Speicherkapazität zu einer NFS-fähigen SVM hinzufügen

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/nfs-config/add-storage-capacity-nfs-enabled-svm-concept.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

Speicherkapazität zu einer NFS-fähigen SVM hinzufügen . . . 1
- Informationen zum Hinzufügen von Speicherkapazität zu einer ONTAP NFS-fähigen SVM . . . 1
- Erstellen einer ONTAP NFS-Exportrichtlinie . . . 1
- Eine Regel zu einer ONTAP NFS-Exportregel hinzufügen . . . 2
- Volume- oder Qtree-Speichercontainer erstellen . . . 7
  - Ein ONTAP NFS-Volume erstellen . . . 7
  - Einen ONTAP NFS Qtree erstellen . . . 9
- NFS-Zugriff mithilfe von Exportrichtlinien absichern . . . 10
  - Informationen zur Sicherung des ONTAP NFS-Zugriffs mithilfe von Exportrichtlinien . . . 10
  - Verwalten der Verarbeitungsreihenfolge von ONTAP NFS Exportregeln . . . 10
  - Einer Volume wird eine ONTAP NFS-Exportregel zugewiesen. . . . 11
  - Einer Qtree eine ONTAP NFS-Exportregel zuweisen . . . 11
- ONTAP NFS-Client-Zugriff vom Cluster aus überprüfen . . . 12
- ONTAP NFS-Zugriff von Clientsystemen testen . . . 13

Speicherkapazität zu einer NFS-fähigen SVM hinzufügen

Informationen zum Hinzufügen von Speicherkapazität zu einer ONTAP NFS-fähigen SVM

Um die Speicherkapazität einer NFS-fähigen SVM zu erweitern, muss ein Volume oder ein Qtree als Speichercontainer erstellt und eine Exportregel für diesen Container erstellt oder geändert werden. Anschließend lässt sich der NFS-Client-Zugriff vom Cluster aus überprüfen und der Zugriff von Clientsystemen testen.

Bevor Sie beginnen

- NFS muss auf der SVM vollständig eingerichtet sein.
- Die Standardexportrichtlinie des SVM-Root-Volumes muss eine Regel enthalten, die den Zugriff für alle Clients erlaubt.
- Alle Aktualisierungen Ihrer Namensdienstkonfiguration müssen vollständig abgeschlossen sein.
- Jegliche Ergänzungen oder Änderungen an einer Kerberos-Konfiguration müssen vollständig sein.

Erstellen einer ONTAP NFS-Exportrichtlinie

Bevor Exportregeln erstellt werden, ist eine Exportrichtlinie zu erstellen, die diese enthält. Mit dem `vserver export-policy create` Befehl kann eine Exportrichtlinie erstellt werden.

Schritte

1. Eine Exportrichtlinie erstellen:

   `vserver export-policy create -vserver` *`vserver_name`* `-policyname` *`policy_name`*

   Der Name der Richtlinie kann bis zu 256 Zeichen lang sein.

2. Es wird überprüft, ob die Exportrichtlinie erstellt wurde:

   `vserver export-policy show -policyname` *`policy_name`*

Beispiel

Die folgenden Befehle erstellen und überprüfen die Erstellung einer Exportrichtlinie mit dem Namen exp1 auf der SVM mit dem Namen vs1:

