sicherheitsstil zuzugreifen, muss der UNIX-Benutzer zuerst einem Windows-Benutzer zugeordnet werden, damit ONTAP die NTFS-Berechtigungen richtig auswerten kann. Wenn ONTAP jedoch den Namen des UNIX-Benutzers in den konfigurierten Servicesquellen für Benutzerinformationen nicht nachsehen kann, kann der UNIX-Benutzer nicht explizit einem bestimmten Windows-Benutzer zugeordnet werden. Sie können entscheiden, wie Sie mit solchen unbekanntem UNIX-Benutzern umgehen:

- Zugriff auf unbekannte UNIX-Benutzer verweigern.

Dies setzt strengere Sicherheit durch, da alle UNIX-Benutzer expliziten Zugriff auf NTFS-Volumes oder qtrees benötigen.

- Weisen Sie unbekannte UNIX-Benutzer einem Windows-Standardbenutzer zu.

Dies bietet weniger Sicherheit und Komfort, da alle Benutzer über einen standardmäßigen Windows Benutzer Zugriff auf NTFS-Volumes oder qtrees erhalten.

### Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie den standardmäßigen Windows-Benutzer für unbekannte UNIX-Benutzer wünschen...	Geben Sie den Befehl ein...
Aktiviert	<pre>vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled</pre>
Deaktiviert	<pre>vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled</pre>

3. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

## Überlegungen zu Clients, die NFS-Exporte mithilfe eines nicht reservierten Ports mounten

Der `-mount-rootonly` Die Option muss auf einem Speichersystem deaktiviert werden, das Clients unterstützen muss, die NFS-Exporte mithilfe eines nicht reservierten Ports bereitstellen, selbst wenn der Benutzer als Root angemeldet ist. Zu diesen Clients gehören Hummingbird Clients und Solaris NFS/IPv6 Clients.

Wenn der `-mount-rootonly` Option ist aktiviert, ONTAP erlaubt NFS-Clients, die nicht reservierte Ports verwenden, was bedeutet, Ports mit mehr als 1,023 Nummern, um NFS-Exporte zu mounten.

## Führen Sie eine strengere Zugriffsüberprüfung für Netgroups durch, indem Sie Domänen überprüfen

Standardmäßig führt ONTAP eine zusätzliche Verifizierung durch, wenn der Client-Zugriff für eine Netzwerkgruppe ausgewertet wird. Bei der zusätzlichen Überprüfung wird sichergestellt, dass die Domäne des Clients mit der Domänenkonfiguration der Storage Virtual Machine (SVM) übereinstimmt. Andernfalls verweigert ONTAP den Client-Zugriff.

### Über diese Aufgabe

Wenn ONTAP die Regeln für die Exportrichtlinie für den Clientzugriff evaluiert und eine Regel für die Exportrichtlinie eine Netzwerkgruppe enthält, muss ONTAP festlegen, ob die IP-Adresse eines Clients zur Netzwerkgruppe gehört. Zu diesem Zweck konvertiert ONTAP die IP-Adresse des Clients mithilfe von DNS in einen Hostnamen und erhält einen vollständig qualifizierten Domänennamen (FQDN).

Wenn in der `netgroup`-Datei nur ein Kurzname für den Host aufgeführt wird und der Kurzname für den Host in mehreren Domänen vorhanden ist, kann ein Client aus einer anderen Domain ohne diese Prüfung Zugriff erhalten.

Um dies zu verhindern, vergleicht ONTAP die Domäne, die vom DNS für den Host zurückgegeben wurde, mit der Liste der für die SVM konfigurierten DNS-Domänennamen. Stimmt das überein, ist der Zugriff zulässig. Stimmt diese nicht überein, wird der Zugriff verweigert.

Diese Überprüfung ist standardmäßig aktiviert. Sie können die IT-Abteilung durch Ändern des `managen -netgroup-dns-domain-search` Parameter, der auf der erweiterten Berechtigungsebene verfügbar ist.

### Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Führen Sie die gewünschte Aktion aus:

Wenn Sie möchten, dass die Domänenüberprüfung für Netzgruppen...	Eingeben...
Aktiviert	<code>vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled</code>
Deaktiviert	<code>vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled</code>

3. Legen Sie die Berechtigungsebene auf admin fest:

```
set -privilege admin
```

## Bearbeiten von Ports, die für NFSv3-Services verwendet werden

Der NFS-Server auf dem Speichersystem verwendet Dienste wie den Mount Daemon und Network Lock Manager, um mit NFS-Clients über bestimmte Standard-Netzwerkports zu kommunizieren. In den meisten NFS-Umgebungen funktionieren die Standard-Ports richtig und erfordern keine Änderung. Wenn Sie jedoch unterschiedliche NFS-Netzwerk-Ports in Ihrer NFSv3-Umgebung verwenden möchten, können Sie dies tun.

### Was Sie benötigen

Wenn Sie NFS-Ports auf dem Storage-System ändern, müssen alle NFS-Clients erneut mit dem System verbunden sein. Daher sollten Sie diese Informationen vor der Änderung an Ihre Benutzer übermitteln.

### Über diese Aufgabe

Sie können die von den Diensten NFS Mount Daemon, Network Lock Manager, Network Status Monitor und NFS Quota Daemon für jede Storage Virtual Machine (SVM) verwendeten Ports festlegen. Die Änderung der Portnummer wirkt sich auf NFS-Clients aus, die über TCP und UDP auf Daten zugreifen.

Die Ports für NFSv4 und NFSv4.1 können nicht geändert werden.

### Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Zugriff auf NFS deaktivieren:

```
vserver nfs modify -vserver vserver_name -access false
```

3. Legen Sie den NFS-Port für den spezifischen NFS-Service fest:

```
vserver nfs modify -vserver vserver_namenfs_port_parameterport_number
```

NFS-Port-Parameter	Beschreibung	Standardport
-mountd-port	NFS-Mount-Daemon	635
-nlm-port	Network Lock Manager	4045
-nsm-port	Netzwerkstatusüberwachung	4046
-rquotad-port	NFS Kontingent-Daemon	4049

Neben dem Standardport beträgt der zulässige Bereich der Portnummern 1024 bis 65535. Jeder NFS-Service muss einen eindeutigen Port verwenden.

4. Zugriff auf NFS aktivieren:

```
vserver nfs modify -vserver vserver_name -access true
```

5. Verwenden Sie die `network connections listening show` Befehl zum Überprüfen der Portnummer.

6. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

### Beispiel

Mit den folgenden Befehlen wird der NFS Mount Daemon Port auf 1113 auf der SVM mit dem Namen vs1 gesetzt:

```

vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
        them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name      Interface Name:Local Port      Protocol/Service
-----
Node: cluster1-01
Cluster           cluster1-01_clus_1:7700        TCP/ctlopcp
vs1               data1:4046                    TCP/sm
vs1               data1:4046                    UDP/sm
vs1               data1:4045                    TCP/nlm-v4
vs1               data1:4045                    UDP/nlm-v4
vs1               data1:1113                    TCP/mount
vs1               data1:1113                    UDP/mount
...
vs1::*> set -privilege admin

```

## Befehle zum Verwalten von NFS-Servern

Zum Verwalten von NFS-Servern gibt es bestimmte ONTAP-Befehle.

Ihr Ziel ist	Befehl
Erstellen Sie einen NFS-Server	<code>vserver nfs create</code>
Zeigen Sie NFS-Server an	<code>vserver nfs show</code>
Ändern Sie einen NFS-Server	<code>vserver nfs modify</code>
Löschen Sie einen NFS-Server	<code>vserver nfs delete</code>

<p>Verbergen Sie die <code>.snapshot</code> Verzeichnisliste unter NFSv3 Bereitstellungspunkte</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Expliziter Zugriff auf den <code>.snapshot</code> Das Verzeichnis wird weiterhin zugelassen, auch wenn die Option aktiviert ist.</p> </div>	<p><code>vserver nfs</code> Befehle mit <code>-v3-hide-snapshot</code> Option aktiviert</p>
--	---

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

## Fehlerbehebung bei Problemen mit dem Namensdienst

Wenn für Clients aufgrund von Problemen mit dem Nameservice Zugriffsfehler auftreten, können Sie das verwenden `vserver services name-service getxxbyyy` Befehlsfamilie, die verschiedene Suchvorgänge für den Namensdienst manuell durchführt und die Details und Ergebnisse der Suche analysiert, um Ihnen bei der Fehlerbehebung zu helfen.

### Über diese Aufgabe

- Sie können für jeden Befehl Folgendes angeben:
  - Name des Node oder der Storage Virtual Machine (SVM), um die Suche durchzuführen.
 

So können Sie die Suche nach einem bestimmten Node oder einer bestimmten SVM testen, um die Suche nach einem potenziellen Name-Service-Konfigurationsproblem zu verfeinern.
  - Gibt an, ob die Quelle für die Suche angezeigt wird.
 

So können Sie überprüfen, ob die richtige Quelle verwendet wurde.
- ONTAP wählt den Service für die Abfrage basierend auf der konfigurierten Name Service Switch-Reihenfolge aus.
- Diese Befehle sind auf der erweiterten Berechtigungsebene verfügbar.

### Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Um den abzurufen...	Verwenden Sie den Befehl...
IP-Adresse eines Host-Namens	<pre>vserver services name-service getxxbyyy getaddrinfo vserver services name- service getxxbyyy gethostbyname (Nur IPv4- Adressen)</pre>
Mitglieder einer Gruppe nach Gruppen-ID	<pre>vserver services name-service getxxbyyy getgrbygid</pre>

Mitglieder einer Gruppe nach Gruppennamen	<code>vserver services name-service getxxbyyy getgrbyname</code>
Liste der Gruppen, denen ein Benutzer angehört	<code>vserver services name-service getxxbyyy getgrlist</code>
Hostname einer IP-Adresse	<code>vserver services name-service getxxbyyy getnameinfo vserver services name- service getxxbyyy gethostbyaddr (Nur IPv4- Adressen)</code>
Benutzerinformationen nach Benutzernamen	<code>vserver services name-service getxxbyyy getpwbyname</code> Sie können die Namensauflösung von RBAC-Benutzern testen, indem Sie die angeben <code>-use-rbac</code> Parameter als <code>true</code> .
Benutzerinformationen nach Benutzer-ID	<code>vserver services name-service getxxbyyy getpwbyuid`</code> Sie können die Namensauflösung von RBAC-Benutzern testen, indem Sie die angeben <code>`-use- rbac</code> Parameter als <code>true</code> .
Netzgruppenmitgliedschaft eines Clients	<code>vserver services name-service getxxbyyy netgrp</code>
Netzwerkgruppenmitgliedschaft eines Clients mit der Suche nach Netgroup-by-Host	<code>vserver services name-service getxxbyyy netgrpbyhost</code>

Das folgende Beispiel zeigt einen DNS-Suchtest für die SVM vs1, indem versucht wird, die IP-Adresse für den Host `acast1.eng.example.com` abzurufen:

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

Das folgende Beispiel zeigt einen NIS-Suchtest für die SVM vs1, indem Sie versuchen, Benutzerinformationen für einen Benutzer mit der UID 501768 abzurufen:



```

cluster1::~*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvC2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash

```

Das folgende Beispiel zeigt einen LDAP-Suchtest für die SVM vs1, indem versucht wird, Benutzerinformationen für einen Benutzer mit dem Namen ldap1 abzurufen:

```

cluster1::~*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh

```

Das folgende Beispiel zeigt einen Netgroup-Lookup-Test für die SVM vs1, indem versucht wird herauszufinden, ob der Client dnshost0 Mitglied der netgroup lnetgroup 136 ist:

```

cluster1::~*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136

```

1. Analysieren Sie die Ergebnisse des durchgeführten Tests und ergreifen Sie die erforderlichen Maßnahmen.

Wenn der...	Überprüfen Sie...
Die Suche nach Host-Name oder IP-Adresse ist fehlgeschlagen oder hat falsche Ergebnisse angezeigt	DNS-Konfiguration
Suche hat eine falsche Quelle abgefragt	Name Service-Switch-Konfiguration

Die Benutzer- oder Gruppensuche ist fehlgeschlagen oder hat falsche Ergebnisse ergeben	Name Service Switch Konfiguration Quellkonfiguration (lokale Dateien, NIS-Domäne, LDAP-Client)  Netzwerkkonfiguration (wie etwa LIFs und Routen)
Die Suche nach dem Hostnamen ist fehlgeschlagen oder Zeitüberschreitung, und der DNS-Server löst keine DNS-Kurznamen auf (z. B. host1)	DNS-Konfiguration für Top-Level-Domain-Abfragen (TLD). Sie können TLD-Abfragen mit dem deaktivieren <code>-is-tld-query-enabled false</code> Option für die <code>vserver services name-service dns modify</code> Befehl.

### Verwandte Informationen

["NetApp Technical Report 4668: Name Services Best Practices Guide"](#)

## Überprüfen Sie die Namensdienstverbindungen

Ab ONTAP 9.2 können Sie die DNS- und LDAP-Namensserver überprüfen, um zu überprüfen, ob sie mit ONTAP verbunden sind. Diese Befehle sind auf der Administrator-Berechtigungsebene verfügbar.

### Über diese Aufgabe

Sie können bei Bedarf anhand des Konfigurationscheckers für den Namensdienst nach einer gültigen DNS- oder LDAP-Namensdienstkonfiguration suchen. Diese Validierungsprüfung kann über die Befehlszeile oder in System Manager initiiert werden.

Für DNS-Konfigurationen werden alle Server getestet und müssen funktionieren, damit die Konfiguration als gültig erachtet wird. Bei LDAP-Konfigurationen ist die Konfiguration gültig, solange ein Server aktiv ist. Die Befehle des Namensdiensts wenden den Konfigurationschecker an, es sei denn, der `skip-config-validation` Das Feld ist TRUE (die Standardeinstellung lautet „false“).

### Schritt

1. Verwenden Sie den entsprechenden Befehl, um eine Namensdienstkonfiguration zu überprüfen. Die Benutzeroberfläche zeigt den Status der konfigurierten Server an.

Prüfung...	Befehl
DNS-Konfigurationsstatus	<code>vserver services name-service dns check</code>
LDAP-Konfigurationsstatus	<code>vserver services name-service ldap check</code>

```
cluster1::> vserver services name-service dns check -vserver vs0
```

```

Vserver          Name Server      Status  Status Details
-----
vs0              10.11.12.13     up      Response time (msec): 55
vs0              10.11.12.14     up      Response time (msec): 70
vs0              10.11.12.15     down    Connection refused.
+-----+

```

```
cluster1::> vserver services name-service ldap check -vserver vs0
```

```

| Vserver: vs0
| Client Configuration Name: c1
| LDAP Status: up
| LDAP Status Details: Successfully connected to LDAP server
| "10.11.12.13".

