# Dateizugriff mit NFS verwalten

ONTAP 9

NetApp
November 05, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/nfs-admin/enable-disable-nfs-task.html on November 05, 2026. Always check docs.netapp.com for the latest.

# Inhalt


Dateizugriff mit NFS verwalten . . . 1
NFS für ONTAP SVMs aktivieren oder deaktivieren . . . 1
ONTAP NFSv4 Storepool-Limits verwalten . . . 4
Verbrauchte Storepool-Ressourcen anzeigen . . . 4
Aktivieren oder Deaktivieren der Storepool-Limitsteuerung . . . 5
Liste blockierter Clients . . . 5
Einen Client aus der Liste der blockierten Clients entfernen . . . 6
pNFS für ONTAP SVMs aktivieren oder deaktivieren . . . 6
NFS-Zugriff über TCP und UDP für ONTAP SVMs steuern . . . 7
NFS-Anfragen von nicht reservierten Ports für ONTAP SVMs steuern . . . 7
NFS-Zugriff auf ONTAP NTFS-Volumes oder Qtrees für unbekannte UNIX-Benutzer verwalten . . . 8
Hinweise für Clients, die ONTAP NFS-Exporte auf nicht reservierten Ports einbinden . . . 9
Strengere Zugriffskontrollen für Netgroups durch Überprüfung der Domains bei ONTAP NFS SVMs . . . 9
Ändern der für NFSv3-Services verwendeten Ports für ONTAP SVMs . . . 10
ONTAP Befehle zur Verwaltung von NFS Servern . . . 12
Behebung von Namensdienstproblemen für ONTAP NAS SVMs . . . 12
Namensdienstverbindungen für ONTAP NAS SVMs überprüfen . . . 15
ONTAP Befehle zur Verwaltung von NAS Name Service Switch-Einträgen . . . 16
ONTAP Befehle zur Verwaltung des NAS Name Service Cache . . . 17
ONTAP Befehle zur Verwaltung von NFS-Namenszuordnungen . . . 17
ONTAP Befehle zur Verwaltung lokaler UNIX-Benutzer für NAS . . . 18
ONTAP Befehle zur Verwaltung von NAS lokalen UNIX-Gruppen . . . 18
Grenzwerte für lokale UNIX-Benutzer, Gruppen und Gruppenmitglieder für ONTAP NFS SVMs . . . 19
Grenzwerte für lokale UNIX-Benutzer und -Gruppen für ONTAP NFS SVMs verwalten . . . 19
ONTAP Befehle zur Verwaltung lokaler NFS-Netgroups . . . 20
ONTAP Befehle zur Verwaltung von NFS NIS-Domänenkonfigurationen . . . 20
ONTAP Befehle zur Verwaltung von NFS-LDAP-Client-Konfigurationen . . . 21
ONTAP Befehle zur Verwaltung von NFS LDAP-Konfigurationen . . . 21
ONTAP Befehle zur Verwaltung von NFS LDAP-Client-Schemavorlagen . . . 22
ONTAP Befehle zur Verwaltung von NFS Kerberos-Schnittstellenkonfigurationen . . . 22
ONTAP Befehle zur Verwaltung von NFS Kerberos Realm-Konfigurationen . . . 23
ONTAP Befehle zur Verwaltung von Exportrichtlinien . . . 23
ONTAP Befehle zur Verwaltung von Exportregeln . . . 23
Den NFS-Anmeldeinformationscache konfigurieren . . . 24
Gründe für die Änderung der Gültigkeitsdauer des NFS-Anmeldeinformationscache für ONTAP SVMs . . . 24
Die Gültigkeitsdauer für zwischengespeicherte NFS-Benutzeranmeldeinformationen für ONTAP SVMs konfigurieren . . . 25
Exportrichtlinien-Caches verwalten . . . 26
Export-Policy-Caches für ONTAP NAS SVMs leeren . . . 26
Anzeige der Export-Policy-Netgroup-Warteschlange und des Caches für ONTAP NFS SVMs . . . 27
Es kann überprüft werden, ob eine Client-IP-Adresse Mitglied einer ONTAP NFS-Netgroup ist. . . . 28
Optimierung der Zugriffscache-Performance für ONTAP NFS SVMs . . . 29
Dateisperren verwalten . . . 30

Informationen zur Dateisperrung zwischen Protokollen für ONTAP NFS SVMs . . . 30
Informationen zu schreibgeschützten Bits für ONTAP NFS SVMs . . . 30
Unterschiede zwischen ONTAP NFS und Windows bei der Handhabung von Sperren auf Freigabepfadkomponenten . . . 31
Informationen zu Sperren für ONTAP NFS SVMs anzeigen . . . 32
Dateisperren für ONTAP NFS SVMs aufheben . . . 34
Funktionsweise der ONTAP FPolicy-Filter für Erstlesen und Erstschreiben mit NFS . . . 35
Die NFSv4.1-Serverimplementierungs-ID für ONTAP SVMs ändern . . . 36
NFSv4-ACLs verwalten . . . 37
Informationen zu den Vorteilen der Aktivierung von NFSv4-ACLs für ONTAP SVMs . . . 37
Informationen zu NFSv4-ACLs für ONTAP SVMs . . . 37
Aktivieren oder Deaktivieren der NFSv4-ACL-Änderung für ONTAP SVMs . . . 38
Wie ONTAP NFSv4-ACLs verwendet, um zu bestimmen, ob Dateien gelöscht werden können . . . 38
NFSv4-ACLs für ONTAP SVMs aktivieren oder deaktivieren . . . 38
Ändern des maximalen ACE-Limits für NFSv4-ACLs für ONTAP SVMs . . . 39
NFSv4 Dateidelegierungen verwalten . . . 40
Aktivieren oder Deaktivieren von NFSv4-Lesedelegationen für ONTAP SVMs . . . 40
NFSv4 Schreibdelegationen für ONTAP SVMs aktivieren oder deaktivieren . . . 40
Konfiguration der NFSv4 Datei- und Datensatzsperrung . . . 41
Informationen zur NFSv4 Datei- und Datensatzsperrung für ONTAP SVMs . . . 41
Die Sperrfrist für NFSv4-Locking bei ONTAP SVMs angeben . . . 41
Die NFSv4-Sperrfrist für ONTAP SVMs angeben . . . 42
Informationen zu NFSv4-Verweisen für ONTAP SVMs . . . 42
NFSv4-Verweise für ONTAP SVMs aktivieren oder deaktivieren . . . 43
Statistiken für ONTAP NFS SVMs anzeigen . . . 43
DNS-Statistiken für ONTAP NFS SVMs anzeigen . . . 44
Überwachung der DNS Statistiken . . . 45
NIS-Statistiken für ONTAP NFS SVMs anzeigen . . . 46
Überwachung der NIS Statistiken . . . 46
Informationen zur Unterstützung von VMware vStorage über ONTAP NFS . . . 48
Unterstützte Funktionen . . . 48
Einschränkungen . . . 48
VMware vStorage über ONTAP NFS aktivieren oder deaktivieren . . . 49
rquota-Unterstützung auf ONTAP NFS SVMs aktivieren oder deaktivieren . . . 50
Informationen zu Leistungsverbesserungen bei NFSv3 und NFSv4 sowie zur TCP-Übertragungsgröße für ONTAP SVMs . . . 50
Die maximale TCP-Übertragungsgröße für NFSv3 und NFSv4 bei ONTAP SVMs anpassen . . . 51
Die Anzahl der für NFS-Benutzer auf ONTAP SVMs zulässigen Gruppen-IDs konfigurieren . . . 52
Root-Benutzerzugriff auf NTFS-Sicherheitsdaten im Sicherheitsstil für ONTAP SVMs steuern . . . 54

# Dateizugriff mit NFS verwalten

## NFS für ONTAP SVMs aktivieren oder deaktivieren

Sie können NFS-Versionen über den System Manager oder die CLI aktivieren oder deaktivieren. Dies ermöglicht Dateizugriff für Clients, die das NFS-Protokoll verwenden.

In allen unterstützten Versionen von ONTAP 9 ist NFSv3 standardmäßig aktiviert. Ab ONTAP 9.9.1 sind NFSv4.1 und NFSv4.2 standardmäßig aktiviert; in früheren Versionen sind sie standardmäßig deaktiviert.

Ab ONTAP 9.19.1 können Sie NFSv4.1 und NFSv4.2 unabhängig voneinander aktivieren oder deaktivieren. Vor ONTAP 9.19.1 konnten Sie NFSv4.1 und NFSv4.2 nur gemeinsam aktivieren oder deaktivieren. Standardmäßig sind sowohl NFSv4.1 als auch NFSv4.2 aktiviert, wenn ein neuer NFS-Service erstellt wird, es sei denn, sie werden vom Administrator explizit deaktiviert.

**System Manager**

**Schritte**

1. Im System Manager wählen Sie **Cluster > Storage VMs**, wählen die Storage VM aus, wählen **Einstellungen** und dann ⚙ oder das ✎ unter **NFS** aus.
2. Aktivieren Sie das Kästchen **NFS aktivieren**.
3. Aktivieren oder Deaktivieren eines NFS-Protokolls:
   - Um NFSv3 zu aktivieren, wählen Sie das Kästchen **Unterstützung für Version 3 aktivieren** und ziehen Sie die folgende Option in Betracht:
     - Aktivieren Sie das Kästchen **64-Bit-FSIDs und Dateikennungen aktivieren**, um die Unterstützung für 64-Bit-Dateisystem-IDs und Dateikennungen für NFSv3 zu aktivieren.
   - Um NFSv3 zu deaktivieren, deaktivieren Sie das Kästchen **Unterstützung für Version 3 aktivieren**.
   - Um NFSv4.0 zu aktivieren, wählen Sie das Kästchen **Unterstützung für Version 4 aktivieren** und beachten Sie die folgenden Optionen:
     - Aktivieren Sie das Kästchen **ACL aktivieren**, um die Verwendung einer Zugriffssteuerungsliste zu ermöglichen.
     - Aktivieren Sie das Kästchen **Lese-Delegierung aktivieren**, um den schreibgeschützten Zugriff zu ermöglichen.
     - Aktivieren Sie das Kästchen **Schreibdelegation**, um Schreibzugriff zu ermöglichen.
     - Wählen Sie das Kästchen **64-Bit-FSIDs und Dateikennungen aktivieren** aus, um die Unterstützung für 64-Bit-Dateisystem-IDs und Dateikennungen zu aktivieren. Dieses Kästchen gilt für NFSv4.0, NFSv4.1 und NFSv4.2. Dies ist getrennt von dem Kästchen, das zur Steuerung der 64-Bit-Unterstützung für NFSv3 verwendet wird.
   - Um NFSv4.0 zu deaktivieren, deaktivieren Sie das Kästchen **Unterstützung für Version 4 aktivieren**.
   - Um NFSv4.1 zu aktivieren, wählen Sie das Kästchen **Unterstützung für Version 4.1 und 4.2 aktivieren** und anschließend das Kästchen **Unterstützung für Version 4.1 aktivieren**. Beachten Sie die folgenden Optionen:
     - Aktivieren Sie das Kästchen **ACL aktivieren**, um die Verwendung einer Zugriffssteuerungsliste zu ermöglichen.

        - Aktivieren Sie das Kästchen **Lese-Delegierung aktivieren**, um den schreibgeschützten Zugriff zu ermöglichen.
        - Aktivieren Sie das Kästchen **Schreibdelegation**, um Schreibzugriff zu ermöglichen.
        - Aktivieren Sie das **pNFS** Kästchen, um Clients die Nutzung von parallelem NFS (pNFS) zur Leistungssteigerung zu ermöglichen.
        - Wählen Sie das Kästchen **64-Bit-FSIDs und Dateikennungen aktivieren** aus, um die Unterstützung für 64-Bit-Dateisystem-IDs und Dateikennungen zu aktivieren. Dieses Kästchen gilt für NFSv4.0, NFSv4.1 und NFSv4.2. Dies ist getrennt von dem Kästchen, das zur Steuerung der 64-Bit-Unterstützung für NFSv3 verwendet wird.
    - Um NFSv4.1 zu deaktivieren, deaktivieren Sie das Kästchen **Unterstützung für Version 4.1 aktivieren**.
    - Um NFSv4.2 zu aktivieren, wählen Sie das Kästchen **Support-Version 4.1 und 4.2 aktivieren** und anschließend das Kästchen **Support-Version 4.2 aktivieren**. Beachten Sie die folgenden Optionen:
        - Aktivieren Sie das Kästchen **ACL aktivieren**, um die Verwendung einer Zugriffssteuerungsliste zu ermöglichen.
        - Aktivieren Sie das Kästchen **Lese-Delegierung aktivieren**, um den schreibgeschützten Zugriff zu ermöglichen.
        - Aktivieren Sie das Kästchen **Schreibdelegation**, um Schreibzugriff zu ermöglichen.
        - Aktivieren Sie das **pNFS** Kästchen, um Clients die Nutzung von parallelem NFS (pNFS) zur Leistungssteigerung zu ermöglichen.
        - Wählen Sie das Kästchen **64-Bit-FSIDs und Dateikennungen aktivieren** aus, um die Unterstützung für 64-Bit-Dateisystem-IDs und Dateikennungen zu aktivieren. Dieses Kästchen gilt für NFSv4.0, NFSv4.1 und NFSv4.2. Dies ist getrennt von dem Kästchen, das zur Steuerung der 64-Bit-Unterstützung für NFSv3 verwendet wird.
    - Um NFSv4.2 zu deaktivieren, deaktivieren Sie das Kästchen **Unterstützung für Version 4.2 aktivieren**.
4. Optional können Sie den **V4-ID-Domänennamen** für das NFS-Protokoll angeben.
5. **Speichern** auswählen.