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
---------------  -------------------
vs1              exp1
```

Eine Regel zu einer ONTAP NFS-Exportregel hinzufügen

Ohne Regeln kann die Exportregel Clients keinen Datenzugriff gewähren. Zum Erstellen einer neuen Exportregel müssen Clients identifiziert und ein Client-Match-Format ausgewählt werden, die Zugriffs- und Sicherheitstypen festgelegt, eine Zuordnung anonymer Benutzer-IDs angegeben, eine Regelindexnummer ausgewählt und das Zugriffsprotokoll festgelegt werden. Anschließend kann der `vserver export-policy rule create` Befehl verwendet werden, um die neue Regel einer Exportregel hinzuzufügen.

Bevor Sie beginnen

- Die Export-Richtlinie, zu der die Exportregeln hinzugefügt werden sollen, muss bereits existieren.
- DNS muss auf der Daten-SVM korrekt konfiguriert sein und die DNS-Server müssen korrekte Einträge für NFS-Clients enthalten.

  Dies liegt daran, dass ONTAP DNS-Abfragen unter Verwendung der DNS-Konfiguration der Daten-SVM für bestimmte Client-Match-Formate durchführt, und Fehler beim Abgleich der Exportregel den Dateizugriff durch Clients verhindern können.

- Wenn Sie die Authentifizierung mit Kerberos verwenden, muss ermittelt sein, welche der folgenden Sicherheitsmethoden auf Ihren NFS-Clients verwendet wird:
  - `krb5` (Kerberos V5-Protokoll)
  - `krb5i` (Kerberos V5-Protokoll mit Integritätsprüfung mittels Prüfsummen)
  - `krb5p` (Kerberos V5-Protokoll mit Datenschutzdienst)

Über diese Aufgabe

Es ist nicht notwendig, eine neue Regel zu erstellen, wenn eine bestehende Regel in einer Exportregel Ihre Anforderungen an Client-Abgleich und Zugriff abdeckt.

Wenn Sie sich mit Kerberos authentifizieren und auf alle Volumes der SVM über Kerberos zugegriffen wird, können die Exportregeloptionen `-rorule`, `-rwrule` und `-superuser` für das Root-Volume auf `krb5`, `krb5i` oder `krb5p` gesetzt werden.

Schritte

1. Die Clients und das Client-Match-Format für die neue Regel werden identifiziert.

   Die `-clientmatch` Option legt die Clients fest, für die die Regel gilt. Einzelne oder mehrere Übereinstimmungswerte für Clients können angegeben werden; mehrere Werte müssen durch Kommas getrennt werden. Die Übereinstimmung kann in einem der folgenden Formate angegeben werden:

Client Match Format	Beispiel
Domainname, dem das Zeichen „.“ vorangestellt ist	`.example.com` oder `.example.com,.example.net,...`
Hostname	`host1` oder `host1,host2, ...`
IPv4-Adresse	`10.1.12.24` oder `10.1.12.24,10.1.12.25, ...`

Client Match Format	Beispiel
IPv4-Adresse mit einer als Bitanzahl ausgedrückten Subnetzmaske	`10.1.12.10/4` oder `10.1.12.10/4,10.1.12.11/4,...`
IPv4-Adresse mit Netzwerkmaske	`10.1.16.0/255.255.255.0` oder `10.1.16.0/255.255.255.0,10.1.17.0/255.255.255.0,...`
IPv6-Adresse im Punktformat	`::1.2.3.4` oder `::1.2.3.4,::1.2.3.5,...`
IPv6-Adresse mit einer als Bitanzahl ausgedrückten Subnetzmaske	`ff::00/32` oder `ff::00/32,ff::01/32,...`
Eine einzelne Netzgruppe mit dem Netzgruppennamen, dem das @-Zeichen vorangestellt ist	`@netgroup1` oder `@netgroup1,@netgroup2,...`

Sie können auch verschiedene Arten von Clientdefinitionen kombinieren, zum Beispiel `.example.com,@netgroup1`.

Bei der Angabe von IP-Adressen ist Folgendes zu beachten:

- Die Eingabe eines IP-Adressbereichs, wie 10.1.12.10-10.1.12.70, ist nicht zulässig.

  Einträge in diesem Format werden als Text-String interpretiert und als Hostname behandelt.

- Bei der Angabe einzelner IP-Adressen in Exportregeln zur detaillierten Verwaltung des Clientzugriffs dürfen keine IP-Adressen angegeben werden, die dynamisch (zum Beispiel DHCP) oder temporär (zum Beispiel IPv6) zugewiesen werden.

  Andernfalls verliert der Client den Zugriff, wenn sich seine IP-Adresse ändert.

