Storage-Kapazität zu einer NFS-fähigen SVM hinzufügen

ONTAP 9

NetApp
June 19, 2024

Inhalt

Storage-Kapazität zu einer NFS-fähigen SVM hinzufügen . . . 1
Fügen Sie einer SVM - Übersicht über NFS-fähige Storage-Kapazität hinzu . . . 1
Erstellen Sie eine Exportrichtlinie . . . 1
Fügen Sie eine Regel zu einer Exportrichtlinie hinzu . . . 2
Erstellung eines Volume oder qtree Storage-Containers . . . 7
Sicherer NFS-Zugriff über Exportrichtlinien . . . 10
Überprüfen Sie den NFS-Client-Zugriff vom Cluster aus . . . 13
Testen Sie den NFS-Zugriff von Client-Systemen . . . 14

Storage-Kapazität zu einer NFS-fähigen SVM hinzufügen

Fügen Sie einer SVM - Übersicht über NFS-fähige Storage-Kapazität hinzu

Um einer NFS-fähigen SVM Storage-Kapazität hinzuzufügen, müssen Sie ein Volume oder qtree erstellen, um einen Storage-Container bereitzustellen, und eine Exportrichtlinie für diesen Container erstellen oder ändern. Anschließend können Sie den NFS-Client-Zugriff vom Cluster aus überprüfen und den Zugriff von Client-Systemen testen.

Was Sie benötigen

- NFS muss auf der SVM vollständig eingerichtet sein.
- Die standardmäßige Exportrichtlinie für das SVM-Root-Volume muss eine Regel enthalten, die den Zugriff auf alle Clients gestattet.
- Alle Aktualisierungen Ihrer Namensdienstkonfiguration müssen abgeschlossen sein.
- Alle Erweiterungen oder Änderungen an einer Kerberos-Konfiguration müssen abgeschlossen sein.

Erstellen Sie eine Exportrichtlinie

Bevor Sie Exportregeln erstellen können, müssen Sie eine Exportrichtlinie erstellen, die diese enthalten soll. Sie können das verwenden `vserver export-policy create` Befehl zum Erstellen einer Exportrichtlinie.

Schritte

1. Exportrichtlinie erstellen:

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

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

2. Überprüfen Sie, ob die Exportrichtlinie erstellt wurde:

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

Beispiel

Mit den folgenden Befehlen wird die Erstellung einer Exportrichtlinie namens exp1 auf der SVM namens vs1 erstellt und überprüft:

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

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

Fügen Sie eine Regel zu einer Exportrichtlinie hinzu

Ohne Regeln kann die Exportrichtlinie keinen Client-Zugriff auf Daten bereitstellen. Um eine neue Exportregel zu erstellen, müssen Sie Clients identifizieren und ein Clientabgleiche-Format auswählen, die Zugriffs- und Sicherheitstypen auswählen, eine anonyme Benutzer-ID-Zuordnung festlegen, eine Regel-Index-Nummer auswählen und das Zugriffsprotokoll auswählen. Anschließend können Sie die verwenden `vserver export-policy rule create` Befehl zum Hinzufügen der neuen Regel zu einer Exportrichtlinie.

Was Sie benötigen

- Die Exportrichtlinie, zu der Sie die Exportregeln hinzufügen möchten, muss bereits vorhanden sein.
- DNS muss auf der Daten-SVM korrekt konfiguriert sein und DNS-Server müssen die richtigen Einträge für NFS-Clients haben.

  Der Grund dafür ist, dass ONTAP DNS-Suchvorgänge mithilfe der DNS-Konfiguration der Daten-SVM für bestimmte Client-Übereinstimmungsformate durchführt. Fehler bei der Abstimmung von Richtlinien für den Export können den Zugriff auf Client-Daten verhindern.

- Wenn Sie mit Kerberos authentifizieren, müssen Sie festgelegt haben, welche der folgenden Sicherheitsmethoden auf Ihren NFS-Clients verwendet werden:
  - `krb5` (Kerberos V5-Protokoll)
  - `krb5i` (Kerberos V5-Protokoll mit Integritätsprüfung mit Prüfsummen)
  - `krb5p` (Kerberos V5-Protokoll mit Datenschutzdienst)

Über diese Aufgabe

Es ist nicht erforderlich, eine neue Regel zu erstellen, wenn eine vorhandene Regel in einer Exportrichtlinie Ihre Anforderungen für Clientabgleiche und Zugang abdeckt.