**CLI**

**Schritt**

1. Führen Sie eine der folgenden Aktionen aus:

| Wenn Sie möchten… | Für Version… | Führen Sie den folgenden Befehl aus… |
| --- | --- | --- |
| NFS aktivieren | NFSv3 | `vserver nfs modify -vserver vserver_name -v3 enabled` |
| | NFSv4.0 | `vserver nfs modify -vserver vserver_name -v4.0 enabled` |
| | NFSv4.1 | `vserver nfs modify -vserver vserver_name -v4.1 enabled` |
| | NFSv4.2 | `vserver nfs modify -vserver vserver_name -v4.2 enabled` |

| Wenn Sie möchten… | Für Version… | Führen Sie den folgenden Befehl aus… |
|---|---|---|
| NFS deaktivieren | NFSv3 | `vserver nfs modify -vserver vserver_name -v3 disabled` |
| | NFSv4.0 | `vserver nfs modify -vserver vserver_name -v4.0 disabled` |
| | NFSv4.1 | `vserver nfs modify -vserver vserver_name -v4.1 disabled` |
| | NFSv4.2 | `vserver nfs modify -vserver vserver_name -v4.2 disabled` |

# ONTAP NFSv4 Storepool-Limits verwalten

Ab ONTAP 9.13 können Administratoren ihre NFSv4 Server so konfigurieren, dass sie NFSv4 Clients Ressourcen verweigern, sobald die Ressourcenlimits des jeweiligen Storepool erreicht sind. Wenn Clients zu viele NFSv4 Storepool-Ressourcen verbrauchen, kann dies dazu führen, dass andere NFSv4 Clients aufgrund fehlender NFSv4 Storepool-Ressourcen blockiert werden.

Durch Aktivierung dieser Funktion können Kunden außerdem den aktiven storepool-Ressourcenverbrauch jedes einzelnen Clients einsehen. Dies erleichtert die Identifizierung von Clients, die Systemressourcen erschöpfen, und macht es möglich, Ressourcenlimits pro Client festzulegen.

## Verbrauchte Storepool-Ressourcen anzeigen

Der `vserver nfs storepool show` Befehl zeigt die Anzahl der verbrauchten Storepool-Ressourcen an. Ein Storepool ist ein Pool von Ressourcen, der von NFSv4-Clients verwendet wird.

**Schritt**

1. Als Administrator kann der `vserver nfs storepool show` Befehl ausgeführt werden, um die Storepool-Informationen der NFSv4-Clients anzuzeigen.

**Beispiel**

Dieses Beispiel zeigt die Speicherpoolinformationen von NFSv4-Clients an.

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-Ip: 10.0.1.1

Client-Ip Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount

-------------- --------- --------- ---------- ---------- ----------
---------

10.0.2.1          nfs4.1     true    2 1 0 4

10.0.2.2          nfs4.2     true    2 1 0 4

2 entries were displayed.
```

## Aktivieren oder Deaktivieren der Storepool-Limitsteuerung

Administratoren können die folgenden Befehle verwenden, um die Speicherpool-Limitsteuerung zu aktivieren oder zu deaktivieren.

**Schritt**

1. Als Administrator kann eine der folgenden Aktionen ausgeführt werden:

| Wenn Sie möchten… | Führen Sie den folgenden Befehl aus… |
|---|---|
| Steuerungen für Speicherpool-Limits aktivieren | `vserver nfs storepool config modify -limit-enforce enabled` |
| Steuerung für Speicherpool-Limits deaktivieren | `vserver nfs storepool config modify -limit-enforce disabled` |

## Liste blockierter Clients

Wenn die Speicherpoolbegrenzung aktiviert ist, können Administratoren sehen, welche Clients blockiert wurden, sobald sie ihren Ressourcenschwellenwert pro Client erreicht haben. Administratoren können den folgenden Befehl verwenden, um zu sehen, welche Clients als blockierte Clients markiert wurden.

**Schritte**

1. Mit dem `vserver nfs storepool blocked-client show` Befehl wird die Liste der blockierten NFSv4-Clients angezeigt.

## Einen Client aus der Liste der blockierten Clients entfernen

Clients, die ihr Client-Limit erreichen, werden getrennt und dem Block-Client-Cache hinzugefügt. Administratoren können den folgenden Befehl verwenden, um den Client aus dem Block-Client-Cache zu entfernen. Dadurch kann der Client eine Verbindung zum ONTAP NFSV4 Server herstellen.

**Schritte**

1. Mit dem `vserver nfs storepool blocked-client flush -client-ip <ip address>` Befehl lässt sich der blockierte Client-Cache des Storepools leeren.
2. Mit dem `vserver nfs storepool blocked-client show` Befehl lässt sich überprüfen, ob der Client aus dem Block Client Cache entfernt wurde.

**Beispiel**

Dieses Beispiel zeigt einen blockierten Client mit der IP-Adresse "10.2.1.1", der von allen Knoten entfernt wird.

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
----------
10.1.1.1

1 entries were displayed.
```

# pNFS für ONTAP SVMs aktivieren oder deaktivieren

pNFS verbessert die Leistung, indem NFS-Clients lesen/schreiben-Operationen direkt und parallel auf Speichermedien ausführen können, wodurch der NFS-Server als potenzieller Engpass umgangen wird. Zum Aktivieren oder Deaktivieren von pNFS (parallel NFS) kann die `-v4.1-pnfs` Option angepasst werden.

| Wenn die ONTAP Version… | Der pNFS-Standardwert ist… |
|---|---|
| 9.8 oder höher | deaktiviert |
| 9.7 oder früher | aktiviert |

**Bevor Sie beginnen**

Für die Nutzung von pNFS ist die Unterstützung von NFSv4.1 erforderlich.

Wenn pNFS aktiviert werden soll, müssen zunächst die NFS-Weiterleitungen deaktiviert werden. Beides kann nicht gleichzeitig aktiviert sein.

Wenn pNFS mit Kerberos auf SVMs verwendet wird, muss Kerberos auf jedem LIF auf der SVM aktiviert sein.

**Schritt**

1. Führen Sie eine der folgenden Aktionen aus:

| Wenn Sie möchten… | Geben Sie den Befehl ein… |
|---|---|
| pNFS aktivieren | `vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled` |
| pNFS deaktivieren | `vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled` |

**Verwandte Informationen**

- NFS Trunking Übersicht

# NFS-Zugriff über TCP und UDP für ONTAP SVMs steuern

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

**Über diese Aufgabe**

Diese Parameter gelten nur für NFS. Sie haben keinen Einfluss auf Hilfsprotokolle. Wenn beispielsweise NFS über TCP deaktiviert ist, sind Mount-Vorgänge über TCP weiterhin erfolgreich. Um TCP- oder UDP-Datenverkehr vollständig zu blockieren, können Exportrichtlinienregeln verwendet werden.

Sie müssen den SnapDiff RPC Server deaktivieren, bevor Sie TCP für NFS deaktivieren, um einen Befehlsfehler zu vermeiden. TCP kann mit dem Befehl `vserver snapdiff-rpc-server off -vserver vserver name` deaktiviert werden.

**Schritt**

1. Führen Sie eine der folgenden Aktionen aus:

| Wenn NFS-Zugriff verfügbar sein soll… | Geben Sie den Befehl ein… |
|---|---|
| Aktiviert über TCP | `vserver nfs modify -vserver vserver_name -tcp enabled` |
| Deaktiviert über TCP | `vserver nfs modify -vserver vserver_name -tcp disabled` |
| Aktiviert über UDP | `vserver nfs modify -vserver vserver_name -udp enabled` |
| Deaktiviert über UDP | `vserver nfs modify -vserver vserver_name -udp disabled` |

# NFS-Anfragen von nicht reservierten Ports für ONTAP SVMs steuern

Sie können NFS-Mount-Anfragen von nicht reservierten Ports ablehnen, indem Sie die `-mount-rootonly` Option aktivieren. Um alle NFS-Anfragen von nicht reservierten Ports abzulehnen, kann die `-nfs-rootonly` Option aktiviert werden.

**Über diese Aufgabe**

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

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

Diese Optionen gelten nicht für die NULL-Prozedur.

**Schritt**

1. Führen Sie eine der folgenden Aktionen aus:

| Wenn Sie möchten… | Geben Sie den Befehl ein… |
|---|---|
| NFS Mount-Anfragen von nicht reservierten Ports zulassen | `vserver nfs modify -vserver vserver_name -mount -rootonly disabled` |
| NFS Mount-Anfragen von nicht reservierten Ports ablehnen | `vserver nfs modify -vserver vserver_name -mount -rootonly enabled` |
| Alle NFS-Anfragen von nicht reservierten Ports zulassen | `vserver nfs modify -vserver vserver_name -nfs -rootonly disabled` |
| Alle NFS-Anfragen von nicht reservierten Ports ablehnen | `vserver nfs modify -vserver vserver_name -nfs -rootonly enabled` |

# NFS-Zugriff auf ONTAP NTFS-Volumes oder Qtrees für unbekannte UNIX-Benutzer verwalten

Kann ONTAP UNIX-Benutzer, die versuchen, eine Verbindung zu Volumes oder Qtrees mit NTFS-Sicherheitsstil herzustellen, nicht identifizieren, kann ONTAP diese Benutzer nicht explizit einem Windows-Benutzer zuordnen. ONTAP kann so konfiguriert werden, dass solchen Benutzern entweder der Zugriff aus Sicherheitsgründen verweigert wird oder sie einem Standard-Windows-Benutzer zugeordnet werden, um allen Benutzern ein Mindestmaß an Zugriff zu gewährleisten.

**Bevor Sie beginnen**

Ein Standard-Windows-Benutzer muss konfiguriert sein, 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 zunächst einem Windows-Benutzer zugeordnet werden, damit ONTAP die NTFS-Berechtigungen korrekt auswerten kann. Kann ONTAP jedoch den Namen des UNIX-Benutzers in den konfigurierten Benutzerinformations-Namensdienstquellen nicht nachschlagen, kann der UNIX-Benutzer nicht explizit einem bestimmten Windows-Benutzer zugeordnet werden. Es bestehen folgende Möglichkeiten, wie mit solchen unbekannten UNIX-Benutzern umgegangen werden kann:

- Unbekannten UNIX-Benutzern wird der Zugriff verweigert.

  Dies gewährleistet eine strengere Sicherheit, indem eine explizite Zuordnung für alle UNIX-Benutzer erforderlich ist, um Zugriff auf NTFS-Volumes oder Qtrees zu erhalten.

- Unbekannte UNIX-Benutzer einem Standard-Windows-Benutzer zuordnen.

  Dies bietet zwar weniger Sicherheit, aber mehr Komfort, da sichergestellt wird, dass alle Benutzer über

einen Standard-Windows-Benutzer ein Mindestmaß an Zugriff auf NTFS Volumes oder Qtrees erhalten.

**Schritte**

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

| Wenn der Standard-Windows-Benutzer für unbekannte UNIX-Benutzer verwendet werden soll… | Geben Sie den Befehl ein… |
|---|---|
| Aktiviert | `vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled` |
| Deaktiviert | `vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled` |

3. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

# Hinweise für Clients, die ONTAP NFS-Exporte auf nicht reservierten Ports einbinden

Die `-mount-rootonly` Option muss auf einem Speichersystem deaktiviert sein, das Clients unterstützen muss, die NFS-Exporte über einen nicht reservierten Port einbinden, selbst wenn der Benutzer als root angemeldet ist. Zu diesen Clients zählen Hummingbird Clients und Solaris NFS/IPv6 Clients.

Wenn die `-mount-rootonly` Option aktiviert ist, erlaubt ONTAP NFS-Clients, die nicht reservierte Ports verwenden, das heißt Ports mit Nummern über 1.023, nicht, NFS-Exporte einzubinden.

# Strengere Zugriffskontrollen für Netgroups durch Überprüfung der Domains bei ONTAP NFS SVMs

Standardmäßig führt ONTAP bei der Überprüfung des Clientzugriffs auf eine Netgroup eine zusätzliche Verifizierung durch. Die zusätzliche Prüfung stellt sicher, dass die Domäne des Clients mit der Domänenkonfiguration der Storage Virtual Machine (SVM) übereinstimmt. Andernfalls verweigert ONTAP den Clientzugriff.

**Über diese Aufgabe**

Wenn ONTAP Exportregel für den Clientzugriff auswertet und eine Exportregel eine Netgroup enthält, muss ONTAP feststellen, ob die IP-Adresse eines Clients zu dieser Netgroup gehört. Zu diesem Zweck wandelt ONTAP die IP-Adresse des Clients mithilfe von DNS in einen Hostnamen um und ermittelt einen vollqualifizierten Domainnamen (FQDN).

Wenn in der Netgroup-Datei nur ein Kurzname für den Host aufgeführt ist und dieser Kurzname in mehreren Domänen existiert, ist es möglich, dass ein Client aus einer anderen Domäne ohne diese Überprüfung Zugriff

erhält.

Um dies zu verhindern, vergleicht ONTAP die vom DNS für den Host zurückgegebene Domain mit der Liste der für die SVM konfigurierten DNS-Domainnamen. Wenn sie übereinstimmt, wird der Zugriff erlaubt. Wenn sie nicht übereinstimmt, wird der Zugriff verweigert.

Diese Überprüfung ist standardmäßig aktiviert. Sie kann durch Ändern des `-netgroup-dns-domain -search` Parameters verwaltet werden, der auf der erweiterten Berechtigungsebene verfügbar ist.

**Schritte**

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Die gewünschte Aktion ausführen:

| Wenn die Domänenverifizierung für Netzgruppen erforderlich ist… | Eingeben… |
|---|---|
| Aktiviert | `vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled` |
| Deaktiviert | `vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled` |

3. Die Berechtigungsstufe wird auf Administrator gesetzt:

   ```
   set -privilege admin
   ```

# Ändern der für NFSv3-Services verwendeten Ports für ONTAP SVMs

Der NFS-Server des Speichersystems nutzt Dienste wie mount daemon und Network Lock Manager, um über bestimmte Standard-Netzwerkports mit NFS-Clients zu kommunizieren. In den meisten NFS-Umgebungen funktionieren die Standard-Netzwerkports korrekt und müssen nicht geändert werden, aber wenn in Ihrer NFSv3-Umgebung andere NFS-Netzwerkports verwendet werden sollen, ist dies möglich.

**Bevor Sie beginnen**

Das Ändern der NFS-Ports auf dem Speichersystem erfordert, dass alle NFS-Clients die Verbindung zum System erneut herstellen. Es empfiehlt sich, diese Information den Benutzern im Voraus mitzuteilen.

**Über diese Aufgabe**

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

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

**Schritte**

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Zugriff auf NFS deaktivieren:

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

3. Den NFS-Port für den jeweiligen NFS-Service festlegen:

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

   | NFS-Portparameter | Beschreibung | Standardport |
   |---|---|---|
   | `-mountd-port` | NFS Mount-Daemon | 635 |
   | `-nlm-port` | Network Lock Manager | 4045 |
   | `-nsm-port` | Network Status Monitor | 4046 |
   | `-rquotad-port` | NFS Quota-Daemon | 4049 |

   Neben dem Standardport ist der zulässige Portbereich 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. Mit dem `network connections listening show`Befehl lässt sich überprüfen, ob sich die Portnummer geändert hat.