- Die Eingabe einer IPv6-Adresse mit einer Netzwerkmaske, wie z. B. ff::12/ff::00, ist nicht zulässig.

2. Wählen Sie die Zugriffs- und Sicherheitstypen für Clientübereinstimmungen aus.

   Sie können einen oder mehrere der folgenden Zugriffsmodi für Clients festlegen, die sich mit den angegebenen Sicherheitstypen authentifizieren:

   - `-rorule` (Nur-Lesezugriff)
   - `-rwrule` (Lese- und Schreibzugriff)
   - `-superuser` (Root-Zugriff)

   > Ein Client erhält nur dann Lese- und Schreibzugriff auf einen bestimmten Sicherheitstyp, wenn die Exportregel auch Lesezugriff für diesen Sicherheitstyp zulässt. Ist der Parameter für Lesezugriff restriktiver als der Parameter für Lese- und Schreibzugriff, erhält der Client möglicherweise keinen Lese- und Schreibzugriff. Dasselbe gilt für Superuser-Zugriff.

   Sie können für eine Regel eine durch Kommas getrennte Liste mehrerer Sicherheitstypen angeben. Wenn der Sicherheitstyp als `any` oder `never` angegeben wird, dürfen keine weiteren Sicherheitstypen angegeben werden. Folgende gültige Sicherheitstypen stehen zur Auswahl:

Wenn der Sicherheitstyp auf … eingestellt ist	Ein passender Client kann auf die exportierten Daten zugreifen…
`any`	Immer, unabhängig vom eingehenden Sicherheitstyp.
`none`	Wenn allein aufgeführt, erhalten Clients mit jedem Sicherheitstyp Zugriff als anonym. Wenn zusammen mit anderen Sicherheitstypen aufgeführt, erhalten Clients mit einem angegebenen Sicherheitstyp Zugriff, und Clients mit jedem anderen Sicherheitstyp erhalten Zugriff als anonym.
`never`	Niemals, unabhängig vom eingehenden Sicherheitstyp.
`krb5`	Wenn die Authentifizierung durch Kerberos 5 erfolgt. Nur Authentifizierung: Der Header jeder Anfrage und Antwort wird signiert.
`krb5i`	Wenn die Authentifizierung über Kerberos 5i erfolgt. Authentifizierung und Integrität: Der Header und der Body jeder Anfrage und Antwort werden signiert.
`krb5p`	Wenn die Authentifizierung über Kerberos 5p erfolgt. Authentifizierung, Integrität und Datenschutz: Der Header und der Body jeder Anfrage und Antwort werden signiert, und die NFS-Nutzlast wird verschlüsselt.
`ntlm`	Wenn sie durch CIFS NTLM authentifiziert wird.
`sys`	Wenn es durch NFS AUTH_SYS authentifiziert wird.

Der empfohlene Sicherheitstyp ist `sys`, oder falls Kerberos verwendet wird, `krb5`, `krb5i`, oder `krb5p`.

Wenn Kerberos mit NFSv3 verwendet wird, muss die Exportregel `-rorule` und `-rwrule` Zugriff auf `sys` zusätzlich zu `krb5` erlauben. Dies ist erforderlich, da der Network Lock Manager (NLM) Zugriff auf den Export benötigt.

3. Eine Zuordnung für anonyme Benutzer-IDs angeben.

   Die `-anon` Option gibt eine UNIX-Benutzer-ID oder einen Benutzernamen an, der Clientanfragen zugeordnet wird, die mit einer Benutzer-ID von 0 (Null) eingehen, was typischerweise mit dem Benutzernamen root verbunden ist. Der Standardwert ist `65534`. NFS-Clients ordnen die Benutzer-ID 65534 üblicherweise dem Benutzernamen nobody zu (auch bekannt als *root squashing*). In ONTAP ist diese Benutzer-ID dem Benutzer pcuser zugeordnet. Um den Zugriff durch beliebige Clients mit einer Benutzer-ID von 0 zu deaktivieren, ist ein Wert von `65535` anzugeben.

4. Wählen Sie die Reihenfolge des Regelindex aus.

   Die `-ruleindex` Option gibt die Indexnummer der Regel an. Regeln werden entsprechend ihrer Reihenfolge in der Liste der Indexnummern ausgewertet; Regeln mit niedrigeren Indexnummern werden zuerst ausgewertet. Zum Beispiel wird die Regel mit der Indexnummer 1 vor der Regel mit der Indexnummer 2 ausgewertet.

Wenn Sie hinzufügen…	Dann…
Die erste Regel einer Exportregel	Drücken Sie `1`.