```

Die Konfigurationsvalidierung ist erfolgreich, wenn mindestens einer der konfigurierten Server (Name-Server/ldap-Server) erreichbar ist und der Dienst bereitgestellt wird. Wenn einige Server nicht erreichbar sind, wird eine Warnung angezeigt.

## Befehle zum Verwalten von Name Service Switch-Einträgen

Sie können Einträge des Namensdienstschalters verwalten, indem Sie sie erstellen, anzeigen, ändern und löschen.

Ihr Ziel ist	Befehl
Erstellen Sie einen Namensdienstschalter-Eintrag	<code>vserver services name-service ns-switch create</code>
Einträge des Namensdienstschalters anzeigen	<code>vserver services name-service ns-switch show</code>
Ändern Sie einen Namensdienstschalter-Eintrag	<code>vserver services name-service ns-switch modify</code>
Löschen Sie einen Namensdienstschalter-Eintrag	<code>vserver services name-service ns-switch delete</code>

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

### Verwandte Informationen

["NetApp Technical Report 4668: Name Services Best Practices Guide"](#)

## Befehle zum Verwalten von Name Service Cache

Sie können den Name-Service-Cache verwalten, indem Sie den Wert für Live (TTL) ändern. Der TTL-Wert bestimmt, wie lange Name-Service-Informationen im Cache persistent sind.

Wenn Sie den TTL-Wert ändern möchten für...	Befehl
UNIX-Benutzer	<code>vserver services name-service cache unix-user settings</code>
UNIX-Gruppen	<code>vserver services name-service cache unix-group settings</code>
UNIX-Netzwerkgruppen	<code>vserver services name-service cache netgroups settings</code>
Hosts	<code>vserver services name-service cache hosts settings</code>
Gruppenmitgliedschaft	<code>vserver services name-service cache group-membership settings</code>

### Verwandte Informationen

["ONTAP 9-Befehle"](#)

## Befehle zum Verwalten von Name-Zuordnungen

Zum Verwalten von Name-Zuordnungen gibt es bestimmte ONTAP-Befehle.

Ihr Ziel ist	Befehl
Erstellen einer Namenszuweisung	<code>vserver name-mapping create</code>
Eine Namenszuordnung an einer bestimmten Position einfügen	<code>vserver name-mapping insert</code>
Namenszuordnungen anzeigen	<code>vserver name-mapping show</code>
Tauschen Sie die Position zweier Namenszuordnungen AUS HINWEIS: Ein Austausch ist nicht zulässig, wenn das Namenszuordnungen mit einem ip-Qualifier-Eintrag konfiguriert ist.	<code>vserver name-mapping swap</code>
Ändern einer Namenszuweisung	<code>vserver name-mapping modify</code>

Löschen einer Namenszuweisung	<code>vserver name-mapping delete</code>
Überprüfen Sie die richtige Namenszuweisung	<code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code>

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

## Befehle zum Verwalten lokaler UNIX-Benutzer

Es gibt bestimmte ONTAP Befehle zum Management lokaler UNIX Benutzer.

Ihr Ziel ist	Befehl
Erstellen Sie einen lokalen UNIX-Benutzer	<code>vserver services name-service unix-user create</code>
Laden Sie lokale UNIX-Benutzer von einem URI	<code>vserver services name-service unix-user load-from-uri</code>
Zeigen Sie lokale UNIX-Benutzer an	<code>vserver services name-service unix-user show</code>
Ändern Sie einen lokalen UNIX-Benutzer	<code>vserver services name-service unix-user modify</code>
Löschen Sie einen lokalen UNIX-Benutzer	<code>vserver services name-service unix-user delete</code>

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

## Befehle zum Verwalten von lokalen UNIX Gruppen

Zum Verwalten von lokalen UNIX Gruppen gibt es bestimmte ONTAP Befehle.

Ihr Ziel ist	Befehl
Erstellen Sie eine lokale UNIX-Gruppe	<code>vserver services name-service unix-group create</code>
Fügen Sie einen Benutzer zu einer lokalen UNIX-Gruppe hinzu	<code>vserver services name-service unix-group adduser</code>
Laden Sie lokale UNIX-Gruppen von einem URI	<code>vserver services name-service unix-group load-from-uri</code>
Zeigen Sie lokale UNIX-Gruppen an	<code>vserver services name-service unix-group show</code>

Ändern einer lokalen UNIX-Gruppe	<code>vserver services name-service unix-group modify</code>
Löschen Sie einen Benutzer aus einer lokalen UNIX-Gruppe	<code>vserver services name-service unix-group deluser</code>
Löschen Sie eine lokale UNIX-Gruppe	<code>vserver services name-service unix-group delete</code>

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

## Grenzwerte für lokale UNIX-Benutzer, -Gruppen und -Gruppenmitglieder

ONTAP hat Grenzwerte für die maximale Anzahl von UNIX Benutzern und Gruppen im Cluster eingeführt und Befehle zum Verwalten dieser Grenzwerte eingeführt. Diese Grenzwerte können dazu beitragen, Performance-Probleme zu vermeiden, da Administratoren nicht mehr zu viele lokale UNIX-Benutzer und -Gruppen im Cluster erstellen können.

Die Gesamtzahl der lokalen UNIX Benutzergruppen und Gruppenmitglieder ist begrenzt. Es gibt ein separates Limit für lokale UNIX-Benutzer. Die Grenzwerte gelten für das gesamte Cluster. Jeder dieser neuen Grenzwerte ist auf einen Standardwert eingestellt, den Sie bis zu einem vorher zugewiesenen harten Limit ändern können.

Datenbank	Standardlimit	Harte Grenze
Lokale UNIX-Benutzer	32,768	65,536
Lokale UNIX-Gruppen und Gruppenmitglieder	32,768	65,536

## Verwalten von Limits für lokale UNIX-Benutzer und -Gruppen

Es gibt bestimmte ONTAP Befehle zum Verwalten von Limits für lokale UNIX Benutzer und Gruppen. Cluster-Administratoren können diese Befehle verwenden, um Performance-Probleme im Cluster zu beheben, denen eine übermäßige Anzahl von lokalen UNIX-Benutzern und -Gruppen zugeordnet werden sollte.

### Über diese Aufgabe

Diese Befehle stehen dem Cluster-Administrator auf der erweiterten Berechtigungsebene zur Verfügung.

### Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Verwenden Sie den Befehl...
Informationen zu lokalen UNIX-Benutzerlimits anzeigen	<code>vserver services unix-user max-limit show</code>

Ihr Ziel ist	Verwenden Sie den Befehl...
Zeigen Sie Informationen über die Grenzwerte der lokalen UNIX-Gruppen an	<code>vserver services unix-group max-limit show</code>
Ändern Sie die lokalen UNIX-Benutzergrenzen	<code>vserver services unix-user max-limit modify</code>
Ändern Sie die Grenzwerte für lokale UNIX-Gruppen	<code>vserver services unix-group max-limit modify</code>

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

## Befehle zum Verwalten von lokalen Netzgruppen

Sie können lokale Netzwerkgruppen verwalten, indem Sie sie von einem URI laden, ihren Status über Knoten hinweg überprüfen, anzeigen und löschen.

Ihr Ziel ist	Verwenden Sie den Befehl...
Laden von Netzgruppen aus einem URI	<code>vserver services name-service netgroup load</code>
Überprüfen Sie den Status von Netzgruppen über Knoten hinweg	<code>vserver services name-service netgroup status</code> Verfügbar auf der erweiterten Berechtigungsebene und höher.
Zeigen Sie lokale Netzgruppen an	<code>vserver services name-service netgroup file show</code>
Lokale Netzwerkgruppe löschen	<code>vserver services name-service netgroup file delete</code>

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

## Befehle zum Verwalten von NIS Domain-Konfigurationen

Es gibt bestimmte ONTAP Befehle zum Verwalten von NIS Domain-Konfigurationen.

Ihr Ziel ist	Befehl
Erstellen Sie eine NIS-Domänenkonfiguration	<code>vserver services name-service nis-domain create</code>
Anzeige der NIS-Domänenkonfigurationen	<code>vserver services name-service nis-domain show</code>

Anzeige des Bindungsstatus einer NIS-Domain-Konfiguration	<code>vserver services name-service nis-domain show-bound</code>
Zeigt NIS-Statistiken an	<code>vserver services name-service nis-domain show-statistics</code> Verfügbar auf der erweiterten Berechtigungsebene und höher.
Löschen Sie NIS-Statistiken	<code>vserver services name-service nis-domain clear-statistics</code> Verfügbar auf der erweiterten Berechtigungsebene und höher.
Ändern Sie eine NIS-Domänenkonfiguration	<code>vserver services name-service nis-domain modify</code>
Löschen Sie eine NIS-Domänenkonfiguration	<code>vserver services name-service nis-domain delete</code>
Aktivieren Sie das Caching für Netzgruppensuche nach Host	<code>vserver services name-service nis-domain netgroup-database config modify</code> Verfügbar auf der erweiterten Berechtigungsebene und höher.

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

## Befehle zum Verwalten von LDAP-Client-Konfigurationen

Für das Management der LDAP-Client-Konfigurationen gibt es bestimmte ONTAP-Befehle.



SVM-Administratoren können LDAP-Client-Konfigurationen, die von Cluster-Administratoren erstellt wurden, nicht ändern oder löschen.

Ihr Ziel ist	Befehl
Erstellen Sie eine LDAP-Client-Konfiguration	<code>vserver services name-service ldap client create</code>
Zeigen Sie die LDAP-Client-Konfigurationen an	<code>vserver services name-service ldap client show</code>
Ändern Sie eine LDAP-Client-Konfiguration	<code>vserver services name-service ldap client modify</code>
Ändern des LDAP-CLIENTBINDUNGSKENNWORTS	<code>vserver services name-service ldap client modify-bind-password</code>
Löschen Sie eine LDAP-Client-Konfiguration	<code>vserver services name-service ldap client delete</code>



Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

## Befehle zum Verwalten von LDAP-Konfigurationen

Für das Management von LDAP-Konfigurationen gibt es bestimmte ONTAP-Befehle.

Ihr Ziel ist	Befehl
LDAP-Konfiguration erstellen	<code>vserver services name-service ldap create</code>
Zeigen Sie LDAP-Konfigurationen an	<code>vserver services name-service ldap show</code>
Ändern Sie eine LDAP-Konfiguration	<code>vserver services name-service ldap modify</code>
Löschen Sie eine LDAP-Konfiguration	<code>vserver services name-service ldap delete</code>

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

## Befehle zum Verwalten von LDAP-Client-Schemavorlagen

Es gibt bestimmte ONTAP-Befehle zum Verwalten von LDAP-Client-Schemavorlagen.



SVM-Administratoren können die von Cluster-Administratoren erstellten LDAP-Client-Schemata nicht ändern oder löschen.

Ihr Ziel ist	Befehl
Vorhandene LDAP-Schemavorlage kopieren	<code>vserver services name-service ldap client schema copy</code> Verfügbar auf der erweiterten Berechtigungsebene und höher.
LDAP-Schemavorlagen anzeigen	<code>vserver services name-service ldap client schema show</code>
Ändern einer LDAP-Schemavorlage	<code>vserver services name-service ldap client schema modify</code> Verfügbar auf der erweiterten Berechtigungsebene und höher.
Löschen einer LDAP-Schemavorlage	<code>vserver services name-service ldap client schema delete</code> Verfügbar auf der erweiterten Berechtigungsebene und höher.

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

## Befehle zum Verwalten von NFS Kerberos Schnittstellenkonfigurationen

Es gibt bestimmte ONTAP-Befehle zum Verwalten von NFS-Kerberos-Schnittstellenkonfigurationen.

Ihr Ziel ist	Befehl
Aktivieren Sie NFS Kerberos auf einem LIF	<code>vserver nfs kerberos interface enable</code>
Zeigt die NFS-Kerberos-Schnittstellenkonfigurationen an	<code>vserver nfs kerberos interface show</code>
Ändern Sie die Konfiguration einer NFS-Kerberos-Schnittstelle	<code>vserver nfs kerberos interface modify</code>
Deaktivieren Sie NFS Kerberos auf einem LIF	<code>vserver nfs kerberos interface disable</code>

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

## Befehle zum Verwalten von NFS-Kerberos-Bereichskonfigurationen

Es gibt bestimmte ONTAP-Befehle zum Verwalten von NFS-Kerberos-Bereichskonfigurationen.

Ihr Ziel ist	Befehl
Erstellen Sie eine NFS-Kerberos-Bereichskonfiguration	<code>vserver nfs kerberos realm create</code>
Anzeigen von NFS-Kerberos-Bereichskonfigurationen	<code>vserver nfs kerberos realm show</code>
Ändern Sie die Konfiguration eines NFS-Kerberos-Bereichs	<code>vserver nfs kerberos realm modify</code>
Löschen Sie eine NFS-Kerberos-Bereichskonfiguration	<code>vserver nfs kerberos realm delete</code>

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

## Befehle zum Verwalten von Exportrichtlinien

Zum Management von Exportrichtlinien gibt es bestimmte ONTAP-Befehle.

Ihr Ziel ist	Befehl
Informationen zu Exportrichtlinien anzeigen	<code>vserver export-policy show</code>
Benennen Sie eine Exportrichtlinie um	<code>vserver export-policy rename</code>

Exportrichtlinie kopieren	<code>vserver export-policy copy</code>
Löschen Sie eine Exportrichtlinie	<code>vserver export-policy delete</code>

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

## Befehle zum Verwalten von Exportregeln

Zum Management von Exportregeln gibt es bestimmte ONTAP-Befehle.

Ihr Ziel ist	Befehl
Erstellen Sie eine Exportregel	<code>vserver export-policy rule create</code>
Informationen zu Exportregeln anzeigen	<code>vserver export-policy rule show</code>
Exportregel ändern	<code>vserver export-policy rule modify</code>
Exportregel löschen	<code>vserver export-policy rule delete</code>



Wenn Sie mehrere identische Exportregeln konfiguriert haben, die verschiedenen Clients entsprechen, sollten Sie diese beim Verwalten von Exportregeln stets synchron halten.

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

## Konfigurieren Sie den NFS-Anmeldeinformationscache

### Gründe für das Ändern der NFS-Anmeldeinformationszeit im Cache

ONTAP verwendet einen Cache für Zugangsdaten, um die für die Benutzerauthentifizierung für NFS-Exportzugriff benötigten Informationen zu speichern. So wird ein schnellerer Zugriff und eine bessere Performance ermöglicht. Sie können konfigurieren, wie lange Informationen im Cache für Anmeldeinformationen gespeichert werden, um sie an Ihre Umgebung anzupassen.

Wenn beim Ändern der TTL (Time-to-Live) für den NFS-Anmeldeinformationscache Probleme behoben werden, gibt es verschiedene Szenarien. Sie sollten verstehen, was diese Szenarien sind sowie die Auswirkungen der Durchführung dieser Änderungen.