   Weitere Informationen zu `network connections listening show` finden sich in der "ONTAP-Befehlsreferenz".

6. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

**Beispiel**

Die folgenden Befehle legen den NFS-Mount-Daemon-Port auf 1113 auf der SVM mit dem Namen vs1 fest:

```
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
```

# ONTAP Befehle zur Verwaltung von NFS Servern

Für die Verwaltung von NFS-Servern gibt es spezielle ONTAP Befehle.

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
|---|---|
| Einen NFS Server erstellen | `vserver nfs create` |
| NFS-Server anzeigen | `vserver nfs show` |
| Einen NFS Server modifizieren | `vserver nfs modify` |
| Einen NFS Server löschen | `vserver nfs delete` |
| Die `.snapshot`Verzeichnisauflistung unter NFSv3-Mount-Punkten ausblenden<br><br>Der explizite Zugriff auf das `.snapshot` Verzeichnis ist weiterhin möglich, selbst wenn die Option aktiviert ist. | `vserver nfs`Befehle mit der `-v3-hide-snapshot`Option aktiviert |

Weitere Informationen zu `vserver nfs` finden sich in der "ONTAP-Befehlsreferenz".

# Behebung von Namensdienstproblemen für ONTAP NAS SVMs

Wenn Clients aufgrund von Problemen mit dem Namensdienst Zugriffsfehler haben, kann die `vserver services name-service getxxbyyy`Befehlsfamilie verwendet werden, um manuell verschiedene Namensdienstabfragen durchzuführen und die Details und

Ergebnisse der Abfrage zu untersuchen, was die Fehlerbehebung unterstützt.

**Über diese Aufgabe**

- Für jeden Befehl kann Folgendes angegeben werden:
  - Name des Knotens oder der Storage Virtual Machine (SVM), auf der die Suche durchgeführt wird.

    Dies ermöglicht es Ihnen, Namensdienstabfragen für einen bestimmten Knoten oder eine SVM zu testen, um die Suche nach einem potenziellen Problem mit der Namensdienstkonfiguration einzugrenzen.

  - Ob die für die Suche verwendete Quelle angezeigt wird.

    Dies ermöglicht Ihnen zu überprüfen, ob die richtige Quelle verwendet wurde.
- ONTAP wählt den Dienst für die Namensauflösung basierend auf der konfigurierten Reihenfolge der Namensdienstumschaltung aus.
- Diese Befehle sind auf der Zugangsstufe „Erweitert“ verfügbar.

**Schritte**

1. Führen Sie eine der folgenden Aktionen aus:

| Um die… | Verwenden Sie den Befehl… |
|---|---|
| IP-Adresse eines Hostnamens | `vserver services name-service getxxbyyy getaddrinfo` `vserver services name-service getxxbyyy gethostbyname` (nur IPv4-Adressen) |
| Mitglieder einer Gruppe nach Gruppen-ID | `vserver services name-service getxxbyyy getgrbygid` |
| Mitglieder einer Gruppe nach Gruppennamen | `vserver services name-service getxxbyyy getgrbyname` |
| Liste der Gruppen, denen ein Benutzer angehört | `vserver services name-service getxxbyyy getgrlist` |
| Hostname einer IP-Adresse | `vserver services name-service getxxbyyy getnameinfo` `vserver services name-service getxxbyyy gethostbyaddr` (nur IPv4-Adressen) |
| Benutzerinformationen nach Benutzername | `vserver services name-service getxxbyyy getpwbyname`Die Namensauflösung von RBAC-Benutzern kann getestet werden, indem der `-use-rbac` Parameter als `true` angegeben wird. |
| Benutzerinformationen nach Benutzer-ID | `vserver services name-service getxxbyyy getpwbyuid`Die Namensauflösung von RBAC-Benutzern kann getestet werden, indem der `-use-rbac` Parameter als `true` angegeben wird. |

| | |
|---|---|
| Netgroup-Mitgliedschaft eines Clients | `vserver services name-service getxxbyyy netgrp` |
| Netzgruppenzugehörigkeit eines Clients mittels Netgroup-by-Host-Suche | `vserver services name-service getxxbyyy netgrpbyhost` |

Das folgende Beispiel zeigt einen DNS-Lookup-Test für die SVM vs1, bei dem versucht wird, die IP-Adresse für den Host acast1.eng.example.com zu ermitteln:

```
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-Lookup-Test für die SVM vs1, bei dem versucht wird, 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-Lookup-Test für die SVM vs1, bei dem 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, bei dem überprüft wird, ob der Client

dnshost0 Mitglied der Netgroup lnetgroup136 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. Die Ergebnisse des durchgeführten Tests werden analysiert und die notwendigen Maßnahmen ergriffen.

| Wenn die… | Die … überprüfen. |
|---|---|
| Die Suche nach Hostnamen oder IP-Adressen schlug fehl oder ergab falsche Ergebnisse. | DNS-Konfiguration |
| Die Suche hat eine falsche Quelle abgefragt. | Name-Service-Switch-Konfiguration |
| Die Suche nach Benutzern oder Gruppen ist fehlgeschlagen oder hat falsche Ergebnisse geliefert | • Name-Service-Switch-Konfiguration<br>• Quellkonfiguration (lokale Dateien, NIS-Domäne, LDAP-Client)<br>• Netzwerkkonfiguration (zum Beispiel LIFs und Routen) |
| Die Hostnamenauflösung ist fehlgeschlagen oder es ist zu einem Timeout gekommen, und der DNS-Server löst DNS-Kurznamen (zum Beispiel host1) nicht auf | DNS-Konfiguration für Top-Level-Domain (TLD)-Abfragen. TLD-Abfragen können mit der `-is-tld-query-enabled false` Option zum `vserver services name-service dns modify` Befehl deaktiviert werden. |

**Verwandte Informationen**

"NetApp Technischer Bericht 4668: Name Services Best Practices-Leitfaden"

# Namensdienstverbindungen für ONTAP NAS SVMs überprüfen

Sie können die DNS- und LDAP-Name-Server überprüfen, um zu verifizieren, dass sie mit ONTAP verbunden sind. Diese Befehle sind auf Administratorebene verfügbar.

**Über diese Aufgabe**

Es besteht die Möglichkeit, bei Bedarf mithilfe des Namensdienstkonfigurationsprüfers zu überprüfen, ob eine gültige DNS- oder LDAP-Name-Service-Konfiguration vorliegt. Diese Validierungsprüfung kann an der Befehlszeile oder im System Manager initiiert werden.

Bei DNS-Konfigurationen werden alle Server getestet und müssen funktionieren, damit die Konfiguration als gültig gilt. Bei LDAP-Konfigurationen ist die Konfiguration gültig, solange mindestens ein Server erreichbar ist. Die Namensdienst-Befehle wenden die Konfigurationsprüfung an, es sei denn, das `skip-config-validation` Feld ist true (Standard ist false).

**Schritt**

1. Der entsprechende Befehl ermöglicht die Überprüfung der Konfiguration eines Name-Service. Die Benutzeroberfläche zeigt den Status der konfigurierten Server.

| Zur Überprüfung… | Verwenden Sie diesen Befehl… |
| --- | --- |
| DNS-Konfigurationsstatus | `vserver services name-service dns check` |
| LDAP-Konfigurationsstatus | `vserver services name-service ldap check` |

```
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 den Dienst bereitstellt. Eine Warnung wird angezeigt, wenn einige der Server nicht erreichbar sind.

# ONTAP Befehle zur Verwaltung von NAS Name Service Switch-Einträgen

Namensdienst-Switch-Einträge lassen sich durch Erstellen, Anzeigen, Ändern und Löschen verwalten.

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
| --- | --- |
| Einen Name Service Switch-Eintrag erstellen | `vserver services name-service ns-switch create` |
| Namensdienst-Switch-Einträge anzeigen | `vserver services name-service ns-switch show` |
| Ändern eines Name Service Switch-Eintrags | `vserver services name-service ns-switch modify` |
| Löschen eines Name Service Switch-Eintrags | `vserver services name-service ns-switch delete` |

Weitere Informationen zu `vserver services name-service ns-switch` finden sich in der "ONTAP-Befehlsreferenz".

**Verwandte Informationen**

"NetApp Technischer Bericht 4668: Name Services Best Practices-Leitfaden"

# ONTAP Befehle zur Verwaltung des NAS Name Service Cache

Sie können den Namensdienstcache verwalten, indem Sie den Wert für die Gültigkeitsdauer (TTL) ändern. Der TTL-Wert bestimmt, wie lange Namensdienstinformationen im Cache gespeichert bleiben.

| Wenn Sie den TTL-Wert für … ändern möchten | Verwenden Sie diesen Befehl… |
|---|---|
| Unix-Benutzer | `vserver services name-service cache unix-user settings` |
| Unix-Gruppen | `vserver services name-service cache unix-group settings` |
| Unix Netgroups | `vserver services name-service cache netgroups settings` |
| Hosts | `vserver services name-service cache hosts settings` |
| Gruppenmitgliedschaft | `vserver services name-service cache group-membership settings` |

**Verwandte Informationen**

"ONTAP-Befehlsreferenz"

# ONTAP Befehle zur Verwaltung von NFS-Namenszuordnungen

Für die Verwaltung von Namenszuordnungen gibt es spezielle ONTAP Befehle.

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
|---|---|
| Eine Namenszuordnung erstellen | `vserver name-mapping create` |
| Eine Namenszuordnung an einer bestimmten Position einfügen | `vserver name-mapping insert` |
| Anzeigenamenzuordnungen anzeigen | `vserver name-mapping show` |

| | |
|---|---|
| Die Position zweier Namenszuordnungen wird getauscht. HINWEIS: Ein Tausch ist nicht zulässig, wenn die Namenszuordnung mit einem ip-qualifier-Eintrag konfiguriert ist. | `vserver name-mapping swap` |
| Eine Namenszuordnung ändern | `vserver name-mapping modify` |
| Eine Namenszuordnung löschen | `vserver name-mapping delete` |
| Die korrekte Namenszuordnung validieren | `vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1` |

Weitere Informationen zu `vserver name-mapping` finden sich in der "ONTAP-Befehlsreferenz".

# ONTAP Befehle zur Verwaltung lokaler UNIX-Benutzer für NAS

Für die Verwaltung lokaler UNIX-Benutzer gibt es spezielle ONTAP-Befehle.

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
|---|---|
| Einen lokalen UNIX-Benutzer erstellen | `vserver services name-service unix-user create` |
| Lokale UNIX-Benutzer von einer URI laden | `vserver services name-service unix-user load-from-uri` |
| Lokale UNIX-Benutzer anzeigen | `vserver services name-service unix-user show` |
| Einen lokalen UNIX-Benutzer ändern | `vserver services name-service unix-user modify` |
| Einen lokalen UNIX-Benutzer löschen | `vserver services name-service unix-user delete` |

Weitere Informationen zu `vserver services name-service unix-user` finden sich in der "ONTAP-Befehlsreferenz".

# ONTAP Befehle zur Verwaltung von NAS lokalen UNIX-Gruppen

Für die Verwaltung lokaler UNIX-Gruppen gibt es spezielle ONTAP-Befehle.

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
|---|---|
| Eine lokale UNIX-Gruppe erstellen | `vserver services name-service unix-group create` |
| Einen Benutzer zu einer lokalen UNIX Gruppe hinzufügen | `vserver services name-service unix-group adduser` |
| Lokale UNIX-Gruppen von einer URI laden | `vserver services name-service unix-group load-from-uri` |

| | |
|---|---|
| Lokale UNIX-Gruppen anzeigen | `vserver services name-service unix-group show` |
| Eine lokale UNIX-Gruppe ändern | `vserver services name-service unix-group modify` |
| Einen Benutzer aus einer lokalen UNIX Gruppe löschen | `vserver services name-service unix-group deluser` |
| Eine lokale UNIX-Gruppe löschen | `vserver services name-service unix-group delete` |

Weitere Informationen zu `vserver services name-service unix-group` finden sich in der "ONTAP-Befehlsreferenz".

# Grenzwerte für lokale UNIX-Benutzer, Gruppen und Gruppenmitglieder für ONTAP NFS SVMs

ONTAP führte Beschränkungen für die maximale Anzahl von UNIX-Benutzern und UNIX-Gruppen im Cluster sowie Befehle zur Verwaltung dieser Beschränkungen ein. Diese Beschränkungen können dazu beitragen, Leistungsprobleme zu vermeiden, indem sie verhindern, dass Administratoren zu viele lokale UNIX-Benutzer und UNIX-Gruppen im Cluster erstellen.

Die Gesamtzahl lokaler UNIX-Benutzergruppen und ihrer Mitglieder ist begrenzt. Für lokale UNIX-Benutzer gilt eine separate Begrenzung. Die Begrenzungen gelten clusterweit. Jede dieser neuen Begrenzungen ist auf einen Standardwert festgelegt, der bis zu einem vordefinierten endgültigen Limit angepasst werden kann.

| Datenbank | Standardlimit | endgültiges Limit |
|---|---|---|
| Lokale UNIX-Benutzer | 32.768 | 65.536 |
| Lokale UNIX-Gruppen und Gruppenmitglieder | 32.768 | 65.536 |

# Grenzwerte für lokale UNIX-Benutzer und -Gruppen für ONTAP NFS SVMs verwalten

Für die Verwaltung von Limits für lokale UNIX-Benutzer und -Gruppen stehen spezielle ONTAP Befehle zur Verfügung. Cluster-Administratoren können diese Befehle nutzen, um Leistungsprobleme im Cluster zu untersuchen, die vermutlich mit einer zu hohen Anzahl lokaler UNIX-Benutzer und -Gruppen zusammenhängen.