Wenn Sie mit Kerberos authentifizieren und wenn über Kerberos auf alle Volumes der SVM zugegriffen wird, können Sie die Export-Regeloptionen festlegen `-rorule`, `-rwrule`, und `-superuser` Für das Root-Volume zu `krb5`, `krb5i`, Oder `krb5p`.

Schritte

1. Identifizieren Sie die Clients und das Clientabgleichen-Format für die neue Regel.

   Der `-clientmatch` Option gibt die Clients an, auf die die Regel zutrifft. Ein- oder mehrere Clientabgleich-Werte können angegeben werden; Spezifikationen mehrerer Werte müssen durch Kommas getrennt werden. Sie können die Übereinstimmung in einem der folgenden Formate festlegen:

Client-Match-Format	Beispiel
Domänenname vorangestellt durch das Zeichen „.“	`.example.com` Oder `.example.com,.example.net,...`
Host-Name	`host1` Oder `host1,host2, ...`
IPv4-Adresse	`10.1.12.24` Oder `10.1.12.24,10.1.12.25, ...`
IPv4-Adresse mit einer Subnetzmaske, die als Anzahl von Bits ausgedrückt wird	`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 gepunkteten Format	`::1.2.3.4` Oder `::1.2.3.4,::1.2.3.5,...`
IPv6-Adresse mit einer Subnetzmaske, die als Anzahl der Bits ausgedrückt wird	`ff::00/32` Oder `ff::00/32,ff::01/32,...`
Eine einzelne Netzwerkgruppe mit dem Namen der Netzwerkgruppe, der dem Zeichen @ vorangestellt ist	`@netgroup1` Oder `@netgroup1,@netgroup2,...`

Sie können auch Arten von Client-Definitionen kombinieren, z. B. `.example.com,@netgroup1`.

Beachten Sie beim Angeben von IP-Adressen Folgendes:

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

  Einträge in diesem Format werden als Textzeichenfolge interpretiert und als Hostname behandelt.

- Geben Sie bei der Angabe einzelner IP-Adressen in Exportregeln für die granulare Verwaltung des Clientzugriffs keine dynamisch (z. B. DHCP) oder vorübergehend (z. B. IPv6) zugewiesenen IP-Adressen an.

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

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

2. Wählen Sie den Zugriff und die Sicherheitstypen für Clientabgleichungen aus.

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

   - `-rorule` (Schreibgeschützter Zugriff)
   - `-rwrule` (Lese-/Schreibzugriff)

◦ `-superuser` (Root-Zugriff)

> Ein Client kann nur Lese-/Schreibzugriff für einen bestimmten Sicherheitstyp erhalten, wenn die Exportregel auch schreibgeschützten Zugriff für diesen Sicherheitstyp zulässt. Wenn der schreibgeschützte Parameter für einen Sicherheitstyp restriktiver ist als der Parameter Read-Write, erhält der Client möglicherweise keinen Lese-Schreib-Zugriff. Dasselbe gilt für Superuser-Zugriff.

Sie können eine kommagetrennte Liste mit mehreren Sicherheitstypen für eine Regel angeben. Wenn Sie den Sicherheitstyp als angeben `any` Oder `never`Geben Sie keine anderen Sicherheitstypen an. Wählen Sie aus den folgenden gültigen Sicherheitstypen:

Wenn der Sicherheitstyp auf festgelegt ist…	**Ein passender Client kann auf die exportierten Daten zugreifen…**
`any`	Immer, unabhängig vom eingehenden Sicherheitstyp.
`none`	Wenn nur aufgeführt, werden Clients mit beliebigen Sicherheitstypen als anonym Zugriff gewährt. Wenn sie mit anderen Sicherheitstypen aufgelistet sind, erhalten Clients mit einem bestimmten Sicherheitstyp Zugriff, und Clients mit anderen Sicherheitstypen werden als anonym Zugriff gewährt.
`never`	Nie, unabhängig vom eingehenden Sicherheitstyp.
`krb5`	Wenn es von Kerberos 5 authentifiziert wird. Nur Authentifizierung: Die Kopfzeile jeder Anfrage und Antwort ist signiert.
`krb5i`	Wenn es von Kerberos 5i authentifiziert wird. Authentifizierung und Integrität: Die Kopfzeile und der Körper jeder Anfrage und Antwort wird signiert.
`krb5p`	Wenn es von Kerberos 5p authentifiziert wird. Authentifizierung, Integrität und Datenschutz: Die Kopfzeile und der Text jeder Anfrage und Antwort wird signiert und die NFS-Datenlast ist verschlüsselt.
`ntlm`	Wenn es durch CIFS NTLM authentifiziert wird.
`sys`	Wenn es durch NFS AUTH_SYS authentifiziert wird.