### Gründe

Unter folgenden Umständen sollte die Standard-TTL geändert werden:

<b>Problem</b>	<b>Korrekturmaßnahmen</b>
Die Nameserver in Ihrer Umgebung weisen aufgrund einer hohen Auslastung von ONTAP eine Performance-Verschlechterung auf.	Erhöhen Sie die TTL für positive und negative zwischengespeicherte Anmeldeinformationen, um die Anzahl der Anfragen von ONTAP auf Nameserver zu reduzieren.
Der Name-Server-Administrator hat Änderungen vorgenommen, um Zugriff auf NFS-Benutzer zu ermöglichen, die zuvor abgelehnt wurden.	Verringern Sie die TTL für negative Anmeldeinformationen im Cache, um die Zeit zu verkürzen, die NFS-Benutzer auf die Anforderung von ONTAP-Zugangsdaten von externen Name-Servern warten müssen, damit sie Zugriff erhalten können.
Der Name-Server-Administrator hat Änderungen vorgenommen, um den Zugriff auf NFS-Benutzer zu verweigern, die zuvor zugelassen waren.	Reduzieren Sie die TTL für positive Anmeldeinformationen im Cache, um die Zeit zu verkürzen, bevor ONTAP neue Zugangsdaten von externen Name-Servern anfordert, damit NFS-Benutzer jetzt keinen Zugriff haben.

### Konsequenzen

Sie können die Zeitdauer individuell ändern, um positive und negative Anmeldeinformationen zwischenspeichern zu können. Sie sollten sich jedoch sowohl der vor- als auch der Nachteile bewusst sein.

<b>Sie suchen...</b>	<b>Der Vorteil liegt...</b>	<b>Der Nachteil ist...</b>
Erhöhen Sie die Cache-Zeit für positive Anmeldeinformationen	ONTAP sendet Anfragen nach Zugangsdaten seltener an Server und reduziert so die Belastung von Name Servern.	Es dauert länger, den Zugriff auf NFS-Benutzer abzulehnen, die zuvor einen Zugriff gewährt hatten, aber nicht mehr.
Verringern Sie die Cache-Zeit für positive Anmeldeinformationen	Es dauert weniger Zeit, den Zugriff auf NFS-Benutzer abzulehnen, die zuvor einen Zugriff gewährt hatten, aber nicht mehr.	ONTAP sendet Anfragen nach Zugangsdaten häufiger an Server und erhöht so die Belastung von Name Servern.
Erhöhen Sie die negative Cachezeit für Zugangsdaten	ONTAP sendet Anfragen nach Zugangsdaten seltener an Server und reduziert so die Belastung von Name Servern.	Es dauert länger, NFS-Benutzern Zugriff zu gewähren, die zuvor keinen Zugriff hatten, sondern jetzt sind.
Verringern Sie die Cache-Zeit für die Anmeldeinformationen	Es dauert weniger Zeit, NFS-Benutzern Zugriff zu gewähren, die zuvor keinen Zugriff hatten, sondern jetzt sind.	ONTAP sendet Anfragen nach Zugangsdaten häufiger an Server und erhöht so die Belastung von Name Servern.

### Konfigurieren Sie die live-Konfiguration für NFS-Anmeldedaten im Cache

Sie können die Länge der Zeit konfigurieren, die ONTAP Anmeldedaten für NFS-Benutzer in seinem internen Cache speichert (time-to-live oder TTL), indem Sie den

NFS-Server der SVM (Storage Virtual Machine) ändern. So werden bestimmte Probleme entschärft, die bei hoher Belastung des Name Servers oder bei Änderungen der Zugangsdaten, die sich auf den Zugriff von NFS-Benutzern auswirken, auftreten können.

**Über diese Aufgabe**

Diese Parameter sind auf der erweiterten Berechtigungsebene verfügbar.

**Schritte**

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Führen Sie die gewünschte Aktion aus:

Wenn Sie die TTL für den Cache ändern möchten...	Verwenden Sie den Befehl...
Positive Referenzen	<pre>vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live</pre> <p>Die TTL wird in Millisekunden gemessen. Der Standardwert ist 24 Stunden (86,400,000 Millisekunden). Der zulässige Bereich für diesen Wert beträgt 1 Minute (60000 Millisekunden) bis 7 Tage (604,800,000 Millisekunden).</p>
Negative Anmeldeinformationen	<pre>vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live</pre> <p>Die TTL wird in Millisekunden gemessen. Der Standardwert ist 2 Stunden (7,200,000 Millisekunden). Der zulässige Bereich für diesen Wert beträgt 1 Minute (60000 Millisekunden) bis 7 Tage (604,800,000 Millisekunden).</p>

3. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

**Management von Caches für Exportrichtlinien**

**Exportrichtlinien-Caches leeren**

ONTAP nutzt mehrere Exportrichtlinien-Caches, um Informationen im Zusammenhang mit Exportrichtlinien zu speichern, um schnelleren Zugriff zu ermöglichen.

Exportrichtlinien werden manuell bereinigt (`vserver export-policy cache flush`) Entfernt potenziell veraltete Informationen und zwingt ONTAP, aktuelle Informationen aus den entsprechenden externen Ressourcen abzurufen. Dies kann dabei helfen, eine Vielzahl von Problemen im Zusammenhang mit dem Client-Zugriff auf NFS-Exporte zu lösen.

**Über diese Aufgabe**

Informationen zum Export-Policy-Cache können aus folgenden Gründen veraltet sein:

- Eine kürzliche Änderung der Exportrichtlinien
- Eine kürzliche Änderung an Hostnamendatensätzen in Namensservern
- Eine kürzliche Änderung zu netgroup-Einträgen in Name-Servern
- Wiederherstellung nach einem Netzwerkausfall, der verhindert hat, dass Netzgruppen voll geladen werden

### Schritte

1. Wenn Sie keinen Cache für den Namensservice aktiviert haben, führen Sie eine der folgenden Aktionen im Modus „Erweiterte Berechtigungen“ aus:

Wenn Sie spülen möchten...	Geben Sie den Befehl ein...
Alle Cache-Speicher für Exportrichtlinien (außer Showmount)	<code>vserver export-policy cache flush -vserver vserver_name</code>
Die Exportrichtlinie regeln den Zugriff auf den Cache	<code>vserver export-policy cache flush -vserver vserver_name -cache access</code> Sie können das optional angeben <code>-node</code> Parameter zum Angeben des Node, auf dem Sie den Zugriffs-Cache bereinigen möchten.
Der Host-Name-Cache	<code>vserver export-policy cache flush -vserver vserver_name -cache host</code>
Der Netzwerk-Cache	<code>vserver export-policy cache flush -vserver vserver_name -cache netgroup</code> Die Verarbeitung von Netzgruppen ist ressourcenintensiv. Sie sollten den Netgroup-Cache nur dann leeren, wenn Sie versuchen, ein Problem mit dem Clientzugriff zu lösen, das durch eine veraltete Netzwerkgruppe verursacht wird.
Der showmount-Cache	<code>vserver export-policy cache flush -vserver vserver_name -cache showmount</code>

2. Wenn der Name Service-Cache aktiviert ist, führen Sie eine der folgenden Aktionen durch:

Wenn Sie spülen möchten...	Geben Sie den Befehl ein...
Die Exportrichtlinie regeln den Zugriff auf den Cache	<code>vserver export-policy cache flush -vserver vserver_name -cache access</code> Sie können das optional angeben <code>-node</code> Parameter zum Angeben des Node, auf dem Sie den Zugriffs-Cache bereinigen möchten.
Der Host-Name-Cache	<code>vserver services name-service cache hosts forward-lookup delete-all</code>

Wenn Sie spülen möchten...	Geben Sie den Befehl ein...
Der Netzwerk-Cache	<code>vserver services name-service cache netgroups ip-to-netgroup delete-all vserver services name-service cache netgroups members delete-all</code> Die Verarbeitung von Netzgruppen ist ressourcenintensiv. Sie sollten den Netgroup-Cache nur dann leeren, wenn Sie versuchen, ein Problem mit dem Clientzugriff zu lösen, das durch eine veraltete Netzwerkgruppe verursacht wird.
Der showmount-Cache	<code>vserver export-policy cache flush -vserver vserver_name -cache showmount</code>

### Anzeige der Netzwerkgruppewarteschlange und des Caches für die Exportrichtlinie

ONTAP verwendet die Netzwerkgruppewarteschlange beim Importieren und Auflösen von Netzgruppen und verwendet den Netzwerkgruppecache, um die resultierenden Informationen zu speichern. Wenn Sie Probleme mit der Netzwerkgruppe der Exportrichtlinie beheben, können Sie das verwenden `vserver export-policy netgroup queue show` Und `vserver export-policy netgroup cache show` Befehle zur Anzeige des Status der Netzwerkgruppewarteschlange und des Inhalts des Netzwerkgruppecache.

#### Schritt

1. Führen Sie eine der folgenden Aktionen aus:

So zeigen Sie die Netzwerkgruppe der Exportrichtlinie an:	Geben Sie den Befehl ein...
Warteschlange	<code>vserver export-policy netgroup queue show</code>
Cache	<code>vserver export-policy netgroup cache show -vserver vserver_name</code>

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

### Prüfen Sie, ob eine Client-IP-Adresse Mitglied einer Netzwerkgruppe ist

Bei der Behebung von Problemen mit dem NFS-Client-Zugriff im Zusammenhang mit Netzgruppen können Sie das verwenden `vserver export-policy netgroup check-membership` Befehl, um zu ermitteln, ob eine Client-IP Mitglied einer bestimmten Netzwerkgruppe ist.

## Über diese Aufgabe

Durch die Überprüfung der Netzgruppenmitgliedschaft können Sie feststellen, ob ONTAP sich bewusst ist, dass ein Client Mitglied einer Netzwerkgruppe ist oder nicht. Damit können Sie auch wissen, ob sich der ONTAP Netzwerkgruppecache im transienten Zustand befindet, während die Informationen der Netzwerkgruppe aktualisiert werden. Diese Informationen können Ihnen dabei helfen zu verstehen, warum einem Kunden ein unerwarteter Zugriff gewährt oder verweigert wird.

## Schritt

1. Überprüfen Sie die Netzgruppenmitgliedschaft einer Client-IP-Adresse: `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

Der Befehl kann die folgenden Ergebnisse zurückgeben:

- Der Client ist Mitglied der Netzwerkgruppe.

Dies wurde durch einen Reverse-Lookup-Scan oder eine netgroup-by-Host-Suche bestätigt.

- Der Client ist Mitglied der Netzwerkgruppe.

Sie wurde im ONTAP Netzwerkgruppecache gefunden.

- Der Client ist kein Mitglied der Netzwerkgruppe.
- Die Mitgliedschaft des Clients kann noch nicht bestimmt werden, da ONTAP derzeit den Netzwerk-Gruppen-Cache aktualisiert.

Bis zu diesem Zeitpunkt kann die Mitgliedschaft nicht explizit in oder aus ausgeschlossen werden. Verwenden Sie die `vserver export-policy netgroup queue show` Befehl zum Überwachen des Ladevorgangs der Netzwerkgruppe und wiederholen Sie die Prüfung, nachdem sie abgeschlossen ist.

## Beispiel

Im folgenden Beispiel wird geprüft, ob ein Client mit der IP-Adresse 172.17.16.72 Mitglied der Netzwerkgruppe Mercury auf der SVM vs1 ist:

```
cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup mercury -client-ip 172.17.16.72
```

## Optimieren Sie die Performance des Zugriffs-Cache

Sie können mehrere Parameter konfigurieren, um den Zugriffs-Cache zu optimieren und ein Gleichgewicht zwischen der Performance und der aktuellen Menge der im Zugriffs-Cache gespeicherten Informationen zu finden.

## Über diese Aufgabe

Wenn Sie die Aktualisierungszeiträume für den Zugriffs-Cache konfigurieren, sollten Sie Folgendes beachten:

- Höhere Werte bedeuten, dass Einträge im Zugriffs-Cache länger bleiben.

Der Vorteil ist eine bessere Performance, weil ONTAP weniger Ressourcen für die Aktualisierung von



Zugriffs-Cache-Einträgen ausgibt. Der Nachteil besteht darin, dass eine Aktualisierung der Regeln für die Exportrichtlinie und die Einträge für den Zugriffs-Cache veraltet ist. Dies führt dazu, dass Clients, die Zugriff erhalten sollen, möglicherweise verweigert werden und Clients, die verweigert werden sollten, möglicherweise Zugriff erhalten.

- Niedrigere Werte bedeuten, dass ONTAP öfter auf Cache-Einträge aktualisiert.

Der Vorteil ist, dass die Einträge aktueller sind und Kunden mit höherer Wahrscheinlichkeit den Zugang korrekt gewährt oder verweigert werden. Der Nachteil ist eine verminderliche Performance, da ONTAP mehr Ressourcen für die Aktualisierung von Zugriffs-Cache-Einträgen ausgibt.

## Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Führen Sie die gewünschte Aktion aus:

So ändern Sie die...	Eingeben...
Zeitraum für positive Einträge aktualisieren	<code>vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value</code>
Aktualisierungszeitraum für negative Einträge	<code>vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value</code>
Timeout-Zeitraum für alte Einträge	<code>vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value</code>

3. Überprüfen Sie die neuen Parametereinstellungen:

```
vserver export-policy access-cache config show-all-vservers
```

4. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

## Verwalten von Dateisperren

### Über die Dateispernung zwischen Protokollen

Die Dateispernung wird von Client-Anwendungen verwendet, um zu verhindern, dass ein Benutzer auf eine Datei zugreift, die zuvor von einem anderen Benutzer geöffnet wurde. Wie ONTAP Dateien sperrt, hängt vom Protokoll des Clients ab.

Wenn es sich bei dem Client um einen NFS-Client handelt, sind Locks Advisory. Wenn es sich bei dem Client um einen SMB-Client handelt, sind Locks obligatorisch.

Aufgrund der Unterschiede zwischen den Dateisperrungen für NFS und SMB kann ein NFS-Client nicht auf eine Datei zugreifen, die zuvor von einer SMB-Applikation geöffnet wurde.

Die folgende Meldung tritt auf, wenn ein NFS-Client versucht, auf eine Datei zuzugreifen, die von einer SMB-Applikation gesperrt wurde:

- In gemischten oder NTFS-Volumes führen Dateimanipulation-Vorgänge wie `rm`, `rmdir`, und `mv` Fehler der NFS-Applikation kann auftreten.
- Lese- und Schreibvorgänge für NFS werden vom SMB Deny-read- bzw. Deny-Write-Open-Modus verweigert.
- NFS-Schreibvorgänge schlagen fehl, wenn der geschriebene Bereich der Datei durch einen exklusiven SMB-Bytelock gesperrt ist.