### Über diese Aufgabe

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

### Schritt

1. Führen Sie eine der folgenden Aktionen aus:

| Wenn Sie möchten… | Verwenden Sie den Befehl… |
|---|---|
| Informationen zu lokalen UNIX-Benutzerlimits anzeigen | `vserver services unix-user max-limit show` |

| Wenn Sie möchten… | Verwenden Sie den Befehl… |
|---|---|
| Informationen zu lokalen UNIX-Gruppenbeschränkungen | `vserver services unix-group max-limit show` |
| Lokale UNIX-Benutzerlimits anpassen | `vserver services unix-user max-limit modify` |
| Lokale UNIX-Gruppenlimits ändern | `vserver services unix-group max-limit modify` |

Weitere Informationen zu `vserver services unix` finden sich in der "ONTAP-Befehlsreferenz".

# ONTAP Befehle zur Verwaltung lokaler NFS-Netgroups

Lokale Netzwerkgruppen lassen sich verwalten, indem sie von einem URI geladen, ihr Status auf den Knoten überprüft, angezeigt und gelöscht werden.

| Wenn Sie möchten… | Verwenden Sie den Befehl… |
|---|---|
| Netzgruppen aus einer URI laden | `vserver services name-service netgroup load` |
| Status der Netgroups auf allen Knoten überprüfen | `vserver services name-service netgroup status`<br>Verfügbar ab der Stufe „Erweitert“ und höher. |
| Lokale Netzgruppen anzeigen | `vserver services name-service netgroup file show` |
| Eine lokale Netzgruppe löschen | `vserver services name-service netgroup file delete` |

Weitere Informationen zu `vserver services name-service netgroup file` finden sich in der "ONTAP-Befehlsreferenz".

# ONTAP Befehle zur Verwaltung von NFS NIS-Domänenkonfigurationen

Es gibt spezifische ONTAP Befehle für die Verwaltung von NIS-Domänenkonfigurationen.

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
|---|---|
| Erstellen einer NIS-Domänenkonfiguration | `vserver services name-service nis-domain create` |
| NIS-Domänenkonfigurationen anzeigen | `vserver services name-service nis-domain show` |
| Anzeige des Bindungsstatus einer NIS-Domänenkonfiguration | `vserver services name-service nis-domain show-bound` |
| NIS Statistiken anzeigen | `vserver services name-service nis-domain show-statistics` Verfügbar ab der Berechtigungsstufe „Erweitert“ und höher. |

| | |
|---|---|
| NIS-Statistiken löschen | `vserver services name-service nis-domain clear-statistics` Verfügbar ab der Berechtigungsstufe „Erweitert“ und höher. |
| Ändern einer NIS Domänenkonfiguration | `vserver services name-service nis-domain modify` |
| Löschen einer NIS Domainkonfiguration | `vserver services name-service nis-domain delete` |
| Caching für netgroup-by-host-Suchen aktivieren | `vserver services name-service nis-domain netgroup-database config modify` Verfügbar ab der Berechtigungsstufe „Erweitert“ und höher. |

Weitere Informationen zu `vserver services name-service nis-domain` finden sich in der "ONTAP-Befehlsreferenz".

# ONTAP Befehle zur Verwaltung von NFS-LDAP-Client-Konfigurationen

Für die Verwaltung von LDAP-Client-Konfigurationen gibt es spezielle ONTAP-Befehle.

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

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
|---|---|
| Erstellen einer LDAP-Client-Konfiguration | `vserver services name-service ldap client create` |
| LDAP-Client-Konfigurationen anzeigen | `vserver services name-service ldap client show` |
| Ändern einer LDAP-Client-Konfiguration | `vserver services name-service ldap client modify` |
| Das BIND-Passwort des LDAP-Clients ändern | `vserver services name-service ldap client modify-bind-password` |
| Löschen einer LDAP-Client-Konfiguration | `vserver services name-service ldap client delete` |

Weitere Informationen zu `vserver services name-service ldap client` finden sich in der "ONTAP-Befehlsreferenz".

# ONTAP Befehle zur Verwaltung von NFS LDAP-Konfigurationen

Für die Verwaltung von LDAP-Konfigurationen gibt es spezielle ONTAP-Befehle.

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
|---|---|
| Erstellen einer LDAP-Konfiguration | `vserver services name-service ldap create` |

| | |
|---|---|
| LDAP-Konfigurationen anzeigen | `vserver services name-service ldap show` |
| Ändern einer LDAP-Konfiguration | `vserver services name-service ldap modify` |
| Eine LDAP-Konfiguration löschen | `vserver services name-service ldap delete` |

Weitere Informationen zu `vserver services name-service ldap` finden sich in der "ONTAP-Befehlsreferenz".

# ONTAP Befehle zur Verwaltung von NFS LDAP-Client-Schemavorlagen

Für die Verwaltung von LDAP-Client-Schemavorlagen gibt es spezielle ONTAP-Befehle.

SVM-Administratoren können von Cluster-Administratoren erstellte LDAP-Client-Schemas weder ändern noch löschen.

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
|---|---|
| Eine vorhandene LDAP-Schemavorlage kopieren | `vserver services name-service ldap client schema copy` Verfügbar ab der Berechtigungsstufe „Erweitert“ und höher. |
| LDAP-Schemavorlagen anzeigen | `vserver services name-service ldap client schema show` |
| Eine LDAP-Schema-Vorlage ändern | `vserver services name-service ldap client schema modify` Verfügbar ab der Berechtigungsstufe „Erweitert“ und höher. |
| Löschen einer LDAP-Schema-Vorlage | `vserver services name-service ldap client schema delete` Verfügbar ab der Berechtigungsstufe „Erweitert“ und höher. |

Weitere Informationen zu `vserver services name-service ldap client schema` finden sich in der "ONTAP-Befehlsreferenz".

# ONTAP Befehle zur Verwaltung von NFS Kerberos-Schnittstellenkonfigurationen

Für die Verwaltung von NFS-Kerberos-Schnittstellenkonfigurationen gibt es spezielle ONTAP-Befehle.

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
|---|---|
| NFS Kerberos auf einer LIF aktivieren | `vserver nfs kerberos interface enable` |
| NFS Kerberos-Schnittstellenkonfigurationen | `vserver nfs kerberos interface show` |
| Ändern einer NFS Kerberos-Schnittstellenkonfiguration | `vserver nfs kerberos interface modify` |
| NFS Kerberos auf einer LIF deaktivieren | `vserver nfs kerberos interface disable` |

Weitere Informationen zu `vserver nfs kerberos interface` finden sich in der "ONTAP-Befehlsreferenz".

# ONTAP Befehle zur Verwaltung von NFS Kerberos Realm-Konfigurationen

Für die Verwaltung von NFS-Kerberos-Realm-Konfigurationen gibt es spezielle ONTAP Befehle.

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
|---|---|
| Erstellen einer NFS Kerberos Realm-Konfiguration | `vserver nfs kerberos realm create` |
| NFS Kerberos Realm-Konfigurationen anzeigen | `vserver nfs kerberos realm show` |
| Ändern einer NFS Kerberos Realm-Konfiguration | `vserver nfs kerberos realm modify` |
| Löschen einer NFS Kerberos Realm-Konfiguration | `vserver nfs kerberos realm delete` |

Weitere Informationen zu `vserver nfs kerberos realm` finden sich in der "ONTAP-Befehlsreferenz".

# ONTAP Befehle zur Verwaltung von Exportrichtlinien

Für die Verwaltung von Exportrichtlinien gibt es spezielle ONTAP Befehle.

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
|---|---|
| Informationen zu Exportrichtlinien anzeigen | `vserver export-policy show` |
| Umbenennen einer Exportregel | `vserver export-policy rename` |
| Exportregel kopieren | `vserver export-policy copy` |
| Exportregel löschen | `vserver export-policy delete` |

Weitere Informationen zu `vserver export-policy` finden sich in der "ONTAP-Befehlsreferenz".

# ONTAP Befehle zur Verwaltung von Exportregeln

Für die Verwaltung von Exportregeln gibt es spezielle ONTAP-Befehle.

| Wenn Sie möchten… | Verwenden Sie diesen Befehl… |
|---|---|
| Exportregel erstellen | `vserver export-policy rule create` |
| Informationen zu Exportregeln | `vserver export-policy rule show` |
| Eine Exportregel ändern | `vserver export-policy rule modify` |

| | |
|---|---|
| Eine Exportregel löschen | `vserver export-policy rule delete` |

Wenn Sie mehrere identische Exportregeln für verschiedene Clients konfiguriert haben, sollten diese bei der Verwaltung von Exportregeln synchron gehalten werden.

Weitere Informationen zu `vserver export-policy` finden sich in der "ONTAP-Befehlsreferenz".

# Den NFS-Anmeldeinformationscache konfigurieren

## Gründe für die Änderung der Gültigkeitsdauer des NFS-Anmeldeinformationscache für ONTAP SVMs

ONTAP verwendet einen Berechtigungs-Cache, um die für die Benutzerauthentifizierung beim Zugriff auf NFS-Exporte benötigten Informationen zu speichern, um einen schnelleren Zugriff und eine bessere Performance zu ermöglichen. Die Dauer der Speicherung der Informationen im Berechtigungs-Cache kann konfiguriert werden, um sie an die jeweilige Umgebung anzupassen.

Es gibt verschiedene Szenarien, in denen die Änderung der Time-to-Live (TTL) des NFS-Credential-Cache zur Problemlösung beitragen kann. Es ist wichtig, diese Szenarien sowie die Konsequenzen solcher Änderungen zu kennen.

### Gründe

Eine Änderung der Standard-TTL ist unter folgenden Umständen in Betracht zu ziehen:

| Problem | Abhilfemaßnahme |
|---|---|
| Die Nameserver in Ihrer Umgebung verzeichnen eine Leistungseinbuße aufgrund einer hohen Anzahl von Anfragen von ONTAP. | Die Gültigkeitsdauer (TTL) für zwischengespeicherte positive und negative Anmeldeinformationen kann erhöht werden, wodurch die Anzahl der Anfragen von ONTAP an die Nameserver verringert wird. |
| Der Name-Server-Administrator nahm Änderungen vor, um NFS-Benutzern, denen zuvor der Zugriff verweigert wurde, den Zugriff zu ermöglichen. | Die TTL für zwischengespeicherte negative Anmeldeinformationen kann verringert werden, um die Zeit zu verkürzen, die NFS-Benutzer warten müssen, bis ONTAP neue Anmeldeinformationen von externen Nameservern anfordert, damit sie Zugriff erhalten. |
| Der Name-Server-Administrator hat Änderungen vorgenommen, um NFS-Benutzern, denen zuvor der Zugriff erlaubt war, den Zugriff zu verweigern. | Die Gültigkeitsdauer (TTL) für zwischengespeicherte positive Anmeldeinformationen wird reduziert, wodurch sich die Zeit verkürzt, bevor ONTAP neue Anmeldeinformationen von externen Nameservern anfordert, sodass NFS-Benutzern nun der Zugriff verweigert wird. |

### Konsequenzen

Sie können die Speicherdauer für positive und negative Anmeldeinformationen individuell anpassen. Allerdings sollten sowohl die Vorteile als auch die Nachteile dieser Vorgehensweise berücksichtigt werden.

| Wenn Sie… | Der Vorteil ist… | Der Nachteil ist… |
|---|---|---|
| Die Zeit für den positiven Anmeldeinformationscache erhöhen | ONTAP sendet Anfragen nach Anmeldeinformationen seltener an die Name-Server, was die Last auf die Name-Server verringert. | Es dauert länger, NFS-Benutzern den Zugriff zu verweigern, denen dieser zuvor erlaubt war, jetzt aber nicht mehr. |
| Die Zeit für den positiven Anmeldeinformationscache verringern | Es dauert weniger lang, NFS-Benutzern den Zugriff zu verweigern, denen dieser zuvor erlaubt war, jetzt aber nicht mehr. | ONTAP sendet Anfragen nach Anmeldeinformationen häufiger an die Name-Server, was die Last auf die Name-Server erhöht. |
| Die Cache-Zeit für negative Anmeldeinformationen erhöhen | ONTAP sendet Anfragen nach Anmeldeinformationen seltener an die Name-Server, was die Last auf die Name-Server verringert. | Es dauert länger, NFS-Benutzern Zugriff zu gewähren, die zuvor keinen Zugriff hatten, nun aber Zugriff erhalten. |
| Die Zeit für den negativen Anmeldeinformationscache verringern | Es nimmt weniger Zeit in Anspruch, NFS-Benutzern Zugriff zu gewähren, denen zuvor kein Zugriff erlaubt war, die nun aber Zugriff erhalten. | ONTAP sendet Anfragen nach Anmeldeinformationen häufiger an die Name-Server, was die Last auf die Name-Server erhöht. |

## Die Gültigkeitsdauer für zwischengespeicherte NFS-Benutzeranmeldeinformationen für ONTAP SVMs konfigurieren

Sie können die Speicherdauer, für die ONTAP Anmeldeinformationen für NFS-Benutzer im internen Cache (Time-to-Live oder TTL) speichert, konfigurieren, indem der NFS-Server der Storage Virtual Machine (SVM) angepasst wird. Dies ermöglicht die Behebung bestimmter Probleme im Zusammenhang mit hoher Auslastung der Nameserver oder Änderungen der Anmeldeinformationen, die den NFS-Benutzerzugriff beeinflussen.

### Über diese Aufgabe

Diese Parameter sind auf der Stufe „Erweitertes Berechtigungsniveau“ verfügbar.

### Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Die gewünschte Aktion ausführen:

| Wenn Sie die TTL für zwischengespeicherte Daten ändern möchten… | Verwenden Sie den Befehl… |
|---|---|

| | |
|---|---|
| Positive Anmeldedaten | `vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live`<br><br>Die TTL wird in Millisekunden gemessen. Ab ONTAP 9.17.1 und höher beträgt der Standardwert 1 Stunde (3,600,000 Millisekunden). In ONTAP 9.16.1 und früher beträgt der Standardwert 24 Stunden (86,400,000 Millisekunden). Der zulässige Bereich für diesen Wert liegt zwischen 1 Minute (60,000 Millisekunden) und 7 Tagen (604,800,000 Millisekunden). |
| Negative Anmeldeinformationen | `vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live`<br><br>Die TTL wird in Millisekunden gemessen. Der Standardwert beträgt 2 Stunden (7.200.000 Millisekunden). Der zulässige Bereich für diesen Wert reicht von 1 Minute (60.000 Millisekunden) bis 7 Tagen (604.800.000 Millisekunden). |

3. Zurück zur Administrator-Privilegstufe:

   `set -privilege admin`

# Exportrichtlinien-Caches verwalten

## Export-Policy-Caches für ONTAP NAS SVMs leeren

ONTAP verwendet mehrere Exportregel-Caches, um Informationen zu Exportregeln für einen schnelleren Zugriff zu speichern. Das manuelle Leeren der Exportregel-Caches (`vserver export-policy cache flush` entfernt möglicherweise veraltete Informationen und zwingt ONTAP, aktuelle Informationen aus den entsprechenden externen Ressourcen abzurufen. Dies kann bei der Lösung verschiedener Probleme im Zusammenhang mit dem Zugriff von Clients auf NFS-Exporte helfen.