Der empfohlene Sicherheitstyp ist `sys`, Oder wenn Kerberos verwendet wird, `krb5`, `krb5i`, Oder

`krb5p`.

Wenn Sie Kerberos mit NFSv3 verwenden, muss die Regel für die Exportrichtlinie zulassen `-rorule` Und `-rwrule` Zugriff auf `sys` Zusätzlich zu `krb5`. Dies liegt daran, dass Network Lock Manager (NLM) Zugriff auf den Export gewährt werden muss.

3. Geben Sie eine anonyme Benutzer-ID-Zuordnung an.

   Der `-anon` Option gibt eine UNIX-Benutzer-ID oder einen Benutzernamen an, der Clientanforderungen zugeordnet ist, die mit einer Benutzer-ID von 0 (Null) ankommen, die normalerweise mit dem Stammverzeichnis des Benutzernamens verknüpft ist. Der Standardwert ist `65534`. NFS-Clients verbinden die Benutzer-ID 65534 normalerweise mit dem Benutzernamen nobody (auch bekannt als *root Squashing*). In ONTAP ist diese Benutzer-ID dem Benutzer-Benutzer zugeordnet. Um den Zugriff von einem Client mit einer Benutzer-ID von 0 zu deaktivieren, geben Sie einen Wert von an `65535`.

4. Wählen Sie die Indexreihenfolge der Regel aus.

   Der `-ruleindex` Option gibt die Indexnummer für die Regel an. Regeln werden nach ihrer Reihenfolge in der Liste der Indexnummern ausgewertet; Regeln mit niedrigeren Indexnummern werden zuerst ausgewertet. So wird die Regel mit Indexnummer 1 vor der Regel mit Indexnummer 2 ausgewertet.

Beim Hinzufügen…	**Dann…**
Die erste Regel für eine Exportrichtlinie	Eingabe `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 je nach Reihenfolge eine Indexnummer für die neue Regel aus, die ausgewertet werden soll.

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

   `nfs` Entspricht jeder Version, `nfs3` Und `nfs4` Stimmen Sie nur den jeweiligen Versionen ab.

6. Erstellen Sie die Exportregel, und fügen Sie sie einer vorhandenen Exportrichtlinie hinzu:

   ```
   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. Zeigen Sie die Regeln für die Exportrichtlinie an, um zu überprüfen, ob die neue Regel vorhanden ist:

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

   Der Befehl zeigt eine Zusammenfassung für diese Exportrichtlinie an, einschließlich einer Liste von Regeln, die auf diese Richtlinie angewendet werden. ONTAP weist jeder Regel eine Indexnummer zu. Wenn Sie die Nummer des Regelindex kennen, können Sie darauf detaillierte Informationen zur angegebenen Exportregel anzeigen.

8. Überprüfen Sie, ob die Regeln, die auf die Exportrichtlinie angewendet werden, richtig 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 Exportrichtlinie namens rs1. Die Regel hat die Indexnummer 1. Die Regel entspricht jedem Client in der Domäne eng.company.com und der netgroup @netgroup1. Die Regel ermöglicht allen NFS-Zugriff. Sie ermöglicht den schreibgeschützten und schreibgeschützten Zugriff auf Benutzer, die mit AUTH_SYS authentifiziert wurden. 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 Exportrichtlinie namens expol2. Die Regel hat die Indexnummer 21. Die Regel stimmt die Clients mit den Mitgliedern der netgroup dev_netgroup_main überein. Die Regel ermöglicht allen NFS-Zugriff. Sie ermöglicht den schreibgeschützten Zugriff für Benutzer, die mit AUTH_SYS authentifiziert wurden, und erfordert Kerberos-Authentifizierung für Lese- und Root-Zugriff. Clients mit der UNIX-Benutzer-ID 0 (Null) werden Root-Zugriff verweigert, es sei denn, sie werden mit Kerberos authentifiziert.