In UNIX-Volumes im Sicherheitsstil ignorieren NFS den SMB-Sperrstatus und erlauben den Zugriff auf die Datei. Alle anderen NFS-Vorgänge auf UNIX Volumes im Sicherheitsstil sorgen für den SMB-Lock-Status.

### **Wie ONTAP schreibgeschützte Bits behandelt**

Das schreibgeschützte Bit wird auf Datei-für-Datei-Basis gesetzt, um zu reflektieren, ob eine Datei beschreibbar (deaktiviert) oder schreibgeschützt (aktiviert) ist.

SMB-Clients, die Windows verwenden, können einen schreibgeschützten Bit pro Datei festlegen. NFS-Clients legen kein Leserbit pro Datei fest, da NFS-Clients über keine Protokollvorgänge verfügen, die ein schreibgeschütztes Bit pro Datei verwenden.

ONTAP kann ein schreibgeschütztes Bit auf einer Datei festlegen, wenn ein SMB-Client, der Windows verwendet, diese Datei erstellt. ONTAP kann auch ein schreibgeschütztes Bit festlegen, wenn eine Datei zwischen NFS-Clients und SMB-Clients gemeinsam genutzt wird. Für einige Software, die von NFS-Clients und SMB-Clients verwendet wird, ist die Aktivierung des Read-Only-Bits erforderlich.

Damit ONTAP die entsprechenden Lese- und Schreibberechtigungen auf eine von NFS Clients und SMB Clients gemeinsam genutzte Datei vorhält, behandelt es das schreibgeschützte Bit gemäß den folgenden Regeln:

- NFS behandelt jede Datei mit aktiviertem Read-Only-Bit, als ob keine Write-Berechtigungsbits aktiviert sind.
- Wenn ein NFS-Client alle Write-Berechtigungsbits deaktiviert und mindestens eines dieser Bits zuvor aktiviert wurde, aktiviert ONTAP das schreibgeschützte Bit für diese Datei.
- Wenn ein NFS-Client ein Schreibberechtigungs-Bit aktiviert, deaktiviert ONTAP das schreibgeschützte Bit für diese Datei.
- Wenn das schreibgeschützte Bit für eine Datei aktiviert ist und ein NFS-Client versucht, Berechtigungen für die Datei zu ermitteln, werden die Berechtigungsbits für die Datei nicht an den NFS-Client gesendet. Stattdessen sendet ONTAP die Berechtigungsbits an den NFS-Client mit maskierten Schreibberechtigungs-Bits.
- Wenn das schreibgeschützte Bit für eine Datei aktiviert ist und ein SMB-Client das schreibgeschützte Bit deaktiviert, aktiviert ONTAP das Schreibberechtigungsbit des Eigentümers für die Datei.
- Dateien mit aktiviertem Read-Only-Bit sind nur als Root beschreibbar.



Änderungen an Dateiberechtigungen wirken sich unmittelbar auf SMB-Clients aus, wirken sich jedoch möglicherweise nicht unmittelbar auf NFS-Clients aus, wenn der NFS-Client das Caching von Attributen ermöglicht.

## Wie unterscheidet sich ONTAP von Windows bei der Handhabung von Sperren auf Share-Pfad-Komponenten

Im Gegensatz zu Windows sperrt ONTAP nicht jede Komponente des Pfads zu einer geöffneten Datei, während die Datei geöffnet ist. Dieses Verhalten wirkt sich auch auf die SMB-Freigabungspfade aus.

Da ONTAP nicht jede Komponente des Pfads sperrt, ist es möglich, eine Pfadkomponente über der offenen Datei oder Freigabe umzubenennen, was zu Problemen für bestimmte Anwendungen führen kann oder dass der Freigabepfad in der SMB-Konfiguration ungültig ist. Dies kann dazu führen, dass der Share nicht zugänglich ist.

Um Probleme zu vermeiden, die durch die Umbenennung von Pfadkomponenten verursacht werden, können Sie Windows Access Control List (ACL)-Sicherheitseinstellungen anwenden, die verhindern, dass Benutzer oder Anwendungen kritische Verzeichnisse umbenennen.

Weitere Informationen zu ["So verhindern Sie, dass Verzeichnisse umbenannt werden, während Clients auf sie zugreifen"](#).

## Informationen zu Sperren anzeigen

Sie können Informationen über die aktuellen Dateisperren anzeigen, einschließlich der Arten von Sperren und des Sperrstatus, Informationen über Byte-Range-Sperren, Sharlock-Modi, Delegiertersicherungen und opportunistische Sperren sowie darüber, ob Sperren mit langlebigen oder dauerhaften Griffen geöffnet werden.

### Über diese Aufgabe

Die Client-IP-Adresse kann nicht für Sperren angezeigt werden, die über NFSv4 oder NFSv4.1 eingerichtet wurden.

Standardmäßig werden mit dem Befehl Informationen zu allen Sperren angezeigt. Mit den Befehlsparametern können Informationen über Sperren für eine bestimmte Storage Virtual Machine (SVM) angezeigt oder die Ausgabe des Befehls nach anderen Kriterien gefiltert werden.

Der `vserver locks show` Befehl zeigt Informationen zu vier Arten von Sperren an:

- Byte-Bereich-Locks, die nur einen Teil einer Datei sperren.
- Sperren freigeben, die geöffnete Dateien sperren
- Opportunistische Sperren, die das Client-seitige Caching über SMB steuern.
- Delegierungen, die das Caching des Clients über NFSv4.x steuern

Durch die Angabe optionaler Parameter können Sie wichtige Informationen zu jedem Sperrtyp ermitteln. Weitere Informationen finden Sie auf der man-Page des Befehls.

### Schritt

1. Zeigen Sie Informationen über Sperren mithilfe des `an vserver locks show` Befehl.

## Beispiele

Im folgenden Beispiel werden zusammenfassende Informationen für eine NFSv4-Sperre auf einer Datei mit dem Pfad angezeigt `/voll1/file1`. Der Zugriffsmodus für sharlock ist `write-Deny_none`, und die Sperre wurde mit der Schreibdelegation gewährt:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path          LIF          Protocol  Lock Type  Client
-----  -----
-----
voll1   /voll1/file1           lif1         nfsv4     share-level -
                Sharelock Mode: write-deny_none
                Delegation Type: write
```

Das folgende Beispiel zeigt detaillierte oplock- und Share-Informationen über die SMB-Sperre auf einer Datei mit dem Pfad `/data2/data2_2/intro.pptx`. Ein dauerhafter Handle wird auf der Datei mit einem Zugriffsmodus für die Freigabesperre von `write-Deny_none` einem Client mit einer IP-Adresse von `10.3.1.3` gewährt. Ein Lease Oplock wird mit einem Batch-Oplock-Niveau gewährt:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                Vserver: vs1
                Volume: data2_2
                Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
                Lock Protocol: cifs
                Lock Type: share-level
                Node Holding Lock State: node3
                Lock State: granted
                Bytelock Starting Offset: -
                Number of Bytes Locked: -
                Bytelock is Mandatory: -
                Bytelock is Exclusive: -
                Bytelock is Superlock: -
                Bytelock is Soft: -
                Oplock Level: -
                Shared Lock Access Mode: write-deny_none
                Shared Lock is Soft: false
                Delegation Type: -
                Client Address: 10.3.1.3
                SMB Open Type: durable
                SMB Connect State: connected
                SMB Expiration Time (Secs): -
```

```
SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

      Vserver: vs1
      Volume: data2_2
Logical Interface: lif2
      Object Path: /data2/data2_2/test.pptx
      Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
      Lock Protocol: cifs
      Lock Type: op-lock
Node Holding Lock State: node3
      Lock State: granted
Bytelock Starting Offset: -
      Number of Bytes Locked: -
      Bytelock is Mandatory: -
      Bytelock is Exclusive: -
      Bytelock is Superlock: -
      Bytelock is Soft: -
      Oplock Level: batch
Shared Lock Access Mode: -
      Shared Lock is Soft: -
      Delegation Type: -
      Client Address: 10.3.1.3
      SMB Open Type: -
      SMB Connect State: connected
SMB Expiration Time (Secs): -
      SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

## Sperrern

Wenn Dateisperren den Client-Zugriff auf Dateien verhindern, können Sie Informationen zu derzeit gespeicherten Sperrern anzeigen und bestimmte Sperrern anschließend unterbrechen. Beispiele für Szenarien, in denen Sie Sperrern benötigen, sind Debugging-Anwendungen.

### Über diese Aufgabe

Der `vserver locks break` Befehl ist nur auf der erweiterten Berechtigungsebene und höher verfügbar. Die man-Page für den Befehl enthält detaillierte Informationen.

### Schritte

1. Um die Informationen zu finden, die Sie benötigen, um eine Sperre zu brechen, verwenden Sie die `vserver locks show` Befehl.

Die man-Page für den Befehl enthält detaillierte Informationen.

2. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

3. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie eine Sperre brechen möchten, indem Sie...	Geben Sie den Befehl ein...
Der Name der SVM, der Name des Volumes, der LIF-Name und der Dateipfad	<code>vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif</code>
Die Lock-ID	<code>vserver locks break -lockid UUID</code>

4. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

## Wie FPolicy Filter zum ersten Lesen und Schreiben mit NFS funktionieren

NFS-Clients erleben während hoher Lese-/Schreib-Traffic-Anforderungen eine hohe Reaktionszeit, wenn die FPolicy über einen externen FPolicy-Server mit Lese-/Schreibvorgängen als überwachte Ereignisse aktiviert wird. Für NFS-Clients verringert die Verwendung von Filtern mit dem ersten Lesen und Schreiben in der FPolicy die Anzahl an FPolicy Benachrichtigungen und verbessert die Performance.

In NFS führt der Client I/O-Vorgänge in einer Datei aus, indem er den Griff ruft. Dieses Handle bleibt bei einem Neustart des Servers und des Clients unter Umständen weiterhin gültig. Somit kann der Client den Griff zwischenspeichern und Anfragen darauf senden, ohne die Griffe erneut abzurufen. In einer normalen Sitzung werden viele Lese-/Schreibanfragen an den Dateiserver gesendet. Wenn Benachrichtigungen für alle diese Anforderungen erzeugt werden, kann dies zu folgenden Problemen führen:

- Eine größere Last durch zusätzliche Benachrichtigungsverarbeitung und höhere Reaktionszeit.
- Eine große Anzahl von Benachrichtigungen an den FPolicy-Server gesendet wird, obwohl der Server von allen Benachrichtigungen nicht betroffen ist.

Nachdem Sie die erste Lese-/Schreibanforderung eines Clients für eine bestimmte Datei erhalten haben, wird ein Cache-Eintrag erstellt und die Anzahl der Lese-/Schreibvorgänge wird erhöht. Diese Anforderung wird als erster Lese-/Schreibvorgang markiert und ein FPolicy-Ereignis generiert. Bevor Sie Ihre FPolicy Filter für einen NFS-Client planen und erstellen, sollten Sie die Grundlagen der Funktionsweise von FPolicy-Filtern verstehen.

- First-read: Filtert die Leseanforderungen des Clients nach First-Read.

Wenn dieser Filter für NFS-Ereignisse verwendet wird, wird der angezeigt `-file-session-io -grouping-count` Und `-file-session-io-grouping-duration` Einstellungen bestimmen die First-Read-Anforderung, für die FPolicy verarbeitet wird.

- First-Write: Filtert die Schreibanforderungen des Clients nach First-Write.

Wenn dieser Filter für NFS-Ereignisse verwendet wird, wird der angezeigt `-file-session-io -grouping-count` Und `-file-session-io-grouping-duration` Einstellungen bestimmen die First-Write-Anforderung, für die FPolicy verarbeitet wurde.

Die folgenden Optionen werden in der NFS-Server-Datenbank hinzugefügt.

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

## Ändern der Implementierungs-ID für den NFSv4.1-Server

Das NFSv4.1 Protokoll enthält eine Server-Implementierungs-ID zur Dokumentation der Server-Domäne, des Namens und des Datums. Sie können die Server-Implementierungs-ID-Standardwerte ändern. Das Ändern der Standardwerte kann sich beispielsweise beim Sammeln von Nutzungsstatistiken oder bei der Behebung von Interoperabilitätsproblemen hilfreich erweisen. Weitere Informationen finden Sie unter RFC 5661.

### Über diese Aufgabe

Die Standardwerte für die drei Optionen lauten wie folgt:

Option	Optionsname	Standardwert
NFSv4.1 Implementierung ID Domain	-v4.1-implementation -domain	netapp.com
Name der NFSv4.1 Implementierung	-v4.1-implementation-name	Name der Cluster-Version
Datum der NFSv4.1 Implementierung-ID	-v4.1-implementation-date	Datum der Cluster-Version

### Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie die NFSv4.1 Implementierungs-ID ändern möchten...	Geben Sie den Befehl ein...
Domäne	<pre>vserver nfs modify -v4.1 -implementation-domain domain</pre>

Wenn Sie die NFSv4.1 Implementierungs-ID ändern möchten...	Geben Sie den Befehl ein...
Name	<code>vserver nfs modify -v4.1 -implementation-name name</code>
Datum	<code>vserver nfs modify -v4.1 -implementation-date date</code>

3. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

## Managen Sie NFSv4-ACLs

### Vorteile durch die Aktivierung von NFSv4 ACLs

Die Aktivierung von NFSv4-ACLs bietet viele Vorteile.

Die Aktivierung von NFSv4-ACLs bietet folgende Vorteile:

- Feinere Kontrolle des Benutzerzugriffs für Dateien und Verzeichnisse
- Bessere NFS-Sicherheit
- Bessere Interoperabilität mit CIFS
- Entfernung der NFS Einschränkung von 16 Gruppen pro Benutzer

### Funktionsweise von NFSv4 ACLs

Ein Client, der NFSv4 ACLs verwendet, kann ACLs auf Dateien und Verzeichnissen im System festlegen und anzeigen. Wenn eine neue Datei oder ein Unterverzeichnis in einem Verzeichnis erstellt wird, das über eine ACL verfügt, übernimmt die neue Datei oder das Unterverzeichnis alle ACL-Einträge (Aces) in der ACL, die mit den entsprechenden Vererbungsflags markiert wurden.

Wenn eine Datei oder ein Verzeichnis als Ergebnis einer NFSv4-Anforderung erstellt wird, hängt die ACL für die resultierende Datei oder das Verzeichnis davon ab, ob die Dateierstellungsanforderung eine ACL oder nur standardmäßige UNIX-Zugriffsberechtigungen enthält und ob das übergeordnete Verzeichnis über eine ACL verfügt:

- Wenn die Anforderung eine ACL enthält, wird diese ACL verwendet.
- Wenn die Anforderung nur Standardzugriffsberechtigungen für UNIX-Dateien enthält, aber das übergeordnete Verzeichnis über eine ACL verfügt, werden die Aces in der ACL des übergeordneten Verzeichnisses von der neuen Datei oder dem neuen Verzeichnis geerbt, solange die Aces mit den entsprechenden Vererbung-Flags gekennzeichnet wurden.



Eine übergeordnete ACL wird auch dann geerbt, wenn `-v4.0-ac1` ist auf festgelegt `off`.

- Wenn die Anforderung nur standardmäßige UNIX-Dateizugriffsberechtigungen enthält und das



übergeordnete Verzeichnis keine ACL besitzt, wird der Client-Dateimodus verwendet, um standardmäßige UNIX-Dateizugriffsberechtigungen festzulegen.

- Wenn die Anforderung nur Standardberechtigungen für den UNIX-Dateizugriff enthält und das übergeordnete Verzeichnis über eine nicht vererbte ACL verfügt, wird das neue Objekt nur mit Modus-Bits erstellt.



Wenn der `-chown-mode` Parameter wurde auf festgelegt `restricted` Mit Befehlen im `vserver nfs` Oder `vserver export-policy rule` Familien, Eigentümer von Dateien können nur durch den Superuser geändert werden, auch wenn die auf der Festplatte mit NFSv4 ACLs festgelegten Berechtigungen einem nicht-Root-Benutzer erlauben, die Eigentümer der Datei zu ändern. Weitere Informationen finden Sie auf den entsprechenden man-Pages.

## Aktivieren oder deaktivieren Sie die Änderung von NFSv4-ACLs

Wenn ONTAP einen erhält `chmod` Befehl für eine Datei oder ein Verzeichnis mit einer ACL wird standardmäßig die ACL beibehalten und geändert, um die Mode-Bit-Änderung zu berücksichtigen. Sie können den deaktivieren `-v4-acl-preserve` Parameter zum Ändern des Verhaltens, wenn stattdessen die ACL gelöscht werden soll.

### Über diese Aufgabe

Bei der Verwendung von Unified Security Style gibt dieser Parameter außerdem an, ob NTFS-Dateiberechtigungen erhalten oder verworfen werden, wenn ein Client einen `chmod`-, `chgroup`- oder `chown`-Befehl für eine Datei oder ein Verzeichnis sendet.

Die Standardeinstellung für diesen Parameter ist aktiviert.

### Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den folgenden Befehl ein...
Aufbewahrung und Änderung vorhandener NFSv4 ACLs aktivieren (Standard)	<code>vserver nfs modify -vserver vserver_name -v4-acl-preserve enabled</code>
Deaktivieren Sie die Aufbewahrung und legen Sie NFSv4-ACLs ab, wenn die Modus-Bits geändert werden	<code>vserver nfs modify -vserver vserver_name -v4-acl-preserve disabled</code>

3. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

## Wie ONTAP NFSv4 ACLs verwendet, um zu bestimmen, ob es eine Datei löschen kann

Um zu ermitteln, ob eine Datei gelöscht werden kann, verwendet ONTAP eine Kombination aus DEM DELETE-Bit der Datei und dem das zugehörige Directory DELETE\_CHILD. Weitere Informationen finden Sie im NFS 4.1 RFC 5661.

### Aktivieren oder Deaktivieren von NFSv4-ACLs

Um NFSv4-ACLs zu aktivieren oder zu deaktivieren, können Sie die ändern `-v4.0-acl` Und `-v4.1-acl` Optionen: Diese Optionen sind standardmäßig deaktiviert.

#### Über diese Aufgabe

Der `-v4.0-acl` Oder `-v4.1-acl` Option steuert die Einstellung und Ansicht von NFSv4 ACLs; es kontrolliert nicht die Durchsetzung dieser ACLs für die Zugriffsprüfung.

#### Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Dann...
Aktivieren Sie NFSv4.0 ACLs	Geben Sie den folgenden Befehl ein:  <pre>vserver nfs modify -vserver vserver_name -v4.0-acl enabled</pre>
Deaktivieren Sie NFSv4.0 ACLs	Geben Sie den folgenden Befehl ein:  <pre>vserver nfs modify -vserver vserver_name -v4.0-acl disabled</pre>
Aktivieren Sie NFSv4.1 ACLs	Geben Sie den folgenden Befehl ein:  <pre>vserver nfs modify -vserver vserver_name -v4.1-acl enabled</pre>
Deaktivieren Sie NFSv4.1 ACLs	Geben Sie den folgenden Befehl ein:  <pre>vserver nfs modify -vserver vserver_name -v4.1-acl disabled</pre>

### Ändern Sie das maximale ACE-Limit für NFSv4 ACLs

Sie können die maximal zulässige Anzahl von Asse für jede NFSv4-ACL ändern, indem Sie den Parameter ändern `-v4-acl-max-aces`. Standardmäßig ist das Limit für jede ACL auf 400 Asse eingestellt. Durch das Erhöhen dieser Beschränkung können Daten mit ACLs, die über 400 ACLs zu Storage-Systemen mit ONTAP enthalten, erfolgreich migriert werden.

#### Über diese Aufgabe

Wenn Sie diese Grenze vergrößern, kann dies Auswirkungen auf die Performance für Clients haben, die mit NFSv4-ACLs auf Dateien zugreifen.

### Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Ändern Sie das maximale ACE-Limit für NFSv4 ACLs:

```
vserver nfs modify -v4-acl-max-aces max_ace_limit
```

Der gültige Bereich von

max\_ace\_limit ist 192 Bis 1024.

3. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

## Managen der NFSv4-Dateidelegationen

### Aktivieren oder deaktivieren Sie NFSv4-Lesedatei-Delegationen

Um NFSv4-Delegationen für Lesedateien zu aktivieren oder zu deaktivieren, können Sie die ändern `-v4.0-read-delegation` Oder Option. Durch die Aktivierung von Read-File-Delegationen können Sie einen Großteil des Nachrichtenaufwands für das Öffnen und Schließen von Dateien beseitigen.

#### Über diese Aufgabe

Standardmäßig sind Lesedatei-Delegationen deaktiviert.

Der Nachteil bei der Aktivierung der Lesedatei-Delegationen besteht darin, dass der Server und seine Clients die Delegationen wiederherstellen müssen, nachdem der Server neu gestartet oder neu gestartet wurde, ein Client neu gestartet oder neu gestartet wurde oder eine Netzwerkpartition stattfindet.

#### Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Dann...
Aktivieren Sie die NFSv4-Delegation für Lesedateien	Geben Sie den folgenden Befehl ein:  <pre>vserver nfs modify -vserver vserver_name -v4.0-read-delegation enabled</pre>

Aktivieren der NFSv4.1-Dateidelegationen	Geben Sie den folgenden Befehl ein:  + vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled
Deaktivieren Sie NFSv4-Lesedelegierungen	Geben Sie den folgenden Befehl ein:  vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled
Deaktivieren Sie NFSv4.1 „Read File Delegationen“	Geben Sie den folgenden Befehl ein:  vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled

### Ergebnis

Die Optionen für die Dateidelegation werden wirksam, sobald sie geändert wurden. Es ist nicht erforderlich, NFS neu zu starten oder neu zu starten.

### Aktivieren oder Deaktivieren von NFSv4-Schreibdateidelegationen

Zum Aktivieren oder Deaktivieren von Delegierungen für Schreibdatei können Sie den ändern `-v4.0-write-delegation` Oder Option. Durch die Aktivierung von Write-File-Delegationen können Sie einen Großteil des Nachrichtenüberaufwands, der mit der Datei- und Datensatzsperrung verbunden ist, sowie das Öffnen und Schließen von Dateien eliminieren.

### Über diese Aufgabe

Standardmäßig sind die Delegierungen der Schreibdatei deaktiviert.

Der Nachteil bei der Aktivierung von Delegierungen von Schreibdateien besteht darin, dass der Server und seine Clients zusätzliche Aufgaben zur Wiederherstellung von Delegierungen durchführen müssen, nachdem der Server neu gestartet oder neu gestartet wurde, ein Client neu gestartet oder neu gestartet wurde oder eine Netzwerkpartition erfolgt.

### Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Dann...
Aktivieren Sie NFSv4-Delegation für Schreibdateien	Geben Sie den folgenden Befehl ein: vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled
Aktivieren Sie NFSv4.1-Schreibdateidelegationen	Geben Sie den folgenden Befehl ein: vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled

Ihr Ziel ist	Dann...
Deaktivieren Sie NFSv4-Schreibdateidelegationen	Geben Sie den folgenden Befehl ein: <code>vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled</code>
Deaktivieren Sie NFSv4.1 „Write File Delegationen“	Geben Sie den folgenden Befehl ein: <code>vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled</code>

## Ergebnis

Die Optionen für die Dateidelegation werden wirksam, sobald sie geändert wurden. Es ist nicht erforderlich, NFS neu zu starten oder neu zu starten.

## Konfigurieren der NFSv4-Datei und der Datensatzsperrung

### Allgemeines zur NFSv4-Datei und zum Sperren von Aufzeichnungen

Für NFSv4-Clients unterstützt ONTAP den NFSv4-Mechanismus zum Sperren von Dateien, wobei der Status aller Dateisperren unter einem Leasing-basierten Modell gewahrt bleibt.

["Technischer Bericht von NetApp 3580: NFSv4 Enhancements and Best Practices Guide Data ONTAP Implementation"](#)

### Geben Sie den Leasing-Zeitraum für das Sperren durch NFSv4 an

Um die NFSv4-Sperrfrist für das Leasing anzugeben (d. h. der Zeitraum, in dem ONTAP einem Kunden unwiderruflich ein Schloss zugibt), können Sie das ändern `-v4-lease -seconds` Option. Durch kürzere Leasing-Zeiten wird die Server-Recovery beschleunigt, während längere Leasing-Zeiten für Server mit einer sehr großen Anzahl von Clients von Vorteil sind.

### Über diese Aufgabe

Standardmäßig ist diese Option auf festgelegt 30. Der Mindestwert für diese Option ist 10. Der Maximalwert für diese Option ist die Sperrfrist, die Sie mit dem festlegen können `locking.lease_seconds` Option.

### Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Geben Sie den folgenden Befehl ein:

```
vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
```

3. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

## Geben Sie die Kulanzzeit für die NFSv4-Sperrung an

Um die Kulanzzeit für die NFSv4-Sperrung festzulegen (das heißt, der Zeitraum, in dem Clients versuchen, ihren Sperrstatus während der Server-Wiederherstellung von ONTAP zurückzufordern), können Sie das ändern `-v4-grace-seconds` Option.

### Über diese Aufgabe

Standardmäßig ist diese Option auf festgelegt 45.

### Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Geben Sie den folgenden Befehl ein:

```
vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
```

3. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

## Funktionsweise von NFSv4-Empfehlungen

Wenn Sie NFSv4-Empfehlungen aktivieren, bietet ONTAP Empfehlungen „`intra-SVM`“ zu NFSv4-Clients. Verweis auf SVM innerhalb eines Clusters, der die NFSv4-Anforderung empfängt, bezeichnet den NFSv4-Client auf eine andere logische Schnittstelle (LIF) auf der Storage Virtual Machine (SVM).

Der NFSv4-Client sollte von diesem Punkt an auf den Pfad zugreifen, der die Empfehlung an die Ziel-LIF erhalten hat. Der ursprüngliche Cluster-Node stellt derartige Empfehlungen bereit, wenn festgestellt wird, dass in der SVM eine LIF vorhanden ist, die sich auf dem Cluster-Node befindet, auf dem sich das Daten-Volumen befindet. Auf diese Weise können Clients schneller auf die Daten zugreifen und eine zusätzliche Cluster-Kommunikation vermieden wird.

## Aktivieren oder Deaktivieren von NFSv4-Empfehlungen

Sie können NFSv4-Empfehlungen auf Storage Virtual Machines (SVMs) aktivieren, indem Sie die Optionen aktivieren `-v4-fsid-change` Und `-v4.0-referrals` Oder. Die Aktivierung DER NFSV4-Empfehlungen kann zu einem schnelleren Datenzugriff für NFSv4-Clients führen, die diese Funktion unterstützen.

### Was Sie benötigen

Wenn Sie NFS-Empfehlungen aktivieren möchten, müssen Sie zuerst Parallel NFS deaktivieren. Sie können beides nicht gleichzeitig aktivieren.

### Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein...
Aktivieren Sie NFSv4-Empfehlungen	<pre>vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled</pre>
Deaktivieren Sie NFSv4-Empfehlungen	<pre>vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled</pre>
Aktivieren Sie NFSv4.1 Empfehlungen	<pre>vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled</pre>
Deaktivieren Sie NFSv4.1 Empfehlungen	<pre>vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled</pre>

3. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

## Zeigt die NFS-Statistiken an

Sie können NFS-Statistiken für Storage Virtual Machines (SVMs) auf dem Storage-System anzeigen, um die Performance zu überwachen und Probleme zu diagnostizieren.

### Schritte

1. Verwenden Sie die `statistics catalog object show` Befehl zum Identifizieren der NFS-Objekte, aus denen Daten angezeigt werden können.

```
statistics catalog object show -object nfs*
```

2. Verwenden Sie die `statistics start` Und optional `statistics stop` Befehle zum Erfassen einer Datenprobe aus einem oder mehreren Objekten.

3. Verwenden Sie die `statistics show` Befehl zum Anzeigen der Beispieldaten.

### Beispiel: Monitoring der NFSv3 Performance

Das folgende Beispiel zeigt die Performance-Daten für das NFSv3-Protokoll.

Mit dem folgenden Befehl wird die Datenerfassung für einen neuen Probe gestartet:

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

Der folgende Befehl zeigt die Daten aus der Probe an, indem Zähler angegeben werden, die die Anzahl der erfolgreichen Lese- und Schreibanforderungen gegenüber der Gesamtzahl der Lese- und Schreibanforderungen anzeigen:

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success
```

```
Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1
```

Counter	Value
read_success	40042
read_total	40042
write_success	1492052
write_total	1492052

## Verwandte Informationen

["Einrichtung der Performance-Überwachung"](#)

## Zeigt DNS-Statistiken an

Sie können DNS-Statistiken für Storage Virtual Machines (SVMs) auf dem Storage-System anzeigen, um die Performance zu überwachen und Probleme zu diagnostizieren.

### Schritte

1. Verwenden Sie die `statistics catalog object show` Befehl zum Identifizieren der DNS-Objekte, aus denen Daten angezeigt werden können.

```
statistics catalog object show -object external_service_op*
```

2. Verwenden Sie die `statistics start` Und `statistics stop` Befehle zum Erfassen einer Datenprobe aus einem oder mehreren Objekten.
3. Verwenden Sie die `statistics show` Befehl zum Anzeigen der Beispieldaten.