### Über diese Aufgabe

Die Informationen im Exportregel-Cache könnten aus folgenden Gründen veraltet sein:

- Eine kürzlich erfolgte Änderung der Exportregel
- Eine kürzlich erfolgte Änderung an den Hostname-Einträgen in den Nameservern
- Eine kürzlich erfolgte Änderung an den Netgroup-Einträgen in den Name Servern
- Wiederherstellung nach einem Netzwerkausfall, der das vollständige Laden von Netgroups verhinderte

### Schritte

1. Falls der Namensdienstcache nicht aktiviert ist, kann eine der folgenden Aktionen im erweiterten Berechtigungsmodus durchgeführt werden:

| Wenn ein Flush durchgeführt werden soll… | Geben Sie den Befehl ein… |
|---|---|
| Alle Export-Policy-Caches (außer showmount) | `vserver export-policy cache flush -vserver vserver_name` |

| Wenn ein Flush durchgeführt werden soll… | Geben Sie den Befehl ein… |
|---|---|
| Der Exportregel-Zugriffs-Cache | `vserver export-policy cache flush -vserver vserver_name -cache access` Sie können den optionalen `-node` Parameter angeben, um den Knoten zu bestimmen, auf dem der Zugriffscache geleert werden soll. |
| Der Hostname-Cache | `vserver export-policy cache flush -vserver vserver_name -cache host` |
| Der Netgroup-Cache | `vserver export-policy cache flush -vserver vserver_name -cache netgroup`Die Verarbeitung von Netzgruppen ist ressourcenintensiv. Der Netzgruppen-Cache sollte nur geleert werden, wenn ein Clientzugriffsproblem durch eine veraltete Netzgruppe verursacht wird. |
| Der Showmount Cache | `vserver export-policy cache flush -vserver vserver_name -cache showmount` |

2. Wenn der Namensdienstcache aktiviert ist, kann eine der folgenden Aktionen durchgeführt werden:

| Wenn ein Flush durchgeführt werden soll… | Geben Sie den Befehl ein… |
|---|---|
| Der Exportregel-Zugriffs-Cache | `vserver export-policy cache flush -vserver vserver_name -cache access` Sie können den optionalen `-node` Parameter angeben, um den Knoten zu bestimmen, auf dem der Zugriffscache geleert werden soll. |
| Der Hostname-Cache | `vserver services name-service cache hosts forward-lookup delete-all` |
| Der Netgroup-Cache | `vserver services name-service cache netgroups ip-to-netgroup delete-all` `vserver services name-service cache netgroups members delete-all`Die Verarbeitung von Netzgruppen ist ressourcenintensiv. Der Netzgruppen-Cache sollte nur geleert werden, wenn ein Clientzugriffsproblem durch eine veraltete Netzgruppe verursacht wird. |
| Der Showmount Cache | `vserver export-policy cache flush -vserver vserver_name -cache showmount` |

## Anzeige der Export-Policy-Netgroup-Warteschlange und des Caches für ONTAP NFS SVMs

ONTAP verwendet die netgroup-Warteschlange beim Importieren und Auflösen von netgroups und nutzt den netgroup-Cache, um die resultierenden Informationen zu speichern. Bei der Fehlerbehebung von Problemen im Zusammenhang mit Exportrichtlinien-netgroup können die `vserver export-policy netgroup queue show` und `vserver export-policy netgroup cache show` Befehle verwendet werden, um den Status der netgroup-Warteschlange und den Inhalt des netgroup-Caches

anzuzeigen.

**Schritt**

1. Führen Sie eine der folgenden Aktionen aus:

| Die Exportrichtlinien-Netzgruppe wird angezeigt… | Geben Sie den Befehl ein… |
|---|---|
| Warteschlange | `vserver export-policy netgroup queue show` |
| Cache | `vserver export-policy netgroup cache show -vserver vserver_name` |

Weitere Informationen zu `vserver export-policy netgroup` finden sich in der "ONTAP-Befehlsreferenz".

## Es kann überprüft werden, ob eine Client-IP-Adresse Mitglied einer ONTAP NFS-Netgroup ist.

Bei der Fehlersuche bei NFS-Client-Zugriffsproblemen im Zusammenhang mit Netzgruppen kann der `vserver export-policy netgroup check-membership` Befehl dabei helfen festzustellen, ob eine Client-IP Mitglied einer bestimmten Netzgruppe ist.

**Über diese Aufgabe**

Die Überprüfung der Netzgruppenmitgliedschaft ermöglicht die Feststellung, ob ONTAP erkennt, dass ein Client Mitglied einer Netzgruppe ist oder nicht. Es wird außerdem ersichtlich, ob sich der ONTAP Netzgruppencache während der Aktualisierung der Netzgruppeninformationen in einem temporären Zustand befindet. Diese Informationen können das Verständnis dafür erleichtern, warum einem Client unerwartet Zugriff gewährt oder verweigert wird.

**Schritt**

1. Die Netgroup-Zugehörigkeit einer Client-IP-Adresse prüfen: `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

   Der Befehl kann folgende Ergebnisse liefern:

   - Der Client ist Mitglied der netgroup.

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

   - Der Client ist Mitglied der netgroup.

     Es wurde im ONTAP Netgroup-Cache gefunden.

   - Der Client ist kein Mitglied der Netgroup.
   - Die Zugehörigkeit des Clients kann noch nicht ermittelt werden, da ONTAP derzeit den Netgroup-Cache aktualisiert.

Solange dies nicht geschehen ist, kann die Mitgliedschaft nicht explizit bestätigt oder ausgeschlossen werden. Mit dem `vserver export-policy netgroup queue show` Befehl lässt sich das Laden der Netzgruppe überwachen, anschließend kann die Überprüfung erneut durchgeführt werden.

**Beispiel**

Das folgende Beispiel prüft, ob ein Client mit der IP-Adresse 172.17.16.72 Mitglied der Netgroup mercury auf der SVM vs1 ist:

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

## Optimierung der Zugriffscache-Performance für ONTAP NFS SVMs

Sie können verschiedene Parameter konfigurieren, um den Zugriffscache zu optimieren und das richtige Gleichgewicht zwischen Leistung und Aktualität der im Zugriffscache gespeicherten Informationen zu finden.

**Über diese Aufgabe**

Bei der Konfiguration der Aktualisierungsintervalle für den Zugriffscache ist Folgendes zu beachten:

- Höhere Werte bedeuten, dass Einträge länger im Zugriffscache verbleiben.

  Der Vorteil liegt in der besseren Performance, da ONTAP weniger Ressourcen für die Aktualisierung der Zugriffscache-Einträge aufwendet. Der Nachteil besteht darin, dass es länger dauert, veraltete Zugriffscache-Einträge zu aktualisieren, wenn sich Exportrichtlinienregeln ändern. Dadurch kann es vorkommen, dass Clients, die Zugriff erhalten sollten, abgelehnt werden und Clients, die abgelehnt werden sollten, Zugriff erhalten.

- Niedrigere Werte bedeuten, dass ONTAP die Zugriffscache-Einträge häufiger aktualisiert.

  Der Vorteil besteht darin, dass die Einträge aktueller sind und Clients mit höherer Wahrscheinlichkeit korrekt Zugriff gewährt oder verweigert wird. Der Nachteil ist eine geringere Leistung, da ONTAP mehr Ressourcen für die Aktualisierung der Zugriffscache-Einträge aufwendet.

**Schritte**

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Die gewünschte Aktion ausführen:

| Um die… | Eingeben… |
|---|---|
| Aktualisierungszeitraum für positive Einträge | `vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value` |
| Aktualisierungszeitraum für negative Einträge | `vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value` |

| Um die… | Eingeben… |
| --- | --- |
| Timeout-Zeitraum für alte Einträge | `vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value` |

3. Die neuen Parametereinstellungen werden überprüft:

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

4. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

# Dateisperren verwalten

## Informationen zur Dateisperrung zwischen Protokollen für ONTAP NFS SVMs

Die Dateisperrung ist eine Methode, mit der Clientanwendungen 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.

Handelt es sich beim Client um einen NFS-Client, sind Sperren empfehlend; handelt es sich beim Client um einen SMB-Client, sind Sperren obligatorisch.

Aufgrund von Unterschieden zwischen den Dateisperren von NFS und SMB kann es vorkommen, dass ein NFS-Client nicht auf eine Datei zugreifen kann, die zuvor von einer SMB-Anwendung geöffnet wurde.

Folgendes geschieht, wenn ein NFS-Client versucht, auf eine von einer SMB-Anwendung gesperrte Datei zuzugreifen:

- In gemischten oder NTFS-Volumes können Dateimanipulationsvorgänge wie `rm`, `rmdir` und `mv` dazu führen, dass die NFS-Anwendung fehlschlägt.
- NFS-Lese- und Schreibvorgänge werden durch die SMB-Öffnungsmodi deny-read und deny-write jeweils für lesen bzw. schreiben verweigert.
- NFS-Schreibvorgänge schlagen fehl, wenn der geschriebene Bereich der Datei mit einer exklusiven SMB-Bytesperre gesperrt ist.

In UNIX-Sicherheitsstil-Volumes ignorieren NFS-Unlink- und Rename-Operationen den SMB-Sperrstatus und ermöglichen den Zugriff auf die Datei. Alle anderen NFS-Operationen auf UNIX-Sicherheitsstil-Volumes berücksichtigen den SMB-Sperrstatus.

## Informationen zu schreibgeschützten Bits für ONTAP NFS SVMs

Das Schreibschutzbit wird für jede Datei einzeln gesetzt, um anzuzeigen, ob eine Datei beschreibbar (deaktiviert) oder schreibgeschützt (aktiviert) ist.

SMB-Clients unter Windows können ein schreibgeschütztes Bit pro Datei setzen. NFS-Clients setzen kein schreibgeschütztes Bit pro Datei, da NFS-Clients keine Protokolloperationen haben, die ein schreibgeschütztes Bit pro Datei verwenden.

ONTAP kann das Schreibschutzbit einer Datei setzen, wenn diese von einem SMB-Client unter Windows erstellt wird. ONTAP kann das Schreibschutzbit auch setzen, wenn eine Datei zwischen NFS-Clients und SMB-Clients gemeinsam genutzt wird. Manche Software erfordert, dass das Schreibschutzbit aktiviert ist, wenn sie von NFS-Clients und SMB-Clients verwendet wird.

Damit ONTAP die korrekten Lese- und Schreibberechtigungen für eine zwischen NFS-Client und SMB-Client gemeinsam genutzte Datei beibehält, wird das Schreibschutzbit nach den folgenden Regeln behandelt:

- NFS behandelt jede Datei, bei der das Schreibschutzbit aktiviert ist, so, als ob keine Schreibberechtigungsbits aktiviert sind.
- Wenn ein NFS-Client alle Schreibberechtigungsbits deaktiviert und mindestens eines dieser Bits zuvor aktiviert war, aktiviert ONTAP das Schreibschutzbit für diese Datei.
- Wenn ein NFS-Client ein Schreibberechtigungsbit aktiviert, deaktiviert ONTAP das Nur-Lesen-Bit für diese Datei.
- Wenn das Schreibschutzbit einer Datei aktiviert ist und ein NFS-Client versucht, die 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, wobei die Schreibberechtigungsbits maskiert sind.
- Wenn das Schreibschutzbit einer Datei aktiviert ist und ein SMB-Client das Schreibschutzbit deaktiviert, aktiviert ONTAP das Schreibberechtigungsbit des Eigentümers für die Datei.
- Dateien, bei denen das Schreibschutzbit aktiviert ist, sind nur für root beschreibbar.

Das Schreibschutzbit interagiert mit den ACL- und Unix-Modusbits auf folgende Weise:

Wenn das Schreibschutzbit einer Datei gesetzt ist:

- An der ACL für diese Datei werden keine Änderungen vorgenommen. NFS-Clients sehen dieselbe ACL wie vor dem Setzen des Schreibschutzbits.
- Sämtliche Unix-Modusbits, die Schreibzugriff auf die Datei ermöglichen, werden ignoriert.
- Sowohl NFS- als auch SMB-Clients können die Datei lesen, aber sie können sie nicht verändern.
- ACLs und UNIX-Modusbits werden zugunsten des Schreibschutzbits ignoriert. Das bedeutet, dass selbst wenn die ACL Schreibzugriff erlaubt, das Schreibschutzbit Änderungen verhindert.

Wenn das Schreibschutzbit einer Datei nicht gesetzt ist:

- ONTAP bestimmt den Zugriff anhand der ACL und der UNIX-Modusbits.
  - Wenn entweder die ACL oder die UNIX-Modusbits den Schreibzugriff verweigern, können NFS- und SMB-Clients die Datei nicht ändern.
  - Wenn weder die ACL noch die UNIX-Modusbits den Schreibzugriff verweigern, können NFS- und SMB-Clients die Datei ändern.



Änderungen an Dateiberechtigungen werden auf SMB-Clients sofort wirksam, auf NFS-Clients hingegen möglicherweise nicht sofort, wenn der NFS-Client das Attribut-Caching aktiviert.

## Unterschiede zwischen ONTAP NFS und Windows bei der Handhabung von Sperren auf Freigabepfadkomponenten

Im Gegensatz zu Windows sperrt ONTAP nicht die einzelnen Komponenten des Pfades zu einer geöffneten Datei, solange die Datei geöffnet ist. Dieses Verhalten betrifft auch

SMB-Freigabepfade.

Da ONTAP die einzelnen Pfadkomponenten nicht sperrt, ist es möglich, eine Pfadkomponente oberhalb der geöffneten Datei oder Freigabe umzubenennen, was bei bestimmten Anwendungen zu Problemen führen oder den Freigabepfad in der SMB-Konfiguration ungültig machen kann. Dies kann dazu führen, dass die Freigabe nicht zugänglich ist.