Zusätzliche Regeln für eine Exportrichtlinie	a. Vorhandene Regeln in der Richtlinie anzeigen: `vserver export-policy rule show -instance -policyname your_policy` b. Wählen Sie für die neue Regel eine Indexnummer entsprechend der Reihenfolge aus, in der sie ausgewertet werden soll.

5. Wählen Sie den entsprechenden NFS-Zugriffswert aus: {`nfs`|`nfs3`|`nfs4`}.

   `nfs` passt zu jeder Version, `nfs3` und `nfs4` passt nur zu diesen spezifischen Versionen.

6. Die Exportregel wird erstellt und einer bestehenden Export-Richtlinie hinzugefügt:

   ```
   vserver export-policy rule create -vserver vserver_name -policyname
   policy_name -ruleindex integer -protocol {nfs|nfs3|nfs4} -clientmatch { text |
   "text,text,…" } -rorule security_type -rwrule security_type -superuser
   security_type -anon user_ID
   ```

7. Die Regeln der Exportrichtlinie anzeigen, um zu überprüfen, ob die neue Regel vorhanden ist:

   ```
   vserver export-policy rule show -policyname policy_name
   ```

   Der Befehl zeigt eine Zusammenfassung der Exportregel an, einschließlich einer Liste der auf diese Regel angewendeten Regeln. ONTAP weist jeder Regel eine Regelindexnummer zu. Nachdem die Regelindexnummer bekannt ist, lässt sich damit eine detaillierte Anzeige der angegebenen Exportregel aufrufen.

8. Es sollte überprüft werden, ob die auf die Exportrichtlinie angewandten Regeln korrekt konfiguriert sind:

   ```
   vserver export-policy rule show -policyname policy_name -vserver vserver_name
   -ruleindex integer
   ```

Beispiele

Die folgenden Befehle erstellen und überprüfen die Erstellung einer Exportregel auf der SVM mit dem Namen vs1 in einer Exportregel mit dem Namen rs1. Die Regel hat die Indexnummer 1. Die Regel gilt für alle Clients in der Domäne eng.company.com und die Netgroup @netgroup1. Die Regel ermöglicht den gesamten NFS-Zugriff. Sie ermöglicht Lese- und Schreibzugriff für Benutzer, die sich mit AUTH_SYS authentifiziert haben. Clients mit der UNIX-Benutzer-ID 0 (null) werden anonymisiert, sofern sie nicht mit Kerberos authentifiziert sind.

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname exp1
-ruleindex 1 -protocol nfs
-clientmatch .eng.company.com,@netgoup1 -rorule sys -rwrule sys -anon
65534 -superuser krb5

vs1::> vserver export-policy rule show -policyname nfs_policy
Virtual      Policy         Rule    Access    Client           RO
```

```
Server       Name           Index   Protocol  Match            Rule
------------ -------------- ------  --------  ---------------- ------
vs1          exp1           1       nfs       eng.company.com, sys
                                              @netgroup1

vs1::> vserver export-policy rule show -policyname exp1 -vserver vs1
-ruleindex 1

                                    Vserver: vs1
                                Policy Name: exp1
                                 Rule Index: 1
                            Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
                             RO Access Rule: sys
                             RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
                   Superuser Security Types: krb5
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

Die folgenden Befehle erstellen und überprüfen die Erstellung einer Exportregel auf der SVM mit dem Namen vs2 in einer Exportregel mit dem Namen expol2. Die Regel hat die Indexnummer 21. Die Regel ordnet Clients den Mitgliedern der Netgroup dev_netgroup_main zu. Die Regel ermöglicht den gesamten NFS-Zugriff. Sie ermöglicht schreibgeschützten Zugriff für Benutzer, die sich mit AUTH_SYS authentifiziert haben, und erfordert Kerberos-Authentifizierung für Lese-/Schreib- und Root-Zugriff. Clients mit der UNIX-Benutzer-ID 0 (null) wird Root-Zugriff verweigert, sofern sie sich nicht mit Kerberos authentifiziert haben.