## Überwachen der DNS-Statistiken

Die folgenden Beispiele zeigen Performance-Daten für DNS-Abfragen. Die folgenden Befehle starten die Datenerfassung für eine neue Probe:

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

Mit dem folgenden Befehl werden die Daten aus der Probe angezeigt, indem Sie Zähler angeben, die die Anzahl der gesendeten DNS-Abfragen im Vergleich zur Anzahl der empfangenen, fehlgeschlagenen oder



## Timeout-DNS-Abfragen anzeigen:

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses
```

```
Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1
```

Counter	Value
num_not_found_responses	0
num_request_failures	0
num_requests_sent	1
num_responses_received	1
num_successful_responses	1
num_timeouts	0

6 entries were displayed.

Mit dem folgenden Befehl werden Daten aus der Probe angezeigt, indem Zähler angegeben werden, die die Anzahl der Male anzeigen, die ein bestimmter Fehler für eine DNS-Abfrage auf dem jeweiligen Server empfangen wurde:

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count
```

```
Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1
```

Counter	Value
count	1
error_string	NXDOMAIN
server_ip_address	10.72.219.109

3 entries were displayed.

## Verwandte Informationen

## Zeigt NIS-Statistiken an

Sie können NIS-Statistiken für Storage Virtual Machines (SVMs) auf dem Storage-System anzeigen, um die Performance zu überwachen und Probleme zu diagnostizieren.

### Schritte

1. Verwenden Sie die `statistics catalog object show` Befehl zum Identifizieren der NIS-Objekte, aus denen Daten angezeigt werden können.

```
statistics catalog object show -object external_service_op*
```

2. Verwenden Sie die `statistics start` Und `statistics stop` Befehle zum Erfassen einer Datenprobe aus einem oder mehreren Objekten.
3. Verwenden Sie die `statistics show` Befehl zum Anzeigen der Beispieldaten.

### Überwachen von NIS-Statistiken

In den folgenden Beispielen werden Performancedaten für NIS-Abfragen angezeigt. Die folgenden Befehle starten die Datenerfassung für eine neue Probe:

```
vs1::*> statistics start -object external_service_op -sample-id  
nis_sample1  
vs1::*> statistics start -object external_service_op_error -sample-id  
nis_sample2
```

Mit dem folgenden Befehl werden die Daten aus der Probe angezeigt, indem Sie Zähler angeben, die die Anzahl der gesendeten NIS-Abfragen im Vergleich zur Anzahl der empfangenen, fehlgeschlagenen oder Zeitüberschreitung bei NIS-Abfragen anzeigen:

```
vs1:*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses
```

```
Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1
```

Counter	Value
num_not_found_responses	0
num_request_failures	1
num_requests_sent	2
num_responses_received	1
num_successful_responses	1
num_timeouts	0

6 entries were displayed.

Mit dem folgenden Befehl werden Daten aus der Probe angezeigt, indem Zähler angegeben werden, die die Anzahl der Male anzeigen, an denen ein bestimmter Fehler bei einer NIS-Abfrage auf dem jeweiligen Server empfangen wurde:

```
vs1:*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count
```

```
Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1
```

Counter	Value
count	1
error_string	YP_NOTFOUND
server_ip_address	10.227.13.221

3 entries were displayed.

## Verwandte Informationen

["Einrichtung der Performance-Überwachung"](#)

## Support für VMware vStorage via NFS

ONTAP unterstützt bestimmte VMware vStorage APIs zur Array Integration (VAAI) Funktionen in einer NFS Umgebung.

### Unterstützte Funktionen

Folgende Funktionen werden unterstützt:

- Copy-Offload

Ermöglicht es einem ESXi Host, Virtual Machines oder Virtual Machine Disks (VMDKs) direkt zwischen dem Quell- und Zielspeicherort zu kopieren, ohne den Host zu involvieren. Dies spart ESXi Host-CPU-Zyklen und Netzwerkbandbreite. Der Copy-Offload behält die Platzeffizienz bei, wenn das Quell-Volumen nur wenige Ressourcen beansprucht.

- Speicherplatzreservierung

Garantiert Speicherplatz für eine VMDK-Datei, indem Speicherplatz dafür reserviert wird.

### Einschränkungen

VMware vStorage via NFS weist folgende Einschränkungen auf:

- Offload-Vorgänge für Kopien können in den folgenden Szenarien fehlschlagen:
  - Während der Ausführung von Wafiron auf dem Quell- oder Ziel-Volumen, da es das Volumen vorübergehend offline nimmt
  - Während Sie das Quell- oder Ziel-Volumen verschieben
  - Während Sie die Quell- oder Ziel-LIF verschieben
  - Während der Durchführung von Takeover- oder Giveback-Vorgängen
  - Während Switchover- oder Switchback-Vorgänge durchgeführt werden
- Serverseitige Kopien können aufgrund von Formatunterschieden bei Datei-Handle im folgenden Szenario fehlschlagen:

Sie versuchen, Daten von SVMs zu kopieren, die derzeit oder zuvor qtrees in SVMs exportiert hatten, die in noch nie qtrees exportiert hatten. Um diese Einschränkung zu umgehen, können Sie mindestens einen qtree auf der Ziel-SVM exportieren.

### Verwandte Informationen

["Welche VAAI Offloaded Operationen werden von Data ONTAP unterstützt?"](#)

## Aktivieren oder deaktivieren Sie VMware vStorage über NFS

Mithilfe des können Sie die Unterstützung für VMware vStorage über NFS auf Storage Virtual Machines (SVMs) aktivieren oder deaktivieren `vserver nfs modify` Befehl.

### Über diese Aufgabe

Standardmäßig ist die Unterstützung für VMware vStorage via NFS deaktiviert.

### Schritte

1. Zeigen Sie den aktuellen vStorage Support-Status für SVMs an:

```
vserver nfs show -vserver vserver_name -instance
```

2. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den folgenden Befehl ein...
Aktivieren Sie den VMware vStorage Support	<pre>vserver nfs modify -vserver vserver_name -vstorage enabled</pre>
Deaktivieren Sie die VMware vStorage Unterstützung	<pre>vserver nfs modify -vserver vserver_name -vstorage disabled</pre>

### Nachdem Sie fertig sind

Bevor Sie diese Funktion nutzen können, müssen Sie das NFS-Plug-in für VMware VAAI installieren. Weitere Informationen finden Sie unter *Installation des NetApp NFS Plug-ins für VMware VAAI*.

### Verwandte Informationen

["NetApp Dokumentation: NetApp NFS Plug-in für VMware VAAI"](#)

## Aktivieren oder deaktivieren Sie rquota-Unterstützung

ONTAP unterstützt das Remote-Quotenprotokoll Version 1 (rquota v1). Das rquota Protokoll ermöglicht NFS-Clients, Quota Informationen für Benutzer von einem entfernten Rechner abzurufen. Mit dem können Sie rquota auf Storage Virtual Machines (SVMs) aktivieren, indem Sie die verwenden `vserver nfs modify` Befehl.

### Über diese Aufgabe

Standardmäßig ist rquota deaktiviert.

### Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den folgenden Befehl ein...
Rquota-Unterstützung für SVMs aktivieren	<pre>vserver nfs modify -vserver vserver_name -rquota enable</pre>
Deaktivieren Sie rquota-Unterstützung für SVMs	<pre>vserver nfs modify -vserver vserver_name -rquota disable</pre>

Weitere Informationen zu Kontingenten finden Sie unter ["Logisches Storage-Management"](#).

## Performance-Steigerung durch NFSv3 und NFSv4 durch Ändern der TCP-Übertragungsgröße

Sie können die Performance von NFSv3- und NFSv4-Clients verbessern, die über ein Netzwerk mit hoher Latenz mit Storage-Systemen verbunden sind, indem Sie die maximale TCP-Übertragungsgröße ändern.

Wenn Clients über ein Netzwerk mit hoher Latenz auf Storage-Systeme zugreifen, z. B. ein Wide Area Network (WAN) oder ein Metro Area Network (MAN) mit einer Latenz über 10 Millisekunden. Können Sie die Verbindungs-Performance möglicherweise verbessern, indem Sie die maximale TCP-Übertragungsgröße ändern. Clients, die in einem Netzwerk mit niedriger Latenz auf Storage-Systeme zugreifen, wie z. B. LAN (Local Area Network), können von der Änderung dieser Parameter kaum oder gar nicht profitieren. Wenn die Durchsatzverbesserung die Auswirkung auf die Latenz nicht überwiegt, sollten Sie diese Parameter nicht verwenden.

Um zu ermitteln, ob Ihre Storage-Umgebung von der Änderung dieser Parameter profitieren würde, sollten Sie zunächst eine umfassende Performance-Bewertung eines NFS-Clients mit schlechter Performance durchführen. Prüfen Sie, ob die geringe Performance auf eine übermäßige Paketumlaufzeit und kleine Anfragen beim Client zurückzuführen ist. Unter diesen Bedingungen können Client und Server die verfügbare Bandbreite nicht vollständig nutzen, da sie die meisten Arbeitszyklen verwenden, die darauf warten, dass kleine Anfragen und Antworten über die Verbindung übertragen werden.

Durch Erhöhung der Anfragegröße für NFSv3 und NFSv4 kann der Client und Server die verfügbare Bandbreite effektiver nutzen, um mehr Daten pro Einheit zu verschieben. Dadurch wird die Gesamteffizienz der Verbindung erhöht.

Beachten Sie, dass die Konfiguration zwischen dem Storage-System und dem Client variieren kann. Das Speichersystem und der Client unterstützen bei Übertragungsvorgängen eine maximale Größe von 1 MB. Wenn Sie jedoch das Speichersystem so konfigurieren, dass es maximal 1 MB Übertragungsgröße unterstützt, aber der Client nur 64 KB unterstützt, ist die Mount-Transfergröße auf 64 KB oder weniger begrenzt.

Bevor Sie diese Parameter ändern, müssen Sie beachten, dass dies zu einem zusätzlichen Speicherverbrauch auf dem Speichersystem für den Zeitraum führt, der für die Montage und Übertragung einer großen Reaktion erforderlich ist. Je mehr latenzarme Verbindungen zum Storage-System, desto höher ist der zusätzliche Speicherverbrauch. Bei Storage-Systemen mit hoher Speicherkapazität kann diese Änderung nur sehr geringe Auswirkungen haben. Bei Storage-Systemen mit niedriger Speicherkapazität kann es zu einer merklichen Verschlechterung der Performance kommen.

Die erfolgreiche Verwendung dieser Parameter hängt von der Fähigkeit ab, Daten von mehreren Nodes eines Clusters abzurufen. Die inhärente Latenz des Cluster-Netzwerks erhöht möglicherweise die gesamte Latenz der Antwort. Die gesamte Latenz erhöht sich bei der Verwendung dieser Parameter normalerweise. Daher können latenzkritische Workloads negative Auswirkungen haben.

## Ändern Sie die maximale Übertragungsgröße von NFSv3 und NFSv4 TCP

Sie können den ändern `-tcp-max-xfer-size` Option zum Konfigurieren der maximalen Übertragungsgrößen für alle TCP-Verbindungen mit den Protokollen NFSv3 und NFSv4.x.

### Über diese Aufgabe

Sie können diese Optionen für jede Storage Virtual Machine (SVM) einzeln ändern.

Ab ONTAP 9 beginnt der `v3-tcp-max-read-size` Und `v3-tcp-max-write-size` Optionen sind veraltet.

Sie müssen den verwenden `-tcp-max-xfer-size` Wählen Sie stattdessen.

### Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein...
Ändern Sie die maximale Übertragungsgröße von NFSv3 oder NFSv4 TCP	<pre>vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size</pre>

Option	Bereich	Standard
<code>-tcp-max-xfer-size</code>	8192 bis 1048576 Byte	65536 Byte



Die maximale Übertragungsgröße, die Sie eingeben, muss ein Vielfaches von 4 KB (4096 Byte) sein. Anfragen, die nicht richtig ausgerichtet sind, wirken sich negativ auf die Performance aus.

3. Verwenden Sie die `vserver nfs show -fields tcp-max-xfer-size` Mit diesem Befehl können Sie die Änderungen überprüfen.
4. Wenn Clients statische Mounts verwenden, heben Sie die Bereitstellung ab und montieren Sie sie neu, damit die neue Parametergröße wirksam wird.

### Beispiel

Mit dem folgenden Befehl wird die maximale Übertragungsgröße von NFSv3 und NFSv4.x TCP auf 1048576 Byte auf der SVM mit dem Namen `vs1` festgelegt:

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

## Konfigurieren Sie die Anzahl der Gruppen-IDs, die für NFS-Benutzer zulässig sind

Standardmäßig unterstützt ONTAP bis zu 32 Gruppen-IDs beim Umgang mit NFS-Anmeldedaten über Kerberos (RPCSEC\_GSS) Authentifizierung. Bei Verwendung der AUTH\_SYS-Authentifizierung beträgt die standardmäßige maximale Anzahl von Gruppen-IDs 16, wie in RFC 5531 definiert. Sie können das Maximum auf 1,024 erhöhen, wenn Sie Benutzer haben, die mehr als die Standardanzahl von Gruppen sind.

### Über diese Aufgabe

Wenn ein Benutzer mehr als die Standardanzahl von Gruppen-IDs in seinen Anmeldedaten hat, werden die übrigen Gruppen-IDs abgeschnitten und der Benutzer erhält beim Versuch, auf Dateien vom Speichersystem zuzugreifen, möglicherweise Fehler. Sie sollten die maximale Anzahl an Gruppen pro SVM auf eine Zahl festlegen, die die maximalen Gruppen in Ihrer Umgebung repräsentiert.

In der folgenden Tabelle werden die beiden Parameter von aufgeführt `vserver nfs modify` Befehl, mit dem die maximale Anzahl von Gruppen-IDs in drei Beispielkonfigurationen bestimmt wird:

Parameter	Einstellungen	Resultierende Gruppen-IDs Limit
-extended-groups-limit	32	RPCSEC_GSS: 32
-auth-sys-extended-groups	disabled  Dies sind die Standardeinstellungen.	AUTH_SYS: 16
-extended-groups-limit	256	RPCSEC_GSS: 256
-auth-sys-extended-groups	disabled	AUTH_SYS: 16
-extended-groups-limit	512	RPCSEC_GSS: 512
-auth-sys-extended-groups	enabled	AUTH_SYS: 512



Einige ältere NFS-Clients sind möglicherweise nicht mit AUTH\_SYS-erweiterten Gruppen kompatibel.

### Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Führen Sie die gewünschte Aktion aus:

Wenn Sie die maximal zulässige Anzahl von Hilfsgruppen festlegen möchten...	Geben Sie den Befehl ein...
Nur für RPCSEC_GSS und lassen Sie AUTH_SYS auf den Standardwert von 16 gesetzt	<code>vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled</code>
Sowohl für RPCSEC_GSS als auch AUTH_SYS	<code>vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled</code>

3. Überprüfen Sie die `-extended-groups-limit` Wert und überprüfen, ob AUTH\_SYS erweiterte Gruppen nutzt: `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`
4. Zurück zur Administratorberechtigungsebene:



```
set -privilege admin
```

### Beispiel

Das folgende Beispiel ermöglicht erweiterte Gruppen für die AUTH\_SYS-Authentifizierung und setzt die maximale Anzahl erweiterter Gruppen für AUTH\_SYS- und RPCSEC\_GSS-Authentifizierung auf 512. Diese Änderungen werden nur für Clients vorgenommen, die auf die SVM mit dem Namen vs1 zugreifen:

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
        them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
-----
vs1      enabled                    512

vs1::*> set -privilege admin
```

## Kontrolle des Root-Benutzerzugriffs auf NTFS-Sicherheitsdaten

Sie können ONTAP so konfigurieren, dass NFS-Clients Zugriff auf NTFS-Sicherheitsdaten und NTFS-Clients auf die Daten im NFS-Sicherheitsstil erhalten. Wenn Sie den NTFS-Sicherheitsstil bei einem NFS-Datenspeicher verwenden, müssen Sie entscheiden, wie der Root-Benutzer den Zugriff behandelt und die SVM (Storage Virtual Machine) entsprechend konfiguriert.

### Über diese Aufgabe

Wenn ein Root-Benutzer auf NTFS-Sicherheitsdaten zugreift, haben Sie zwei Optionen:

- Ordnen Sie den Root-Benutzer wie jeder andere NFS-Benutzer einem Windows-Benutzer zu und verwalten Sie den Zugriff nach NTFS ACLs.
- Ignorieren Sie NTFS ACLs und bieten Sie vollständigen Zugriff auf das Root.

### Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Führen Sie die gewünschte Aktion aus:

Wenn der Root-Benutzer...

Geben Sie den Befehl ein...

Werden einem Windows-Benutzer zugeordnet	<code>vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled</code>
Umgehen Sie die NT-ACL-Prüfung	<code>vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled</code>

Dieser Parameter ist standardmäßig deaktiviert.

Wenn dieser Parameter aktiviert ist, aber keine Namenszuweisung für den Root-Benutzer vorhanden ist, verwendet ONTAP für die Prüfung eine standardmäßige SMB-Administratoranmeldungs-Berechtigung.

3. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

## Unterstützte NFS-Versionen und -Clients

### Überblick über die unterstützten NFS-Versionen und -Clients

Bevor Sie NFS in Ihrem Netzwerk verwenden können, müssen Sie wissen, welche NFS-Versionen und Clients ONTAP unterstützt.

Diese Tabelle zeigt, dass größere und kleinere NFS-Protokollversionen standardmäßig in ONTAP unterstützt werden. Die Unterstützung weist standardmäßig nicht darauf hin, dass dies die früheste Version von ONTAP ist, die dieses NFS-Protokoll unterstützt.

Version	Standardmäßig aktiviert
NFSv3	Ja.
NFSv4.0	Ja, ab ONTAP 9.9.1
NFSv4.1	Ja, ab ONTAP 9.9.1
NFSv4.2	Ja, ab ONTAP 9.9.1
PNFS	Nein

Aktuelle Informationen dazu, welche NFS-Clients ONTAP unterstützt, finden Sie in der Interoperabilitäts-Matrix.

["NetApp Interoperabilitäts-Matrix-Tool"](#)

### NFSv4.0 wird von ONTAP unterstützt

ONTAP unterstützt alle obligatorischen Funktionen in NFSv4.0 mit Ausnahme der Sicherheitsmechanismen SPKM3 und LIPKEY.

Die folgende NFSV4-Funktion wird unterstützt:

- **\* COMPOUND\***

Ermöglicht einem Client, mehrere Dateivorgänge in einer einzigen RPC-Anforderung (Remote Procedure Call) anzufordern.

- **Dateidelegation**

Ermöglicht dem Server, Dateikontrolle an bestimmte Client-Typen für Lese- und Schreibzugriff zu delegieren.

- **Pseudo-fs**

Wird von NFSv4-Servern verwendet, um Mount-Punkte auf dem Speichersystem zu ermitteln. Es gibt kein Mount-Protokoll in NFSv4.

- **\* Verriegelung\***

Leasing-basiert: Es gibt keine separaten Protokolle NLM (Network Lock Manager) oder NSM (Network Status Monitor) in NFSv4.

Weitere Informationen zum NFSv4.0-Protokoll finden Sie unter RFC 3530.

## **Einschränkungen der ONTAP-Unterstützung für NFSv4**

Sie sollten mehrere Einschränkungen der ONTAP-Unterstützung für NFSv4 beachten.

- Die Delegierten-Funktion wird nicht von jedem Client-Typ unterstützt.
- In ONTAP 9.4 und früheren Versionen werden Namen mit nicht-ASCII-Zeichen auf anderen Volumes als UTF8-Volumes vom Speichersystem abgelehnt.

In ONTAP 9.5 und neueren Versionen unterliegen Volumes, die mit der Einstellung utf8mb4 Sprache erstellt und mit NFS v4 gemountet wurden, nicht mehr dieser Einschränkung.

- Alle Datei-Handles sind persistent; der Server gibt keine flüchtigen Datei-Handles.
- Migration und Replikation werden nicht unterstützt.
- NFSv4-Clients werden nicht mit Spiegelungen zur schreibgeschützten Lastverteilung unterstützt.

ONTAP leitet NFSv4-Clients an die Quelle der Load-Sharing-Spiegelung für direkten Lese- und Schreibzugriff.

- Benannte Attribute werden nicht unterstützt.
- Alle empfohlenen Attribute werden unterstützt, mit Ausnahme der folgenden:

- archive
- hidden
- homogeneous
- mimetype
- quota\_avail\_hard
- quota\_avail\_soft

- quota\_used
- system
- time\_backup



Obwohl sie das nicht unterstützt `quota*` Attribute: ONTAP unterstützt Benutzer- und Gruppenkontingente über das RQUOTA Side-Band-Protokoll.

## ONTAP Unterstützung für NFSv4.1

Ab ONTAP 9.8 ist `nconnect` standardmäßig verfügbar, wenn NFSv4.1 aktiviert ist.

Bei früheren NFS-Client-Implementierungen wird nur eine einzige TCP-Verbindung mit einem Mount verwendet. Im ONTAP kann eine einzelne TCP-Verbindung zu einem Engpass mit einer höheren IOPS werden. Ein `nconnect`-fähiger Client kann jedoch mehrere TCP-Verbindungen (bis zu 16) haben, die einem einzelnen NFS-Mount zugeordnet sind. Dieser NFS-Client vergrößert Dateivorgänge auf mehrere TCP-Verbindungen nach Round Robin-Verfahren und erzielt so einen höheren Durchsatz aus der verfügbaren Netzwerkbandbreite. `Nconnect` wird nur für NFSv3- und NFSv4.1-Mounts empfohlen.

Überprüfen Sie in der Dokumentation des NFS-Clients, ob `nconnect` in Ihrer Client-Version unterstützt wird.

NFSv4.1 ist standardmäßig in ONTAP 9.9.1 und höher aktiviert. In früheren Versionen können Sie die Aktivierung durch Angabe des aktivieren `-v4.1` Option und Einstellung auf `enabled` Beim Erstellen eines NFS-Servers auf der Storage Virtual Machine (SVM)

ONTAP unterstützt keine Delegationen auf Verzeichnis- und Dateiebene in NFSv4.1.

## ONTAP unterstützt NFSv4.2

Ab ONTAP 9.8 wird das NFSv4.2 Protokoll unterstützt, um den Zugriff für NFSv4.2-fähige Clients zu ermöglichen.

Standardmäßig ist NFSv4.2 in ONTAP 9.9.1 und höher aktiviert. In ONTAP 9.8 können Sie v4.2 aktivieren, indem Sie die angeben `-v4.1` Option und Einstellung auf `enabled` Beim Erstellen eines NFS-Servers auf der Storage Virtual Machine (SVM) Durch die Aktivierung von NFSv4.1 können Clients auch die NFSv4.1 Funktionen verwenden, während sie als v4.2 gemountet werden.

Die folgenden NFSv4.2 optionalen Funktionen werden unterstützt:

Merkmal	Unterstützt ab ...
Obligatorische Zugriffssteuerung (MAC) mit NFS	ONTAP 9.9.1
Erweiterte NFS-Attribute	ONTAP 9.12.1

Weitere NFSv4.2 optionale Funktionen werden später in einer ONTAP Version hinzugefügt.

### Aktivieren Sie die NFS v4.2-Sicherheitsetiketten

Ab ONTAP 9.9 können NFS-Sicherheitslabels aktiviert werden. Sie sind standardmäßig deaktiviert.

Bei NFS v4.2-Sicherheitsetiketten sind ONTAP-NFS-Server der MAC-Adresse (Pflichtzugriff) bewusst und speichern und abrufen von Clients gesendete `sec_Label`-Attribute.

Weitere Informationen finden Sie unter ["RFC 7240"](#)

Ab ONTAP 9.12.1 werden NFS v4.2-Sicherheitsetiketten bei NDMP-Dump-Vorgängen unterstützt. Wenn in früheren Versionen auf Dateien oder Verzeichnissen Sicherheitsetiketten gefunden werden, schlägt der Dump fehl.

### Schritte

1. Ändern Sie die Berechtigungseinstellung in erweitert:

```
set -privilege advanced
```

2. Sicherheitsetiketten aktivieren:

```
vserver nfs modify -vserver svm_name -v4.2-seclabel enabled
```

### Erweiterte NFS-Attribute aktivieren

Ab ONTAP 9.12.1 sind die erweiterten NFS-Attribute (`xattrs`) standardmäßig aktiviert.

Erweiterte Attribute sind von definierte NFS-Standardattribute ["RFC 8276"](#) Und wird in modernen NFS Clients aktiviert. Sie können dazu verwendet werden, benutzerdefinierte Metadaten an Filesystem-Objekte anzuhängen und sind von Interesse an erweiterten Sicherheitsimplementierungen.

Erweiterte NFS-Attribute werden derzeit für NDMP Dump-Vorgänge nicht unterstützt. Wenn erweiterte Attribute auf Dateien oder Verzeichnissen gefunden werden, wird der Dump fortgesetzt, die erweiterten Attribute jedoch nicht auf diesen Dateien oder Verzeichnissen gesichert.

Wenn Sie erweiterte Attribute deaktivieren müssen, verwenden Sie das `vserver nfs modify -v4.2 -xattrs disabled` Befehl.

## ONTAP-Unterstützung für Parallel NFS

ONTAP unterstützt Parallel NFS (pNFS). Das pNFS Protokoll bietet Performance-Verbesserungen, indem es Clients direkten Zugriff auf die Daten eines Dateisatzes bietet, der über mehrere Nodes eines Clusters verteilt ist. Damit können die Clients den optimalen Pfad zu einem Volume finden.

## Verwendung von festen Halterungen

Bei der Fehlerbehebung bei Montageproblemen müssen Sie sicher sein, dass Sie den richtigen Mount-Typ verwenden. NFS unterstützt zwei Mount-Typen: Weiche Mounts und harte Montage. Aus Gründen der Zuverlässigkeit sollten Sie nur harte Halterungen verwenden.

Sie sollten keine sanften Mounts verwenden, besonders wenn die Möglichkeit häufiger NFS Timeouts besteht. Aus diesen Zeitüberschreitungen können Race-Bedingungen auftreten, die zu Datenbeschädigung führen können.

# Abhängigkeiten von NFS- und SMB-Dateien und Verzeichnissen

## Überblick über die Benennungsabhängigkeiten von NFS und SMB-Dateien und Verzeichnissen

Die Namenskonventionen für Dateien und Verzeichnisse hängen sowohl von den Betriebssystemen der Netzwerk-Clients als auch von den Protokollen für die Dateifreigabe ab. Darüber hinaus hängen die Spracheinstellungen auf dem ONTAP-Cluster und den Clients ab.

Das Betriebssystem und die Dateifreigabeprotokolle bestimmen Folgendes:

- Zeichen, die ein Dateiname verwenden kann
- Groß-/Kleinschreibung eines Dateinamens

ONTAP unterstützt abhängig von der ONTAP Version mehrere Byte an Zeichen in Datei-, Verzeichnis- und qtree-Namen.

## Zeichen, die ein Datei- oder Verzeichnisname verwenden kann

Wenn Sie von Clients mit unterschiedlichen Betriebssystemen auf eine Datei oder ein Verzeichnis zugreifen, sollten Sie Zeichen verwenden, die in beiden Betriebssystemen gültig sind.

Wenn Sie beispielsweise UNIX verwenden, um eine Datei oder ein Verzeichnis zu erstellen, verwenden Sie keinen Doppelpunkt (:) im Namen, da der Doppelpunkt in MS-DOS-Datei- oder Verzeichnisnamen nicht zulässig ist. Da die Beschränkungen für gültige Zeichen von einem Betriebssystem zum anderen variieren, finden Sie in der Dokumentation Ihres Client-Betriebssystems weitere Informationen zu unzulässigen Zeichen.

## Groß-/Kleinschreibung von Datei- und Verzeichnisnamen in einer Multi-Protokoll-Umgebung

Datei- und Verzeichnisnamen werden bei NFS-Clients Groß-/Kleinschreibung berücksichtigt, und die Groß-/Kleinschreibung wird nicht berücksichtigt. Sie müssen die Auswirkungen in einer Multi-Protokoll-Umgebung und die Aktionen verstehen, die Sie bei der Angabe des Pfads beim Erstellen von SMB-Freigaben und beim Zugriff auf Daten innerhalb der Freigaben ergreifen müssen.

Wenn ein SMB-Client ein Verzeichnis mit dem Namen erstellt `testdir`, Sowohl SMB- als auch NFS-Clients zeigen den Dateinamen als an `testdir`. Wenn jedoch ein SMB-Benutzer später versucht, ein Verzeichnisnamen zu erstellen `TESTDIR`, Der Name ist nicht zulässig, da, für den SMB-Client, dieser Name derzeit existiert. Wenn ein NFS-Benutzer später ein Verzeichnis mit dem Namen erstellt `TESTDIR`, NFS- und SMB-Clients zeigen den Verzeichnisnamen anders an, wie folgt:

- Auf NFS-Clients werden beispielsweise beide Verzeichnisnamen angezeigt, wie sie erstellt wurden `testdir` Und `TESTDIR`, Weil Verzeichnisnamen die Groß-/Kleinschreibung beachten.
- SMB-Clients verwenden die 8.3 Namen, um zwischen den beiden Verzeichnissen zu unterscheiden. Ein Verzeichnis hat den Basisdateinamen. Zusätzlichen Verzeichnissen wird ein Dateiname von 8.3

zugewiesen.

- Auf SMB-Clients wird angezeigt `testdir` Und `TESTDI~1`.
- ONTAP erstellt das `TESTDI~1` Verzeichnisname zur Unterscheidung der beiden Verzeichnisse.

In diesem Fall müssen Sie den Namen 8.3 verwenden, wenn Sie einen Freigabepfad angeben, während Sie eine Freigabe auf einer Storage Virtual Machine (SVM) erstellen oder ändern.

Gleiches gilt für Dateien, wenn ein SMB-Client erstellt wird `test.txt`, Sowohl SMB- als auch NFS-Clients zeigen den Dateinamen als an `text.txt`. Wenn jedoch ein SMB-Benutzer später versucht, es zu erstellen `Test.txt`, Der Name ist nicht zulässig, da, für den SMB-Client, dieser Name derzeit existiert. Wenn ein NFS-Benutzer später eine Datei mit dem Namen erstellt `Test.txt`, NFS- und SMB-Clients zeigen den Dateinamen anders an, wie folgt:

- Auf NFS-Clients werden beide Dateinamen angezeigt, während sie erstellt wurden. `test.txt` Und `Test.txt`, Weil Dateinamen Groß- und Kleinschreibung beachten.
- SMB-Clients verwenden die 8.3 Namen, um zwischen den beiden Dateien zu unterscheiden. Eine Datei hat den Basisdateinamen. Zusätzlichen Dateien wird ein Dateiname von 8.3 zugewiesen.
  - Auf SMB-Clients wird angezeigt `test.txt` Und `TEST~1.TXT`.
  - ONTAP erstellt das `TEST~1.TXT` Dateiname zur Unterscheidung der beiden Dateien.



Wenn Sie die Zeichenzuordnung über die CIFS-Befehle zur Character Mapping von Vserver aktiviert oder geändert haben, wird bei einer Windows Lookup im Normalfall die Groß-/Kleinschreibung nicht berücksichtigt.

## Wie ONTAP Datei- und Verzeichnisnamen erstellt

ONTAP erstellt und pflegt zwei Namen für Dateien oder Verzeichnisse in jedem Verzeichnis, das Zugriff auf einen SMB-Client hat: Den ursprünglichen Long-Namen und einen Namen im 8.3-Format.

Bei Datei- oder Verzeichnisnamen, die den Namen von acht Zeichen oder die maximal drei Zeichen (für Dateien) überschreiten, generiert ONTAP wie folgt einen Namen im 8.3-Format:

- Der ursprüngliche Datei- oder Verzeichnisname wird auf sechs Zeichen gekürzt, wenn der Name sechs Zeichen überschreitet.
- Er fügt einen Tilde (~) und eine Zahl, eine bis fünf, an Datei- oder Verzeichnisnamen an, die nach dem Abschneiden nicht mehr eindeutig sind.

Wenn es aus Zahlen heraus läuft, weil es mehr als fünf ähnliche Namen gibt, erstellt es einen eindeutigen Namen, der keine Beziehung zum ursprünglichen Namen hat.

- Bei Dateien schneidet es die Dateinamenerweiterung auf drei Zeichen ab.

Beispiel: Wenn ein NFS-Client eine Datei mit dem Namen erstellt `specifications.html`, Der Dateiname im Format 8.3, der von ONTAP erstellt wurde, ist `specif~1.htm`. Wenn dieser Name bereits vorhanden ist, verwendet ONTAP am Ende des Dateinamens eine andere Nummer. Beispiel: Wenn ein NFS-Client dann eine andere Datei mit dem Namen erstellt `specifications_new.html`, Das Format 8.3 von `specifications_new.html` ist `specif~2.htm`.

## So verarbeitet ONTAP Datei-, Verzeichnis- und qtree-Namen mit mehreren Bytes

Ab ONTAP 9.5 ermöglicht die Unterstützung von 4-Byte-UTF-8-kodierten Namen die Erstellung und Anzeige von Datei-, Verzeichnis- und Baumnamen, die Unicode-Zusatzzeichen außerhalb der Basic Mehrsprachige Ebene (BMP) enthalten. In früheren Versionen wurden diese Zusatzzeichen in Multi-Protokoll-Umgebungen nicht korrekt angezeigt.

Um die Unterstützung von 4-Byte-UTF-8-kodierten Namen zu ermöglichen, steht für den ein neuer *utf8mb4* -Sprachcode zur Verfügung *vserver* Und *volume* Befehlsfamilien.

- Sie müssen ein neues Volume auf eine der folgenden Arten erstellen:
- Einstellen der Lautstärke *-language* Option explizit:

```
volume create -language utf8mb4 {...}
```

- Vererben des Volumes *-language* Option von einem SVM, der mit oder für die Option geändert wurde:

```
vserver [create|modify] -language utf8mb4 {...}``volume create {...}
```

- Vorhandene Volumes können nicht für die Unterstützung von *utf8mb4* geändert werden. Sie müssen ein neues *utf8mb4*-fähiges Volume erstellen und dann die Daten mithilfe clientbasierter Kopier-Tools migrieren.

Sie können SVMs für *utf8mb4*-Unterstützung aktualisieren, vorhandene Volumes behalten jedoch ihre ursprünglichen Sprachcodes bei.



LUN-Namen mit 4-Byte UTF-8 Zeichen werden derzeit nicht unterstützt.

- Unicode-Zeichendaten werden in der Regel in Windows-Dateisystemanwendungen mit dem 16-Bit-Unicode-Transformationsformat (UTF-16) und in NFS-Dateisystemen mit dem 8-Bit-Unicode-Transformationsformat (UTF-8) dargestellt.

In Versionen vor ONTAP 9.5 wurden Namen einschließlich UTF-16-Zusatzzeichen, die von Windows-Clients erstellt wurden, anderen Windows-Clients korrekt angezeigt, für NFS-Clients jedoch nicht richtig in UTF-8 übersetzt. Auch Namen mit UTF-8 Zusatzzeichen von erstellten NFS-Clients wurden für Windows-Clients nicht richtig in UTF-16 übersetzt.

- Wenn Sie Dateinamen auf Systemen mit ONTAP 9.4 oder einer älteren Version erstellen, die gültige oder ungültige Zusatzzeichen enthalten, weist ONTAP den Dateinamen zurück und gibt einen ungültigen Dateinamen zurück.

Um dieses Problem zu vermeiden, verwenden Sie nur BMP-Zeichen in Dateinamen und vermeiden Sie die Verwendung zusätzlicher Zeichen, oder aktualisieren Sie auf ONTAP 9.5 oder höher.

In *qtree*-Namen sind Unicode-Zeichen zulässig.

- Sie können entweder die verwenden *volume qtree* Befehlssfamilie oder System Manager zum Festlegen oder Ändern von *qtree*-Namen
- *Qtree*-Namen können mehrere Byte-Zeichen im Unicode-Format enthalten, z. B. japanische und chinesische Zeichen.
- In Releases vor ONTAP 9.5 wurden nur BMP-Zeichen unterstützt (also solche, die in 3 Byte dargestellt



werden konnten).



In Releases vor ONTAP 9.5 kann der Verbindungspfad des übergeordneten Volume des qtree qtree qtree qtree qtree qtree qtree und Verzeichnisnamen mit Unicode-Zeichen enthalten. Der `volume show` Befehl zeigt diese Namen korrekt an, wenn das übergeordnete Volume über eine UTF-8-Spracheinstellung verfügt. Wenn die übergeordnete Volume-Sprache jedoch nicht zu den UTF-8-Spracheinstellungen gehört, werden einige Teile des Verbindungspfads mit einem numerischen NFS-alternativen Namen angezeigt.

- In 9.5 und höher werden 4-Byte-Zeichen in qtree-Namen unterstützt, vorausgesetzt, der qtree ist in einem aktivierten Volume für utf8mb4.

## Konfigurieren Sie die Zeichenzuordnung für die Übersetzung von SMB-Dateinamen auf Volumes

NFS-Clients können Dateinamen mit Zeichen erstellen, die für SMB-Clients und bestimmte Windows-Applikationen nicht gültig sind. Sie können die Zeichenzuordnung für die Übersetzung von Dateinamen auf Volumes konfigurieren, damit SMB-Clients auf Dateien mit NFS-Namen zugreifen können, die ansonsten nicht gültig wären.

### Über diese Aufgabe

Wenn von NFS-Clients erstellte Dateien von SMB Clients abgerufen werden, wird der Name der Datei von ONTAP angezeigt. Wenn der Name kein gültiger SMB-Dateiname ist (z. B. wenn er ein eingebettetes Doppelpunkt “.” Zeichen hat), gibt ONTAP den Dateinamen von 8.3 zurück, der für jede Datei gepflegt wird. Dies führt jedoch zu Problemen für Anwendungen, die wichtige Informationen in lange Dateinamen kodieren.

Wenn Sie also eine Datei zwischen Clients auf verschiedenen Betriebssystemen gemeinsam nutzen, sollten Sie Zeichen in den Dateinamen verwenden, die in beiden Betriebssystemen gültig sind.

Wenn Sie jedoch NFS-Clients haben, die Dateinamen mit Zeichen erstellen, die keine gültigen Dateinamen für SMB-Clients sind, können Sie eine Karte definieren, die ungültige NFS-Zeichen in Unicode-Zeichen umwandelt, die sowohl SMB- als auch bestimmte Windows-Anwendungen akzeptieren. Diese Funktionalität unterstützt beispielsweise die CATIA MCAD- und Mathematica-Anwendungen sowie andere Anwendungen, die diese Anforderung haben.

Sie können die Zeichenzuordnung auf Volume-Basis konfigurieren.

Bei der Konfiguration der Zeichenzuordnung auf einem Volume müssen Sie Folgendes beachten:

- Die Zeichenzuordnung wird nicht über Kreuzungspunkte angewendet.

Sie müssen die Zeichenzuordnung für jedes Verbindungsvolume explizit konfigurieren.

- Sie müssen sicherstellen, dass die Unicode-Zeichen, die für ungültige oder illegale Zeichen verwendet werden, Zeichen sind, die normalerweise nicht in Dateinamen angezeigt werden. Andernfalls werden unerwünschte Zuordnungen angezeigt.

Wenn Sie beispielsweise versuchen, einen Doppelpunkt (:) einem Bindestrich (-) zuzuordnen, aber der Bindestrich (-) wurde im Dateinamen richtig verwendet, würde ein Windows-Client, der versucht, auf eine Datei namens „a-b“ zuzugreifen, seine Anfrage dem NFS-Namen „a : b“ zugeordnet haben (nicht das gewünschte Ergebnis).

- Wenn die Zuordnung nach dem Anwenden der Zeichenzuordnung noch ein ungültiges Windows-Zeichen

enthält, wird ONTAP auf Windows 8.3-Dateinamen zurückfallend.

- In FPolicy Benachrichtigungen, NAS-Prüfprotokollen und Security-Trace-Meldungen werden die zugeordneten Dateinamen angezeigt.
- Wenn eine SnapMirror Beziehung des Typs DP erstellt wird, wird die Charakterzuordnung des Quell-Volumes nicht auf dem Ziel-DP Volume repliziert.
- Case-Sensitivität: Da die zugeordneten Windows-Namen in NFS-Namen umgewandelt werden, folgt die Suche nach den Namen NFS-Semantik. Das schließt auch die Tatsache ein, dass NFS-Lookups Groß- und Kleinschreibung beachten. Das bedeutet, dass Anwendungen, die auf zugewiesene Freigaben zugreifen, nicht auf Groß- und Kleinschreibung von Windows angewiesen sein dürfen. Der Name 8.3 ist jedoch verfügbar, und der Groß-/Kleinschreibung wird nicht berücksichtigt.
- Partielle oder ungültige Zuordnungen: Nachdem ein Name zugeordnet wurde, um zu Clients zurückzukehren, die die Verzeichnisenumeration („dir“) ausführen, wird der resultierende Unicode-Name auf Windows-Gültigkeit überprüft. Wenn dieser Name noch ungültige Zeichen enthält oder wenn er ansonsten für Windows ungültig ist (z. B. endet er in "." oder leer), wird der Name 8.3 anstelle des ungültigen Namens zurückgegeben.

## Schritt

### 1. Zeichenzuordnung konfigurieren:

```
vserver cifs character-mapping create -vserver vserver_name -volume  
volume_name -mapping mapping_text, ...
```

Die Zuordnung besteht aus einer Liste von Quell-Ziel-Zeichenpaaren getrennt durch “.”. Bei den Zeichen handelt es sich um Unicode-Zeichen, die mit Hexadezimalziffern eingegeben werden. Zum Beispiel: 3C:E03C.

Der erste Wert jeder `mapping_text` Das Paar, das durch einen Doppelpunkt getrennt wird, ist der hexadezimale Wert des zu übersetzenden NFS-Zeichens, und der zweite Wert ist der Unicode-Wert, den SMB verwendet. Die Zuordnungspaare müssen eindeutig sein (es sollte ein 1:1-Mapping vorhanden sein).

- Quellenzuordnung

Die folgende Tabelle zeigt den zulässigen Unicode-Zeichensatz für die Quellenzuordnung:

Unicode-Zeichen	Gedrucktes Zeichen	Beschreibung
0x01-0x19	Keine Angabe	Nicht druckende Kontrollzeichen
0x5C	\	Umgekehrter Schrägstrich
0x3A	:	Doppelpunkt
0x2A	*	Sternchen
0x3F	?	Fragezeichen
0x22	”	Anführungszeichen
0x3C	<	Kleiner als

0x3E	>	Größer als
0x7C	.	Vertikale Linie
0xB1	±	Plus-Minus-Zeichen

- Zielzuordnung

Im Bereich „Private Use Area“ von Unicode können Sie Zielzeichen im folgenden Bereich angeben: U+E0000...U+F8FF.

### Beispiel

Mit dem folgenden Befehl wird eine Zeichenzuordnung für ein Volume mit dem Namen „data“ auf der Storage Virtual Machine (SVM) vs1 erstellt:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show
```

Vserver	Volume Name	Character Mapping
vs1	data	3c:e17c, 3e:f17d, 2a:f745

### Befehle zum Verwalten von Zeichenmappings für die Übersetzung von SMB-Dateinamen

Sie können die Zeichenzuordnung verwalten, indem Sie auf FlexVol Volumes für die Übersetzung von SMB-Dateinamen verwendete Dateizeichenzuordnungen erstellen, ändern, Informationen anzeigen oder löschen.

Ihr Ziel ist	Befehl
Neue Dateizeichenzuordnungen erstellen	<code>vserver cifs character-mapping create</code>
Informationen zur Zuordnung von Dateizeichen anzeigen	<code>vserver cifs character-mapping show</code>
Vorhandene Dateizeichenzuordnungen ändern	<code>vserver cifs character-mapping modify</code>
Dateizeichenzuordnungen löschen	<code>vserver cifs character-mapping delete</code>

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

## Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.