Um Probleme zu vermeiden, die durch das Umbenennen von Pfadkomponenten entstehen, lassen sich Sicherheitseinstellungen der Windows Access Control List (ACL) anwenden, die verhindern, dass Benutzer oder Anwendungen kritische Verzeichnisse umbenennen.

Weitere Informationen zu "Wie verhindert werden kann, dass Verzeichnisse umbenannt werden, während Clients darauf zugreifen".

## Informationen zu Sperren für ONTAP NFS SVMs anzeigen

Informationen über die aktuellen Dateisperren können angezeigt werden, einschließlich der Art der gehaltenen Sperren und des Sperrstatus, Details zu Bytebereichssperren, Sharelock-Modi, Delegation Locks und Opportunistic Locks sowie darüber, ob Sperren mit dauerhaften oder persistenten Handles geöffnet sind.

### Über diese Aufgabe

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

Standardmäßig zeigt der Befehl Informationen zu allen Sperren an. Mit Befehlsparametern lässt sich die Anzeige von Informationen zu Sperren für eine bestimmte Storage Virtual Machine (SVM) steuern oder die Ausgabe des Befehls nach anderen Kriterien filtern.

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

- Byte-Range-Sperren, die nur einen Teil einer Datei sperren.
- Freigabesperren, die geöffnete Dateien sperren.
- Opportunistische Sperren, die das Client-seitige Caching über SMB steuern.
- Delegationen, die das Client-seitige Caching über NFSv4.x steuern.

Durch die Angabe optionaler Parameter lassen sich wichtige Informationen zu jedem Sperrtyp ermitteln. Weitere Informationen zu `vserver locks show` finden sich in der "ONTAP-Befehlsreferenz".

### Schritt

1. Informationen zu Sperren werden mit dem `vserver locks show` Befehl angezeigt.

### Beispiele

Das folgende Beispiel zeigt zusammenfassende Informationen zu einer NFSv4-Sperre für eine Datei mit dem Pfad `/vol1/file1`. Der Zugriffsmodus von Sharelock ist write-deny_none, und die Sperre wurde mit Schreibdelegation gewährt:

```
cluster1::> vserver locks show

Vserver: vs0
```

```
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
              Sharelock Mode: write-deny_none
                                                        delegation  -
              Delegation Type: write
```

Das folgende Beispiel zeigt detaillierte Oplock- und Sharelock-Informationen zur SMB-Sperre einer Datei mit dem Pfad `/data2/data2_2/intro.pptx`. Ein dauerhafter Handle wird für die Datei mit dem Sharelock-Zugriffsmodus write-deny_none an einen Client mit der IP-Adresse 10.3.1.3 gewährt. Ein Lease-Oplock wird mit dem Oplock-Level Batch 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
```

## Dateisperren für ONTAP NFS SVMs aufheben

Wenn Dateisperren den Zugriff von Clients auf Dateien verhindern, können Informationen über die aktuell bestehenden Sperren angezeigt und anschließend bestimmte Sperren aufgehoben werden. Beispiele für Szenarien, in denen das Aufheben von Sperren erforderlich sein kann, sind das Debuggen von Anwendungen.

### Über diese Aufgabe

Der `vserver locks break`Befehl ist nur auf der erweiterten Berechtigungsstufe und höher verfügbar. Weitere Informationen zu `vserver locks break` finden sich in der "ONTAP-Befehlsreferenz".

### Schritte

1. Um die Informationen zu finden, die Sie zum Aufheben einer Sperre benötigen, verwenden Sie den `vserver locks show` Befehl.

   Weitere Informationen zu `vserver locks show` finden sich in der "ONTAP-Befehlsreferenz".

2. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

3. Führen Sie eine der folgenden Aktionen aus:

| Wenn ein Schloss durch Angabe von… aufgehoben werden soll | Geben Sie den Befehl ein… |
|---|---|

| | |
|---|---|
| Der SVM Name, der Volumenname, der LIF Name und der Dateipfad | `vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif` |
| Die Lock-ID | `vserver locks break -lockid UUID` |

4. Zurück zur Administrator-Privilegstufe:

   `set -privilege admin`

# Funktionsweise der ONTAP FPolicy-Filter für Erstlesen und Erstschreiben mit NFS

NFS-Clients erleben eine hohe Antwortzeit bei hohem Datenverkehr von lesen/schreiben-Anfragen, wenn die FPolicy unter Verwendung eines externen FPolicy-Servers mit lesen/schreiben-Operationen als überwachte Ereignisse aktiviert ist. Für NFS-Clients verringert der Einsatz von First-Read- und First-Write-Filtern in der FPolicy die Anzahl der FPolicy-Benachrichtigungen und verbessert die Performance.

Bei NFS führt der Client Ein-/Ausgabeoperationen an einer Datei durch, indem er deren Handle abruft. Dieses Handle kann auch nach Neustarts von Server und Client gültig bleiben. Daher kann der Client das Handle zwischenspeichern und Anfragen darüber senden, ohne die Handles erneut abrufen zu müssen. In einer regulären Sitzung werden zahlreiche Lese-/Schreibanfragen an den Dateiserver gesendet. Wenn für all diese Anfragen Benachrichtigungen generiert werden, kann dies zu folgenden Problemen führen:

- Eine höhere Last aufgrund zusätzlicher Benachrichtigungsverarbeitung und längerer Reaktionszeit.
- Es werden zahlreiche Benachrichtigungen an den FPolicy Server gesendet, obwohl der Server von keiner der Benachrichtigungen betroffen ist.

Nach dem Empfang der ersten lesen/schreiben-Anfrage eines Clients für eine bestimmte Datei wird ein Cache-Eintrag erstellt und der lesen/schreiben-Zähler erhöht. Diese Anfrage wird als erster lesen/schreiben-Schreibvorgang markiert und ein FPolicy-Ereignis wird generiert. Vor der Planung und Erstellung von FPolicy-Filtern für einen NFS-Client ist es wichtig, die Grundlagen der Funktionsweise von FPolicy-Filtern zu verstehen.

- First-read: Filtert die Client-Leseanfragen für First-read.

  Wenn dieser Filter für NFS-Ereignisse verwendet wird, bestimmen die `-file-session-io-grouping-count`- und `-file-session-io-grouping-duration`-Einstellungen die erste Leseanforderung, für die FPolicy verarbeitet wird.

- First-write: Filtert die Schreibanfragen des Clients nach dem Prinzip „First-write“.

  Wenn dieser Filter für NFS-Ereignisse verwendet wird, bestimmen die `-file-session-io-grouping-count`- und `-file-session-io-grouping-duration`-Einstellungen die erste Schreibanforderung, die von FPolicy verarbeitet wurde.

Die folgenden Optionen werden in die NFS-Datenbank aufgenommen.