```
vs2::> vserver export-policy rule create -vserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5

vs2::> vserver export-policy rule show -policyname nfs_policy
Virtual  Policy       Rule    Access    Client              RO
Server   Name         Index   Protocol  Match               Rule
-------- ------------ ------  --------  ------------------  ------
vs2      expol2       21       nfs      @dev_netgroup_main  sys

vs2::> vserver export-policy rule show -policyname expol2 -vserver vs1
-ruleindex 21

                                    Vserver: vs2
                                Policy Name: expol2
                                 Rule Index: 21
                            Access Protocol: nfs
```

```
Client Match Hostname, IP Address, Netgroup, or Domain:
                                            @dev_netgroup_main
                             RO Access Rule: sys
                             RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
                   Superuser Security Types: krb5
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

Volume- oder Qtree-Speichercontainer erstellen

Ein ONTAP NFS-Volume erstellen

Ein Volume kann erstellt und dessen Verbindungspunkt sowie weitere Eigenschaften mit dem `volume create` Befehl angegeben werden.

Über diese Aufgabe

Ein Volume muss einen Verbindungspfad enthalten, damit seine Daten für Clients verfügbar sind. Der Verbindungspfad kann beim Erstellen eines neuen Volumes angegeben werden. Wird ein Volume ohne Angabe eines Verbindungspfads erstellt, muss das Volume im SVM-Namespace mit dem `volume mount` Befehl eingebunden werden.

Bevor Sie beginnen

- NFS sollte eingerichtet sein und ausgeführt werden.
- Der SVM-Sicherheitsstil muss UNIX sein.
- Ab ONTAP 9.13.1 ist es möglich, Volumes mit aktivierter Kapazitätsanalyse und Aktivitätsverfolgung zu erstellen. Zum Aktivieren der Kapazitäts- oder Aktivitätsverfolgung wird der `volume create` Befehl mit `-analytics-state` oder `-activity-tracking-state` auf `on` ausgeführt.

  Weitere Informationen zu Kapazitätsanalysen und Aktivitätsverfolgung finden sich unter "Dateisystemanalyse aktivieren". Weitere Informationen zu `volume create` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Das Volume mit einer Verbindung erstellen:

   `volume create -vserver` *`svm_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {`*`integer`*`[KB|MB|GB|TB|PB]} -security-style unix -user` *`user_name_or_number`* `-group` *`group_name_or_number`* `-junction-path` *`junction_path`* `[-policy` *`export_policy_name`*`]`

   Die Auswahlmöglichkeiten für `-junction-path`sind die folgenden:

   - Direkt unter dem Stammverzeichnis, zum Beispiel */`new_vol`*

     Sie können ein neues Volume erstellen und angeben, dass es direkt im SVM Root-Volume eingebunden wird.

   - Unter einem bestehenden Verzeichnis, zum Beispiel */`existing_dir/new_vol`*

Sie können ein neues Volume erstellen und angeben, dass es in ein vorhandenes Volume (in einer vorhandenen Hierarchie) als Verzeichnis eingebunden wird.

Wenn ein Volume in einem neuen Verzeichnis (in einer neuen Hierarchie unter einem neuen Volume) erstellt werden soll, zum Beispiel */new_dir/new_vol*, muss zunächst ein neues übergeordnetes Volume erstellt werden, das mit dem SVM-Root-Volume verbunden ist. Das neue untergeordnete Volume würde dann im Verbindungspfad des neuen übergeordneten Volumes (neues Verzeichnis) erstellt.

Wenn Sie eine bestehende Exportregel verwenden möchten, kann diese beim Erstellen des Volumes angegeben werden. Eine Exportregel kann auch später mit dem `volume modify` Befehl hinzugefügt werden.

2. Es sollte überprüft werden, ob das Volume mit dem gewünschten Verbindungspunkt erstellt wurde:

   `volume show -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction`

Beispiele

Der folgende Befehl erstellt ein neues Volume namens users1 auf der SVM vs1.example.com und dem Aggregat aggr1. Das neue Volume ist unter `/users` verfügbar. Das Volume ist 750 GB groß und seine Volume-Garantie ist standardmäßig vom Typ Volume.