```
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
```

# Die NFSv4.1-Serverimplementierungs-ID für ONTAP SVMs ändern

Das NFSv4.1-Protokoll enthält eine Server-Implementierungs-ID, die die Serverdomäne, den Namen und das Datum dokumentiert. Die Standardwerte der Server-Implementierungs-ID können angepasst werden. Eine Änderung der Standardwerte kann beispielsweise beim Erfassen von Nutzungsstatistiken oder beim Beheben von Interoperabilitätsproblemen hilfreich sein. Weitere Informationen stehen in RFC 5661.

**Über diese Aufgabe**

Die Standardwerte für die drei Optionen lauten wie folgt:

| Option | Optionsname | Standardwert |
|---|---|---|
| NFSv4.1 Implementierungs-ID-Domäne | `-v4.1-implementation -domain` | netapp.com |
| NFSv4.1 Implementierungs-ID Name | `-v4.1-implementation-name` | Cluster Versionsname |
| NFSv4.1 Implementierungs-ID Datum | `-v4.1-implementation-date` | Datum der Clusterversion |

**Schritte**

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   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 | `vserver nfs modify -v4.1 -implementation-domain domain` |
| Name | `vserver nfs modify -v4.1 -implementation-name name` |
| Datum | `vserver nfs modify -v4.1 -implementation-date date` |

3. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

# NFSv4-ACLs verwalten

## Informationen zu den Vorteilen der Aktivierung von NFSv4-ACLs für ONTAP SVMs

Die Aktivierung von NFSv4 ACLs bietet viele Vorteile.

Die Vorteile der Aktivierung von NFSv4-ACLs umfassen Folgendes:

- Feinere Steuerung des Benutzerzugriffs auf Dateien und Verzeichnisse
- Bessere NFS-Sicherheit
- Verbesserte Interoperabilität mit CIFS
- Aufhebung der NFS-Beschränkung von 16 Gruppen pro Benutzer

## Informationen zu NFSv4-ACLs für ONTAP SVMs

Ein Client, der NFSv4-ACLs verwendet, kann ACLs für Dateien und Verzeichnisse im System festlegen und anzeigen. Wenn in einem Verzeichnis mit einer ACL eine neue Datei oder ein neues Unterverzeichnis erstellt wird, erbt die neue Datei bzw. das neue Unterverzeichnis alle Zugriffssteuerungseinträge (ACEs) in der ACL, die mit den entsprechenden Vererbungsflags versehen sind.

Wird eine Datei oder ein Verzeichnis als Ergebnis einer NFSv4-Anfrage erstellt, hängt die ACL der resultierenden Datei oder des resultierenden Verzeichnisses davon ab, ob die Dateierstellungsanfrage eine ACL oder nur die standardmäßigen UNIX-Dateizugriffsberechtigungen enthält und ob das übergeordnete Verzeichnis über eine ACL verfügt:

- Wenn die Anfrage eine ACL enthält, wird diese ACL verwendet.
- Enthält die Anfrage lediglich Standard-UNIX-Dateizugriffsberechtigungen, verfügt das übergeordnete Verzeichnis jedoch über eine ACL, werden die ACEs in der ACL des übergeordneten Verzeichnisses von der neuen Datei oder dem neuen Verzeichnis übernommen, sofern die ACEs mit den entsprechenden Vererbungsflags versehen wurden.

  Eine übergeordnete ACL wird auch dann vererbt, wenn `-v4.0-acl` auf `off` gesetzt ist.

- Wenn die Anfrage nur Standard-UNIX-Dateizugriffsberechtigungen enthält und das übergeordnete Verzeichnis keine ACL hat, wird der Client-Dateimodus verwendet, um die Standard-UNIX-Dateizugriffsberechtigungen festzulegen.
- Wenn die Anfrage nur Standard-UNIX-Dateizugriffsberechtigungen enthält und das übergeordnete Verzeichnis eine nicht vererbbare ACL hat, wird das neue Objekt nur mit Modusbits erstellt.

Wenn der `-chown-mode` Parameter auf `restricted` mit Befehlen aus den `vserver nfs`- oder `vserver export-policy rule`-Familien gesetzt wurde, kann die Dateibesitzberechtigung nur vom Superuser geändert werden, selbst wenn die mit NFSv4-ACLs festgelegten Berechtigungen auf der Festplatte es einem Nicht-Root-Benutzer erlauben, die Dateibesitzberechtigung zu ändern. Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

## Aktivieren oder Deaktivieren der NFSv4-ACL-Änderung für ONTAP SVMs

Wenn ONTAP einen `chmod` Befehl für eine Datei oder ein Verzeichnis mit einer ACL empfängt, wird die ACL standardmäßig beibehalten und entsprechend der Änderung des Modusbits angepasst. Es besteht die Möglichkeit, den `-v4-acl-preserve` Parameter zu deaktivieren, wodurch das Verhalten geändert wird, sodass die ACL stattdessen entfernt wird.

**Über diese Aufgabe**

Bei Verwendung des einheitlichen Sicherheitsstils legt dieser Parameter auch fest, ob die NTFS-Dateiberechtigungen erhalten bleiben oder verworfen werden, wenn ein Client einen chmod, chgroup oder chown Befehl für eine Datei oder ein Verzeichnis sendet.

Dieser Parameter ist standardmäßig aktiviert.

**Schritte**

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

| Wenn Sie möchten… | Führen Sie den folgenden Befehl aus… |
|---|---|
| Beibehaltung und Änderung bestehender NFSv4-ACLs (Standard) ermöglichen | `vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled` |
| Beibehaltung deaktivieren und NFSv4-ACLs beim Ändern der Modusbits entfernen | `vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled` |

3. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

## Wie ONTAP NFSv4-ACLs verwendet, um zu bestimmen, ob Dateien gelöscht werden können

Um festzustellen, ob eine Datei gelöscht werden kann, verwendet ONTAP eine Kombination aus dem DELETE-Bit der Datei und dem DELETE_CHILD-Bit des übergeordneten Verzeichnisses. Weitere Informationen enthält die NFS 4.1 RFC 5661.

## NFSv4-ACLs für ONTAP SVMs aktivieren oder deaktivieren

Um NFSv4-ACLs zu aktivieren oder zu deaktivieren, können die Optionen `-v4.0-acl` und `-v4.1-acl` geändert werden. Diese Optionen sind standardmäßig deaktiviert.

**Über diese Aufgabe**

Die `-v4.0-acl` oder `-v4.1-acl` Option steuert das Festlegen und Anzeigen von NFSv4-ACLs; sie steuert nicht die Durchsetzung dieser ACLs für die Zugriffsprüfung.

**Schritt**

1. Führen Sie eine der folgenden Aktionen aus:

| Wenn Sie möchten… | Dann… |
|---|---|
| NFSv4.0-ACLs aktivieren | Führen Sie den folgenden Befehl aus:<br><br>`vserver nfs modify -vserver vserver_name -v4.0-acl enabled` |
| NFSv4.0 ACLs deaktivieren | Führen Sie den folgenden Befehl aus:<br><br>`vserver nfs modify -vserver vserver_name -v4.0-acl disabled` |
| NFSv4.1-ACLs aktivieren | Führen Sie den folgenden Befehl aus:<br><br>`vserver nfs modify -vserver vserver_name -v4.1-acl enabled` |
| NFSv4.1 ACLs deaktivieren | Führen Sie den folgenden Befehl aus:<br><br>`vserver nfs modify -vserver vserver_name -v4.1-acl disabled` |

## Ändern des maximalen ACE-Limits für NFSv4-ACLs für ONTAP SVMs

Sie können die maximale Anzahl zulässiger ACEs für jede NFSv4-ACL durch Ändern des Parameters `-v4-acl-max-aces` anpassen. Standardmäßig ist das Limit auf 400 ACEs pro ACL festgelegt. Eine Erhöhung dieses Limits kann dazu beitragen, die erfolgreiche Migration von Daten mit ACLs, die mehr als 400 ACEs enthalten, auf Speichersysteme mit ONTAP sicherzustellen.

**Über diese Aufgabe**

Eine Erhöhung dieses Grenzwerts könnte die Leistung von Clients beeinträchtigen, die auf Dateien mit NFSv4-ACLs zugreifen.

**Schritte**

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Das maximale ACE-Limit für NFSv4-ACLs ändern:

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

   Der gültige Bereich von

   `max_ace_limit` ist `192` zu `1024`.

3. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

# NFSv4 Dateidelegierungen verwalten

## Aktivieren oder Deaktivieren von NFSv4-Lesedelegationen für ONTAP SVMs

Um die NFSv4-Dateilesedelegierungen zu aktivieren oder zu deaktivieren, kann die `-v4.0-read-delegation`oder Option geändert werden. Durch das Aktivieren von Dateilesedelegierungen kann ein Großteil des mit dem Öffnen und Schließen von Dateien verbundenen Nachrichtenaufwands eliminiert werden.

**Über diese Aufgabe**

Standardmäßig sind Lese-Dateidelegationen deaktiviert.

Der Nachteil der Aktivierung von Lesedateidelegierungen besteht darin, dass der Server und seine Clients die Delegierungen nach einem Neustart oder Reboot des Servers, eines Clients oder wenn eine Netzwerkpartition auftritt, wiederherstellen müssen.

**Schritt**

1. Führen Sie eine der folgenden Aktionen aus:

| Wenn Sie möchten… | Dann… |
|---|---|
| NFSv4-Lesedelegationen für Dateien aktivieren | Führen Sie den folgenden Befehl aus:<br><br>`vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled` |
| NFSv4.1-Lesedelegationen für Dateien aktivieren | Führen Sie den folgenden Befehl aus:<br><br>+<br>`vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled` |
| NFSv4 Lese-Dateidelegationen deaktivieren | Führen Sie den folgenden Befehl aus:<br><br>`vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled` |
| NFSv4.1 Lese-Dateidelegationen deaktivieren | Führen Sie den folgenden Befehl aus:<br><br>`vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled` |

**Ergebnis**

Die Dateidelegierungsoptionen werden sofort nach ihrer Änderung wirksam. Ein Neustart oder das erneute Starten von NFS ist nicht erforderlich.

## NFSv4 Schreibdelegationen für ONTAP SVMs aktivieren oder deaktivieren

Um Schreibdelegationen für Dateien zu aktivieren oder zu deaktivieren, kann die `-v4.0 -write-delegation`oder Option angepasst werden. Durch das Aktivieren von Schreibdelegationen für Dateien wird ein Großteil des Nachrichtenaufwands vermieden, der mit Datei- und Datensatzsperren sowie dem Öffnen und Schließen von Dateien

verbunden ist.

**Über diese Aufgabe**

Standardmäßig sind Schreibdelegationen deaktiviert.

Der Nachteil der Aktivierung von Schreibdelegationen besteht darin, dass der Server und seine Clients zusätzliche Aufgaben ausführen müssen, um die Delegationen nach einem Neustart oder Reboot des Servers, eines Clients oder bei einer Netzwerkpartition wiederherzustellen.

**Schritt**

1. Führen Sie eine der folgenden Aktionen aus:

| Wenn Sie möchten… | Dann… |
|---|---|
| NFSv4 Schreibdateidelegierungen aktivieren | Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled` |
| NFSv4.1 Schreibdateidelegierungen aktivieren | Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled` |
| Deaktivieren von NFSv4 schreiben Datei-Delegationen | Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled` |
| Deaktivieren von NFSv4.1 schreiben Datei-Delegationen | Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled` |

**Ergebnis**

Die Dateidelegierungsoptionen werden sofort nach ihrer Änderung wirksam. Ein Neustart oder das erneute Starten von NFS ist nicht erforderlich.

# Konfiguration der NFSv4 Datei- und Datensatzsperrung

## Informationen zur NFSv4 Datei- und Datensatzsperrung für ONTAP SVMs

Für NFSv4-Clients unterstützt ONTAP den NFSv4-Dateisperrmechanismus und verwaltet den Status aller Dateisperren nach einem lease-basierten Modell.

"NetApp Technical Report 3580: NFSv4-Erweiterungen und Best Practices-Leitfaden Data ONTAP Implementierung"

## Die Sperrfrist für NFSv4-Locking bei ONTAP SVMs angeben

Um den Sperr-Lease-Zeitraum für NFSv4 festzulegen (das heißt, den Zeitraum, in dem ONTAP einem Client unwiderruflich eine Sperre gewährt), kann die `-v4-lease -seconds` Option angepasst werden. Kürzere Lease-Zeiträume beschleunigen die Serverwiederherstellung, während längere Lease-Zeiträume für Server mit einer sehr großen Anzahl von Clients vorteilhaft sind.

**Über diese Aufgabe**

Standardmäßig ist diese Option auf `30` eingestellt. Der Mindestwert für diese Option ist `10`. Der Höchstwert für diese Option ist die Sperrfrist, die mit der `locking.lease_seconds` Option festgelegt werden kann.

**Schritte**

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Führen Sie den folgenden Befehl aus:

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

3. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

### Die NFSv4-Sperrfrist für ONTAP SVMs angeben

Um die NFSv4-Sperrfrist festzulegen (d. h. den Zeitraum, in dem Clients versuchen, ihren Sperrstatus von ONTAP während der Serverwiederherstellung zurückzuerhalten), kann die `-v4-grace-seconds` Option angepasst werden.

**Über diese Aufgabe**

Standardmäßig ist diese Option auf `45` eingestellt.

**Schritte**

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Führen Sie den folgenden Befehl aus:

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

3. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

# Informationen zu NFSv4-Verweisen für ONTAP SVMs

Wenn NFSv4-Weiterleitungen aktiviert sind, stellt ONTAP „Intra-SVM“-Weiterleitungen für NFSv4-Clients bereit. Eine Intra-SVM-Weiterleitung liegt vor, wenn ein Cluster-Knoten, der die NFSv4-Anfrage empfängt, den NFSv4-Client an eine andere logische Schnittstelle (LIF) auf der Storage Virtual Machine (SVM) verweist.

Der NFSv4-Client sollte ab diesem Zeitpunkt auf den Pfad zugreifen, der die Weiterleitung am Ziel-LIF erhalten hat. Der ursprüngliche Cluster-Node stellt eine solche Weiterleitung bereit, wenn festgestellt wird, dass im SVM ein LIF existiert, das auf dem Cluster-Node residiert, auf dem sich das Daten-Volume befindet. Dadurch wird den Clients ein schnellerer Zugriff auf die Daten ermöglicht und zusätzliche Cluster-Kommunikation vermieden.

# NFSv4-Verweise für ONTAP SVMs aktivieren oder deaktivieren

Sie können NFSv4-Verweise auf Storage Virtual Machines (SVMs) aktivieren, indem Sie die Optionen `-v4-fsid-change` und `-v4.0-referrals` oder aktivieren. Die Aktivierung von NFSv4-Verweisen kann zu schnellerem Datenzugriff für NFSv4-Clients führen, die diese Funktion unterstützen.

**Bevor Sie beginnen**

Wenn Sie NFS-Verweise aktivieren möchten, müssen Sie zuerst paralleles NFS deaktivieren. Sie können nicht beides gleichzeitig aktivieren.

**Schritte**

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

| Wenn Sie möchten… | Geben Sie den Befehl ein… |
|---|---|
| NFSv4 Verweise aktivieren | `vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled` |
| NFSv4-Verweise deaktivieren | `vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled` |
| NFSv4.1 Verweise aktivieren | `vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled` |
| NFSv4.1-Verweise deaktivieren | `vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled` |

3. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

# Statistiken für ONTAP NFS SVMs anzeigen

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

**Schritte**

1. Mit dem `statistics catalog object show`Befehl lassen sich die NFS-Objekte identifizieren, von denen Daten angezeigt werden können.

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

2. Verwenden Sie die `statistics start` und optionalen `statistics stop` Befehle, um eine Datenprobe von einem oder mehreren Objekten zu erfassen.
3. Mit dem `statistics show` Befehl lassen sich die Beispieldaten anzeigen.

**Beispiel: Überwachung der NFSv3 Leistung**

Das folgende Beispiel zeigt Leistungsdaten für das NFSv3 Protokoll.

Der folgende Befehl startet die Datenerfassung für eine neue Probe:

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

Der folgende Befehl zeigt Daten aus der Stichprobe an, indem Zähler angegeben werden, die die Anzahl erfolgreicher Lese- und Schreibanforderungen im Verhältnis zur 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 Leistungsüberwachung"
- "Statistiken Katalogobjekt anzeigen"
- "Statistiken zeigen"
- "Statistiken Start"
- "Statistiken stoppen"

# DNS-Statistiken für ONTAP NFS SVMs anzeigen

Sie können DNS-Statistiken für Storage Virtual Machines (SVMs) auf dem Speichersystem anzeigen, um die Leistung zu überwachen und Probleme zu diagnostizieren.

**Schritte**

1. Mit dem `statistics catalog object show`Befehl lassen sich die DNS-Objekte identifizieren, von denen Daten angezeigt werden können.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Die `statistics start`- und `statistics stop`-Befehle dienen dazu, eine Datenprobe von einem oder mehreren Objekten zu erfassen.
3. Mit dem `statistics show` Befehl lassen sich die Beispieldaten anzeigen.

## Überwachung der DNS Statistiken

Die folgenden Beispiele zeigen Leistungsdaten für DNS-Abfragen. Die folgenden Befehle starten die Datenerfassung für eine neue Stichprobe:

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

Der folgende Befehl zeigt Daten aus der Stichprobe an, indem Zähler angegeben werden, die die Anzahl der gesendeten DNS-Abfragen der Anzahl der empfangenen, fehlgeschlagenen oder abgelaufenen DNS-Abfragen gegenüberstellen:

```
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.
```

Der folgende Befehl zeigt Daten aus der Stichprobe an, indem Zähler angegeben werden, die die Anzahl der

Male anzeigen, bei denen ein bestimmter Fehler bei einer 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**

- "Einrichtung der Leistungsüberwachung"
- "Statistiken Katalogobjekt anzeigen"
- "Statistiken zeigen"
- "Statistiken Start"
- "Statistiken stoppen"

# NIS-Statistiken für ONTAP NFS SVMs anzeigen

Sie können NIS-Statistiken für Storage Virtual Machines (SVMs) auf dem Speichersystem anzeigen, um die Leistung zu überwachen und Probleme zu diagnostizieren.

**Schritte**

1. Mit dem `statistics catalog object show`Befehl lassen sich die NIS-Objekte identifizieren, von denen Daten angezeigt werden können.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Die `statistics start`- und `statistics stop`-Befehle dienen dazu, eine Datenprobe von einem oder mehreren Objekten zu erfassen.
3. Mit dem `statistics show` Befehl lassen sich die Beispieldaten anzeigen.

## Überwachung der NIS Statistiken

Die folgenden Beispiele zeigen Leistungsdaten für NIS-Abfragen. Die folgenden Befehle starten die Datenerfassung für eine neue Stichprobe:

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

Der folgende Befehl zeigt Daten aus der Stichprobe an, indem Zähler angegeben werden, die die Anzahl der gesendeten NIS-Abfragen der Anzahl der empfangenen, fehlgeschlagenen oder abgelaufenen NIS-Abfragen gegenüberstellen:

```
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.
```

Der folgende Befehl zeigt Daten aus der Stichprobe an, indem Zähler angegeben werden, die die Anzahl der Male anzeigen, bei 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 Leistungsüberwachung"
- "Statistiken Katalogobjekt anzeigen"
- "Statistiken zeigen"
- "Statistiken Start"
- "Statistiken stoppen"

# Informationen zur Unterstützung von VMware vStorage über ONTAP NFS

ONTAP unterstützt bestimmte VMware vStorage APIs für Array Integration (VAAI)-Funktionen in einer NFS-Umgebung.

## Unterstützte Funktionen

Folgende Funktionen werden unterstützt:

- Copy Offload

  Ermöglicht einem ESXi-Host, virtuelle Maschinen oder virtuelle Festplatten (VMDKs) direkt zwischen Quell- und Ziel-Datenspeicherort zu kopieren, ohne den Host einzubeziehen. Dadurch werden ESXi-Host-CPU-Zyklen und Netzwerkbandbreite eingespart. Copy Offload erhält die Speicherplatzeffizienz, wenn das Quellvolume dünn bereitgestellt ist.

- Platzreservierung

  Gewährleistet Speicherplatz für eine VMDK-Datei, indem Speicherplatz dafür reserviert wird.

- Speicherplatzrückgewinnung (ab ONTAP 9.20.1)

  Gibt Speicherplatz von Thin-Provisioning-VMDKs über das NetApp NFS-Plug-in für VMware VAAI 3.0 oder höher frei. Wenn Gastbetriebssysteme Daten löschen oder anderweitig Speicherplatz in einer virtuellen Maschine freigeben, kann das Plug-in die freigegebenen Blöcke aus dem zugrunde liegenden ONTAP Volume zurückgewinnen.

## Einschränkungen

VMware vStorage over NFS weist folgende Einschränkungen auf:

- Copy-Offload-Vorgänge können in folgenden Szenarien fehlschlagen:
  - Während der Ausführung von wafliron auf dem Quell- oder Zielvolume, da das Volume dadurch

vorübergehend offline genommen wird

- Beim Verschieben des Quell- oder Ziel-Volumes
- Beim Verschieben des Quell- oder Ziel-LIF
- Während der Durchführung von Takeover- oder Giveback-Operationen
- Während der Durchführung von Umschalt- oder Rückschaltvorgängen

- Serverseitiges Kopieren kann aufgrund von Unterschieden im Dateihandle-Format im folgenden Szenario fehlschlagen:

  Sie versuchen, Daten von SVMs, die aktuell oder zuvor Qtrees exportiert haben, auf SVMs zu kopieren, die noch nie Qtrees exportiert haben. Um diese Einschränkung zu umgehen, ist es möglich, mindestens einen Qtree auf der Ziel SVM zu exportieren.

**Verwandte Informationen**

"Welche VAAI-Offloaded-Operationen werden von Data ONTAP unterstützt?"

# VMware vStorage über ONTAP NFS aktivieren oder deaktivieren

Sie können die Unterstützung für VMware vStorage über NFS auf Storage Virtual Machines (SVMs) mithilfe des `vserver nfs modify` Befehls aktivieren oder deaktivieren. Diese Einstellung steuert VMware VAAI über NFS Vorgänge wie Copy Offload und Speicherplatzreservierung.

**Über diese Aufgabe**

Standardmäßig ist die Unterstützung für VMware vStorage über NFS deaktiviert.

Ab ONTAP 9.20.1 unterstützt die Aktivierung von VMware vStorage over ONTAP NFS auch die automatische Speicherplatzrückgewinnung für per Thin Provisioning bereitgestellte NFSv3- und NFSv4.1-Datastores.

**Schritte**

1. Überprüfung der aktuellen VMware vStorage over NFS-Einstellung für die SVM:

   ```
   vserver nfs show -vserver vserver_name -fields vstorage
   ```

2. Führen Sie eine der folgenden Aktionen aus:

| Wenn Sie möchten… | Führen Sie den folgenden Befehl aus… |
|---|---|
| VMware vStorage-Unterstützung aktivieren | `vserver nfs modify -vserver vserver_name -vstorage enabled` |
| VMware vStorage-Support deaktivieren | `vserver nfs modify -vserver vserver_name -vstorage disabled` |

3. Überprüfung, ob die Einstellung aktualisiert ist:

   ```
   vserver nfs show -vserver vserver_name -fields vstorage
   ```

**Nachdem Sie fertig sind**

Sie müssen das NetApp NFS Plug-in für VMware VAAI installieren, bevor Sie diese Funktionalität verwenden können. Die automatische Speicherplatzfreigabe erfordert Version 3.0 oder höher.

Informationen zu VMware Host-, Plug-in- und Interoperabilitätsanforderungen sind in der NetApp NFS Plug-in for VMware VAAI Dokumentation und im NetApp Interoperability Matrix Tool zu finden.

**Verwandte Informationen**

"NetApp Dokumentation: NetApp NFS Plug-in für VMware VAAI"

"NetApp Interoperabilitätsmatrix-Tool"

# rquota-Unterstützung auf ONTAP NFS SVMs aktivieren oder deaktivieren

Das Remote Quota Protocol (rquota) ermöglicht es NFS-Clients, Kontingentinformationen für Benutzer von einem entfernten Rechner abzurufen. Die Unterstützung für rquota-Versionen variiert je nach Ihrer ONTAP-Version.

- rquota v1 wird in ONTAP 9 und höher unterstützt.
- rquota v2 wird in ONTAP 9.12.1 und später unterstützt.

  Wenn Sie von rquota v1 auf rquota v2 aktualisieren, kann es zu einer unerwarteten Änderung Ihres Benutzerkontingents kommen. Diese Änderung ergibt sich aus dem Unterschied in der Berechnung des Kontingents zwischen rquota v1 und rquota v2. Weitere Informationen sind in der "NetApp Knowledge Base: Warum hat sich das Benutzerkontingent unerwartet geändert?" zu finden.

**Über diese Aufgabe**

Standardmäßig ist rquota deaktiviert.

**Schritt**

1. rquota aktivieren oder deaktivieren:

| Wenn Sie möchten… | Führen Sie den folgenden Befehl aus… |
|---|---|
| rquota-Unterstützung für SVMs aktivieren | `vserver nfs modify -vserver vserver_name -rquota enable` |
| rquota-Unterstützung für SVMs deaktivieren | `vserver nfs modify -vserver vserver_name -rquota disable` |

Weitere Informationen zu Quoten sind unter "Logische Speicherverwaltung" zu finden.

# Informationen zu Leistungsverbesserungen bei NFSv3 und NFSv4 sowie zur TCP-Übertragungsgröße für ONTAP SVMs

Die Leistung von NFSv3- und NFSv4-Clients, die über ein Netzwerk mit hoher Latenz eine Verbindung zu Speichersystemen herstellen, kann durch Ändern der maximalen

TCP-Übertragungsgröße verbessert werden.

Wenn Clients über ein Netzwerk mit hoher Latenz, wie zum Beispiel ein Weitverkehrsnetz (WAN) oder ein Metropolnetz (MAN) mit einer Latenz von über 10 Millisekunden, auf Speichersysteme zugreifen, kann die Verbindungsleistung durch Anpassen der maximalen TCP-Übertragungsgröße möglicherweise verbessert werden. Clients, die in einem Netzwerk mit niedriger Latenz, wie einem lokalen Netzwerk (LAN), auf Speichersysteme zugreifen, profitieren in der Regel kaum oder gar nicht von der Änderung dieser Parameter. Überwiegt die Verbesserung des Durchsatzes die Auswirkungen auf die Latenz nicht, empfiehlt sich die Verwendung dieser Parameter nicht.

Um festzustellen, ob Ihre Speicherumgebung von einer Anpassung dieser Parameter profitieren würde, sollte zunächst eine umfassende Leistungsbewertung eines leistungsschwachen NFS-Client durchgeführt werden. Es ist zu prüfen, ob die geringe Leistung auf eine übermäßige Roundtrip-Latenz und kleine Anfragen auf dem Client zurückzuführen ist. Unter diesen Bedingungen können der Client und der Server die verfügbare Bandbreite nicht vollständig nutzen, da sie den Großteil ihrer Arbeitszyklen mit dem Warten auf die Übertragung kleiner Anfragen und Antworten verbringen.

Durch die Erhöhung der NFSv3- und NFSv4-Anforderungsgröße können Client und Server die verfügbare Bandbreite effektiver nutzen, um mehr Daten pro Zeiteinheit zu übertragen, wodurch die Gesamteffizienz der Verbindung steigt.

Beachten Sie, dass die Konfiguration zwischen Speichersystem und Client variieren kann. Das Speichersystem und der Client unterstützen eine maximale Übertragungsgröße von 1 MB für Übertragungsvorgänge. Wenn das Speichersystem jedoch für eine maximale Übertragungsgröße von 1 MB konfiguriert ist, der Client aber nur 64 KB unterstützt, ist die Übertragungsgröße beim Mounten auf 64 KB oder weniger begrenzt.

Vor einer Änderung dieser Parameter ist zu beachten, dass dies zu einem zusätzlichen Speicherverbrauch im Speichersystem für die Zeit führt, die zum Zusammenstellen und Übertragen einer großen Antwort erforderlich ist. Je mehr Verbindungen mit hoher Latenz zum Speichersystem bestehen, desto höher ist der zusätzliche Speicherverbrauch. Speichersysteme mit hoher Speicherkapazität sind von dieser Änderung möglicherweise kaum betroffen. Speichersysteme mit geringer Speicherkapazität können hingegen eine spürbare Verschlechterung der Performance erfahren.

Die erfolgreiche Nutzung dieser Parameter setzt die Fähigkeit voraus, Daten von mehreren Knoten eines Clusters abzurufen. Die systembedingte Latenz des Clusternetzwerks kann die Gesamtlatenz der Antwort erhöhen. Die Gesamtlatenz steigt tendenziell bei Verwendung dieser Parameter. Daher kann sich dies negativ auf latenzempfindliche Workloads auswirken.

# Die maximale TCP-Übertragungsgröße für NFSv3 und NFSv4 bei ONTAP SVMs anpassen

Sie können die `-tcp-max-xfer-size` Option ändern, um die maximalen Übertragungsgrößen für alle TCP-Verbindungen mit den Protokollen NFSv3 und NFSv4.x zu konfigurieren.

**Über diese Aufgabe**

Sie können diese Optionen für jede Storage Virtual Machine (SVM) einzeln anpassen.

Ab ONTAP 9 sind die Optionen `v3-tcp-max-read-size` und `v3-tcp-max-write-size` veraltet. Stattdessen ist die Option `-tcp-max-xfer-size` zu verwenden.

**Schritte**

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

| Wenn Sie möchten… | Geben Sie den Befehl ein… |
|---|---|
| Die maximale Übertragungsgröße für NFSv3 oder NFSv4 TCP ändern | `vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size` |

| Option | Bereich | Standard |
|---|---|---|
| `-tcp-max-xfer-size` | 8192 bis 1048576 Bytes | 65536 Bytes |



Die maximal einzugebende Übertragungsgröße muss ein Vielfaches von 4 KB (4096 Byte) sein. Nicht korrekt ausgerichtete Anfragen beeinträchtigen die Leistung.

3. Mit dem `vserver nfs show -fields tcp-max-xfer-size` Befehl lassen sich die Änderungen überprüfen.
4. Falls Clients statische Mounts verwenden, müssen diese ausgehängt und anschließend erneut eingehängt werden, damit die neue Parametergröße wirksam wird.

**Beispiel**

Der folgende Befehl legt die maximale TCP-Übertragungsgröße für NFSv3 und NFSv4.x auf 1048576 Bytes auf der SVM mit dem Namen vs1 fest:

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

# Die Anzahl der für NFS-Benutzer auf ONTAP SVMs zulässigen Gruppen-IDs konfigurieren

Standardmäßig unterstützt ONTAP bis zu 32 Gruppen-IDs bei der Verarbeitung von NFS-Benutzeranmeldeinformationen mit Kerberos (RPCSEC_GSS) Authentifizierung. Bei Verwendung der AUTH_SYS Authentifizierung beträgt die maximale Anzahl an Gruppen-IDs standardmäßig 16, wie in RFC 5531 definiert. Die maximale Anzahl kann auf bis zu 1.024 erhöht werden, wenn Benutzer Mitglied in mehr als der standardmäßigen Anzahl an Gruppen sind.

**Über diese Aufgabe**

Wenn ein Benutzer mehr als die standardmäßige Anzahl an Gruppen-IDs in seinen Anmeldeinformationen besitzt, werden die verbleibenden Gruppen-IDs abgeschnitten und der Benutzer kann beim Zugriff auf Dateien im Speichersystem Fehler erhalten. Die maximale Anzahl an Gruppen pro SVM sollte auf eine Zahl festgelegt werden, die die maximale Anzahl an Gruppen in Ihrer Umgebung widerspiegelt.



Um die Voraussetzungen für die AUTH_SYS Authentifizierung zur Aktivierung erweiterter

> Gruppen (`-auth-sys-extended-groups` zu verstehen, die Gruppen-IDs über das standardmäßige Maximum von 16 hinaus verwenden, siehe die "NetApp Knowledge Base: Welche Voraussetzungen müssen für die Aktivierung von auth-sys-extended-groups erfüllt sein?"

Die folgende Tabelle zeigt die beiden Parameter des `vserver nfs modify` Befehls, die die maximale Anzahl von Gruppen-IDs in drei Beispielkonfigurationen bestimmen:

| Parameter | Einstellungen | Beschränkung der resultierenden Gruppen-IDs |
|---|---|---|
| `-extended-groups-limit`<br><br>`-auth-sys-extended-groups` | `32`<br><br>`disabled`<br><br>Dies sind die Standardeinstellungen. | RPCSEC_GSS: 32<br><br>AUTH_SYS: 16 |
| `-extended-groups-limit`<br><br>`-auth-sys-extended-groups` | `256`<br><br>`disabled` | RPCSEC_GSS: 256<br><br>AUTH_SYS: 16 |
| `-extended-groups-limit`<br><br>`-auth-sys-extended-groups` | `512`<br><br>`enabled` | RPCSEC_GSS: 512<br><br>AUTH_SYS: 512 |

**Schritte**

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Die gewünschte Aktion ausführen:

| Wenn Sie die maximale Anzahl zulässiger Hilfsgruppen festlegen möchten… | Geben Sie den Befehl ein… |
|---|---|
| Nur für RPCSEC_GSS und AUTH_SYS auf dem Standardwert 16 belassen | `vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled` |
| Sowohl für RPCSEC_GSS als auch für AUTH_SYS | `vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled` |

3. Den `-extended-groups-limit`Wert überprüfen und feststellen, ob AUTH_SYS erweiterte Gruppen verwendet: `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`
4. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

**Beispiel**

Das folgende Beispiel aktiviert erweiterte Gruppen für die AUTH_SYS Authentifizierung und legt die maximale Anzahl erweiterter Gruppen sowohl für die AUTH_SYS als auch für die RPCSEC_GSS Authentifizierung auf 512 fest. Diese Änderungen gelten nur für Clients, 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
```

**Verwandte Informationen**

- "NetApp Knowledge Base: Änderungen an den erweiterten AUTH_SYS-Gruppen für die NFS Authentifizierung für ONTAP 9"

# Root-Benutzerzugriff auf NTFS-Sicherheitsdaten im Sicherheitsstil für ONTAP SVMs steuern

ONTAP kann so konfiguriert werden, dass NFS-Clients auf Daten im NTFS-Sicherheitsstil zugreifen können und NTFS-Clients auf Daten im NFS-Sicherheitsstil zugreifen können. Bei Verwendung des NTFS-Sicherheitsstils auf einem NFS Datastore ist festzulegen, wie der Zugriff durch den Root-Benutzer behandelt wird, und die Storage Virtual Machine (SVM) entsprechend zu konfigurieren.

**Über diese Aufgabe**

Wenn ein Root-Benutzer auf NTFS Security-Style-Daten zugreift, bestehen zwei Optionen:

- Der Root-Benutzer wird wie jeder andere NFS-Benutzer einem Windows-Benutzer zugeordnet, und der Zugriff erfolgt gemäß den NTFS-ACLs.
- NTFS-ACLs ignorieren und vollen Zugriff für den Root-Benutzer bereitstellen.

**Schritte**

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Die gewünschte Aktion ausführen:

| Wenn der Root-Benutzer… | Geben Sie den Befehl ein… |
| --- | --- |
| Einem Windows-Benutzer zugeordnet sein | `vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled` |
| Die NT-ACL-Prüfung umgehen | `vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled` |

Dieser Parameter ist standardmäßig deaktiviert.

Wenn dieser Parameter aktiviert ist, aber keine Namenszuordnung für den Root-Benutzer vorhanden ist, verwendet ONTAP für die Überwachung standardmäßig die SMB-Administratoranmeldeinformationen.

3. Zurück zur Administrator-Privilegstufe:

```
set -privilege admin
```

**Copyright-Informationen**

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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, BEISPIELHAFTE 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 IRGENDEINER 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.