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver           Volume  Active   Junction Path   Path Source
----------------- ------- -------- --------------- -----------
vs1.example.com   users1  true     /users          RW_volume
```

Der folgende Befehl erstellt ein neues Volume namens „home4“ auf der SVM „vs1.example.com“ und dem Aggregat „aggr1“. Das Verzeichnis `/eng/` existiert bereits im Namespace der SVM vs1, und das neue Volume wird unter `/eng/home` bereitgestellt, das zum Home-Verzeichnis für den `/eng/` Namespace wird. Das Volume ist 750 GB groß und seine Volume-Garantie ist standardmäßig vom Typ `volume`.

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                          Junction                 Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4   true     /eng/home       RW_volume
```

Einen ONTAP NFS Qtree erstellen

Sie können einen Qtree erstellen, um Ihre Daten zu speichern, und seine Eigenschaften mithilfe des `volume qtree create` Befehls angeben.

Bevor Sie beginnen

- Die SVM und das Volume, das den neuen Qtree enthalten soll, müssen bereits existieren.
- Der SVM-Sicherheitsstil muss UNIX sein, und NFS muss eingerichtet und funktionsfähig sein.

Schritte

1. Den Qtree erstellen:

   `volume qtree create -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `} -security-style unix [-policy` *`export_policy_name`*`]`

   Sie können das Volume und den Qtree als separate Argumente angeben oder das Qtree-Pfadargument im Format `/vol/`*`volume_name/_qtree_name`* angeben.

   Standardmäßig übernehmen Qtrees die Exportregeln ihres übergeordneten Volumes, können aber auch so konfiguriert werden, dass sie eigene verwenden. Wenn eine vorhandene Exportregel verwendet werden soll, kann diese beim Erstellen des Qtrees angegeben werden. Eine Exportregel kann auch später mit dem `volume qtree modify` Befehl hinzugefügt werden.

2. Es sollte überprüft werden, ob der Qtree mit dem gewünschten Verbindungspfad erstellt wurde:

   `volume qtree show -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `}`

Beispiel

Das folgende Beispiel erstellt einen Qtree namens qt01 auf SVM vs1.example.com, der einen Verbindungspfad `/vol/data1` hat:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style unix
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                    Vserver Name: vs1.example.com
                     Volume Name: data1
                      Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                  Security Style: unix
                     Oplock Mode: enable
                Unix Permissions: ---rwxr-xr-x
                         Qtree Id: 2
                    Qtree Status: normal
```

```
                    Export Policy: default
        Is Export Policy Inherited: true
```

NFS-Zugriff mithilfe von Exportrichtlinien absichern

Informationen zur Sicherung des ONTAP NFS-Zugriffs mithilfe von Exportrichtlinien

Sie können Exportrichtlinien verwenden, um den NFS-Zugriff auf Volumes oder Qtrees auf Clients zu beschränken, die bestimmten Parametern entsprechen. Beim Bereitstellen neuen Speichers ist es möglich, eine vorhandene Richtlinie und Regeln zu verwenden, einer vorhandenen Richtlinie Regeln hinzuzufügen oder eine neue Richtlinie und Regeln zu erstellen. Auch die Konfiguration der Exportrichtlinien kann überprüft werden.

> ⓘ Ab ONTAP 9.3 kann die Überprüfung der Exportrichtlinienkonfiguration als Hintergrundprozess aktiviert werden, der alle Regelverstöße in einer Fehlerregelliste protokolliert. Die `vserver export-policy config-checker` Befehle rufen die Überprüfung auf und zeigen die Ergebnisse an, die zur Überprüfung der Konfiguration und zum Löschen fehlerhafter Regeln aus der Richtlinie verwendet werden können. Die Befehle validieren die Exportkonfiguration nur für Hostnamen, Netzgruppen und anonyme Benutzer.

Verwalten der Verarbeitungsreihenfolge von ONTAP NFS Exportregeln

Mit dem `vserver export-policy rule setindex` Befehl lässt sich die Indexnummer einer bestehenden Exportregel manuell festlegen. Dies ermöglicht die Angabe der Reihenfolge, in der ONTAP Exportregeln auf Clientanfragen anwendet.

Über diese Aufgabe

Falls die neue Indexnummer bereits verwendet wird, fügt der Befehl die Regel an der angegebenen Stelle ein und ordnet die Liste entsprechend neu.

Schritt

1. Die Indexnummer einer bestimmten Exportregel ändern:

   ```
   vserver export-policy rule setindex -vserver virtual_server_name -policyname
   policy_name -ruleindex integer -newruleindex integer
   ```

Beispiel

Der folgende Befehl ändert die Indexnummer einer Exportregel mit der Indexnummer 3 auf die Indexnummer 2 in einer Exportregel namens rs1 auf der SVM namens vs1:

```
vs1::> vserver export-policy rule setindex -vserver vs1
-policyname rs1 -ruleindex 3 -newruleindex 2
```

Einer Volume wird eine ONTAP NFS-Exportregel zugewiesen.

Jedes im SVM enthaltene Volume muss mit einer Exportrichtlinie verknüpft sein, die Exportregeln für Clients enthält, damit auf Daten im Volume zugegriffen werden kann.

Über diese Aufgabe

Sie können einer Volume beim Erstellen oder jederzeit danach eine Exportregel zuweisen. Sie können einer Volume nur eine Exportregel zuweisen, wobei eine Exportregel mehreren Volumes zugeordnet werden kann.

Schritte

1. Wurde beim Erstellen des Volumes keine Exportregel angegeben, ist dem Volume eine Exportregel zuzuweisen:

   ```
   volume modify -vserver vserver_name -volume volume_name -policy
   export_policy_name
   ```

2. Es wird überprüft, ob die Richtlinie dem Volume zugewiesen wurde:

   ```
   volume show -volume volume_name -fields policy
   ```

Beispiel

Die folgenden Befehle weisen dem Volume vol1 auf der SVM vs1 die Exportregel nfs_policy zu und überprüfen die Zuweisung:

```
cluster::> volume modify -v1server vs1 -volume vol1 -policy nfs_policy

cluster::>volume show -volume vol -fields policy
vserver volume       policy
------- ------------ ----------------
vs1     vol1         nfs_policy
```

Einer Qtree eine ONTAP NFS-Exportregel zuweisen

Anstatt ein gesamtes Volume zu exportieren, kann auch ein bestimmter qtree auf einem Volume exportiert werden, um ihn Clients direkt zugänglich zu machen. Ein qtree kann exportiert werden, indem ihm eine Exportregel zugewiesen wird. Die Exportregel kann entweder beim Erstellen eines neuen qtrees oder durch Ändern eines bestehenden qtrees zugewiesen werden.

Bevor Sie beginnen

Die Exportrichtlinie muss vorhanden sein.

Über diese Aufgabe

Standardmäßig erben Qtrees die übergeordnete Exportregel des enthaltenden Volumes, sofern bei der Erstellung nichts anderes angegeben wurde.

Sie können einer qtree beim Erstellen oder jederzeit nach dem Erstellen eine Exportregel zuordnen. Einer qtree kann nur eine Exportregel zugeordnet werden, wobei eine Regel mit vielen qtrees verknüpft sein kann.

Schritte

1. Wurde beim Erstellen des Qtree keine Exportregel angegeben, kann dem Qtree eine Exportregel zugewiesen werden:

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

2. Es wird überprüft, ob die Richtlinie dem Qtree zugewiesen wurde:

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

Beispiel

Die folgenden Befehle weisen dem Qtree qt1 auf der SVM vs1 die Exportregel nfs_policy zu und überprüfen die Zuweisung:

```
cluster::> volume modify -v1server vs1 -qtree-path /vol/vol1/qt1 -policy
nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy
------- ------ ----- -------------
vs1     data1  qt01  nfs_policy
```

ONTAP NFS-Client-Zugriff vom Cluster aus überprüfen

Sie können ausgewählten Clients Zugriff auf die Freigabe gewähren, indem Sie die UNIX-Dateiberechtigungen auf einem UNIX-Administrationsrechner festlegen. Der Clientzugriff kann mit dem `vserver export-policy check-access` Befehl überprüft und die Exportregeln bei Bedarf angepasst werden.

Schritte

1. Auf dem Cluster lässt sich der Clientzugriff auf Exporte mit dem `vserver export-policy check-access` Befehl überprüfen.

   Der folgende Befehl prüft den lesen/schreiben-Zugriff für einen NFSv3-Client mit der IP-Adresse 1.2.3.4 auf das Volume home2. Die Befehlsausgabe zeigt, dass das Volume die Exportregel `exp-home-dir` verwendet und der Zugriff verweigert wird.

   ```
   cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
   1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
   -type read-write
                                       Policy    Policy     Rule
   Path                    Policy      Owner     Owner Type Index  Access
   ----------------------- ----------- --------- ---------- ------
   ----------
   /                       default     vs1_root  volume          1 read
   /eng                    default     vs1_root  volume          1 read
   ```

```
/eng/home2              exp-home-dir  home2     volume          1 denied

3 entries were displayed.
```

2. Die Ausgabe kann daraufhin überprüft werden, ob die Exportregel wie vorgesehen funktioniert und der Clientzugriff wie erwartet erfolgt.

   Insbesondere ist zu überprüfen, welche Exportregel vom Volume oder Qtree verwendet wird und welche Art von Zugriff der Client dadurch erhält.

3. Gegebenenfalls sind die Exportregel-Definitionen neu zu konfigurieren.

ONTAP NFS-Zugriff von Clientsystemen testen

Nachdem der NFS-Zugriff auf das neue Speicherobjekt überprüft wurde, empfiehlt es sich, die Konfiguration zu testen, indem Sie sich an einem NFS-Administrationshost anmelden und Daten vom SVM lesen sowie Daten auf das SVM schreiben. Anschließend empfiehlt es sich, den Vorgang als Nicht-Root-Benutzer auf einem Client-System zu wiederholen.

Bevor Sie beginnen

- Das Clientsystem muss über eine IP-Adresse verfügen, die von der zuvor angegebenen Exportregel erlaubt ist.
- Sie benötigen die Anmeldeinformationen für den Root-Benutzer.

Schritte

1. Im Cluster lässt sich die IP-Adresse des LIF überprüfen, das das neue Volume hostet:

   `network interface show –vserver` *`svm_name`*

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

2. Als Root-Benutzer am Administrationshost-Clientsystem anmelden.
3. Das Verzeichnis wird in den Mount-Ordner geändert:

   `cd /mnt/`

4. Einen neuen Ordner unter Verwendung der IP-Adresse der SVM erstellen und einbinden:

   a. Einen neuen Ordner erstellen:
   `mkdir /mnt/`*`folder`*

   b. Das neue Volume in diesem neuen Verzeichnis einbinden:
   `mount -t nfs -o hard` *`IPAddress`*`:/`*`volume_name`* `/mnt/`*`folder`*

   c. Das Verzeichnis in den neuen Ordner ändern:
   `cd` *`folder`*

   Die folgenden Befehle erstellen einen Ordner namens test1, mounten das Volume vol1 an der IP-Adresse 192.0.2.130 im Mount-Ordner test1 und wechseln in das neue Verzeichnis test1:

```
host# mkdir /mnt/test1
host# mount -t nfs -o hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

5. Eine neue Datei wird erstellt, das Vorhandensein überprüft und Text hineingeschrieben:
   a. Eine Testdatei erstellen:
   `touch filename`
   b. Es wird überprüft, ob die Datei existiert. `ls -l filename`
   c. Eingabe:
   `cat > filename`

      Geben Sie einen Text ein und anschließend Strg+D, um den Text in die Testdatei zu schreiben.

   d. Den Inhalt der Testdatei anzeigen.
   `cat filename`
   e. Die Testdatei entfernen:
   `rm filename`
   f. Zurück zum übergeordneten Verzeichnis:
   `cd ..`

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

6. Als Root-Benutzer die gewünschten UNIX-Besitzrechte und Berechtigungen für das gemountete Volume festlegen.
7. Auf einem in Ihren Exportregeln angegebenen UNIX-Clientsystem als einer der autorisierten Benutzer mit Zugriff auf das neue Volume anmelden und die Schritte 3 bis 5 wiederholen, um zu überprüfen, ob das Volume gemountet und eine Datei erstellt werden kann.

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.