```
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
```

Erstellung eines Volume oder qtree Storage-Containers

Erstellen eines Volumes

Sie können ein Volume erstellen und dessen Verbindungspunkt und andere Eigenschaften mit der festlegen `volume create` Befehl.

Über diese Aufgabe

Ein Volume muss einen Verbindungspfad_ enthalten, damit seine Daten den Clients zur Verfügung gestellt werden können. Sie können den Verbindungspfad angeben, wenn Sie ein neues Volume erstellen. Wenn Sie ein Volume erstellen, ohne einen Verbindungspfad anzugeben, müssen Sie das Volume über den im SVM Namespace mounten `volume mount` Befehl.

Bevor Sie beginnen

- NFS sollte eingerichtet und ausgeführt werden.
- Der SVM-Sicherheitsstil muss UNIX sein.
- Ab ONTAP 9.13.1 können Sie Volumes mit aktivierten Kapazitätsanalysen und Aktivitätsverfolgung erstellen. Um die Kapazitäts- oder Aktivitätsverfolgung zu aktivieren, geben Sie das ein `volume create`

Befehl mit `-analytics-state` Oder `-activity-tracking-state` Auf einstellen `on`.

Weitere Informationen zur Kapazitätsanalyse und Aktivitätsverfolgung finden Sie unter Dateisystemanalyse Aktivieren.

Schritte

1. Volume mit einem Verbindungspunkt 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 Wahl für `-junction-path` Sind die folgenden:

   - Beispielsweise direkt unter root */`new_vol`*

     Sie können ein neues Volume erstellen und festlegen, dass es direkt in das SVM Root-Volume eingebunden wird.

   - Unter einem vorhandenen Verzeichnis z.B. */`existing_dir/new_vol`*

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

     Wenn Sie ein Volume in einem neuen Verzeichnis erstellen möchten (in einer neuen Hierarchie unter einem neuen Volume), zum Beispiel, */`new_dir/new_vol`*, Anschließend müssen Sie zuerst ein neues übergeordnetes Volume erstellen, das mit dem SVM Root Volume verbunden ist. Anschließend würde das neue untergeordnete Volume im Verbindungspfad des neuen übergeordneten Volume (neues Verzeichnis) erstellt.

   + Wenn Sie eine vorhandene Exportrichtlinie verwenden möchten, können Sie diese beim Erstellen des Volumes angeben. Sie können später auch eine Exportrichtlinie mit dem hinzufügen `volume modify` Befehl.

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

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

Beispiele

Mit dem folgenden Befehl wird ein neues Volume mit dem Namen „user1“ auf der SVM vs1.example.com und auf dem Aggregat aggr1 erstellt. Der neue Band wird bei zur Verfügung gestellt `/users`. Das Volume ist 750 GB groß und seine Volumengarantie ist vom Typ Volume (standardmäßig).

```
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
```

Mit dem folgenden Befehl wird ein neues Volume namens „home4“ auf der SVM „vs1.example.com“ und das Aggregat „aggr1“ erstellt. Das Verzeichnis `/eng/` Im Namespace für die vs1 SVM ist bereits vorhanden, und das neue Volume wird unter zur Verfügung gestellt `/eng/home`, Das zum Home-Verzeichnis für das wird `/eng/` Namespace. Das Volumen ist 750 GB groß und seine Volumengarantie ist vom Typ `volume` (Standardmäßig).

```
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
```

Erstellen Sie einen qtree

Sie können einen qtree erstellen, der Ihre Daten enthält, und seine Eigenschaften mit der festlegen `volume qtree create` Befehl.

Was Sie benötigen

- Es muss bereits die SVM und das Volume, das den neuen qtree enthalten soll, vorhanden sein.
- Der SVM-Sicherheitsstil muss UNIX sein, und NFS sollte eingerichtet und in Betrieb sein.

Schritte

1. Erstellen Sie den qtree:

   `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 qtree als separate Argumente angeben oder das qtree-Pfad-Argument im Format angeben `/vol/`*`volume_name/_qtree_name`*.

   Standardmäßig übernehmen die qtrees die Exportrichtlinien für ihr übergeordnetes Volume, können jedoch

so konfiguriert werden, dass sie ein eigenes Volume verwenden. Wenn Sie eine vorhandene Exportrichtlinie verwenden möchten, können Sie diese beim Erstellen des qtree angeben. Sie können später auch eine Exportrichtlinie mit dem hinzufügen `volume qtree modify` Befehl.

2. Vergewissern Sie sich, dass 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

Im folgenden Beispiel wird ein qtree mit dem Namen qt01 auf der SVM vs1.example.com erstellt, der über einen Verbindungspfad verfügt `/vol/data1`:

```
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
```

Sicherer NFS-Zugriff über Exportrichtlinien

Sicherer NFS-Zugriff über Exportrichtlinien

Sie können Exportrichtlinien verwenden, um den NFS-Zugriff auf Volumes oder qtrees zu beschränken, die bestimmten Parametern entsprechen. Bei der Bereitstellung von neuem Speicher können Sie eine vorhandene Richtlinie und Regeln verwenden, einer vorhandenen Richtlinie Regeln hinzufügen oder neue Richtlinien und Regeln erstellen. Sie können auch die Konfiguration von Exportrichtlinien überprüfen

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

Verwalten der Verarbeitungsreihenfolge der Exportregeln

Sie können das verwenden `vserver export-policy rule setindex` Befehl zum manuellen Festlegen der Indexnummer einer vorhandenen Exportregel. Dadurch können Sie festlegen, durch welche Priorität ONTAP Exportregeln auf Client-Anforderungen anwendet.

Über diese Aufgabe

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

Schritt

1. Die Indexnummer einer angegebenen Exportregel ändern:

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

Beispiel

Mit dem folgenden Befehl wird die Indexnummer einer Exportregel unter Indexnummer 3 in die Indexnummer 2 in einer Exportrichtlinie namens rs1 auf der SVM mit dem Namen vs1 geändert:

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

Weisen Sie einer Exportrichtlinie einem Volume zu

Jedes Volume in der SVM muss einer Exportrichtlinie zugeordnet werden, die Exportregeln für Clients enthält, um auf Daten im Volume zuzugreifen.

Über diese Aufgabe

Sie können eine Exportrichtlinie einem Volume zuordnen, wenn Sie das Volume erstellen oder zu einem beliebigen Zeitpunkt nach der Erstellung des Volumes. Sie können eine Exportrichtlinie dem Volume zuweisen, obwohl eine Richtlinie vielen Volumes zugeordnet werden kann.

Schritte

1. Wenn beim Erstellen des Volumes keine Exportrichtlinie angegeben wurde, weisen Sie dem Volume eine Exportrichtlinie zu:

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

2. Vergewissern Sie sich, dass die Richtlinie dem Volume zugewiesen wurde:

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

Beispiel

Die folgenden Befehle weisen der Exportrichtlinie nfs_Policy dem Volume vol1 auf der SVM vs1 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
```

Weisen Sie einer Exportrichtlinie einem qtree zu

Anstatt ein ganzes Volume zu exportieren, können Sie auch einen bestimmten qtree auf ein Volume exportieren und direkt für Clients zugänglich machen. Sie können einen qtree exportieren, indem Sie ihm eine Exportrichtlinie zuweisen. Sie können die Exportrichtlinie entweder beim Erstellen eines neuen qtree oder durch Ändern eines vorhandenen qtree zuweisen.

Was Sie benötigen

Die Exportrichtlinie muss vorhanden sein.

Über diese Aufgabe

Standardmäßig übernehmen die qtrees die übergeordneten Exportrichtlinien des enthaltenden Volumes, wenn dies zum Zeitpunkt der Erstellung nicht anders angegeben wird.

Sie können eine Exportrichtlinie einem qtree zuweisen, wenn Sie den qtree erstellen oder jederzeit nach dem Erstellen des qtree. Sie können eine Exportrichtlinie dem qtree zuordnen, obwohl eine Richtlinie mit vielen qtrees verknüpft werden kann.

Schritte

1. Wenn beim Erstellen des qtree keine Exportrichtlinie angegeben wurde, weisen Sie dem qtree eine Exportrichtlinie zu:

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

2. Vergewissern Sie sich, dass die Richtlinie dem qtree zugewiesen war:

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

Beispiel

Die folgenden Befehle ordnen Sie der SVM vs1 die Exportrichtlinie nfs_Policy dem qtree qt1 zu und überprüfen Sie 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
```

Überprüfen Sie den NFS-Client-Zugriff vom Cluster aus

Sie können ausgewählten Clients Zugriff auf die Freigabe gewähren, indem Sie UNIX-Dateiberechtigungen auf einem UNIX-Administrationshost festlegen. Sie können den Client-Zugriff über das überprüfen `vserver export-policy check-access` Befehl, ggf. die Exportregeln anpassen.

Schritte

1. Überprüfen Sie im Cluster den Client-Zugriff auf Exporte mithilfe des `vserver export-policy check-access` Befehl.

   Der folgende Befehl überprüft den Lese-/Schreibzugriff auf einen NFSv3 Client mit der IP-Adresse 1.2.3.4 auf das Volume home2. Die Befehlsausgabe gibt an, dass das Volume die Exportrichtlinie verwendet `exp-home-dir` Und dieser Zugriff wird verweigert.

   ```
   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. Überprüfen Sie die Ausgabe, um zu bestimmen, ob die Export-Richtlinie wie vorgesehen funktioniert und sich der Client-Zugriff wie erwartet verhält.

   Konkret sollten Sie überprüfen, welche Export-Richtlinie vom Volume oder qtree verwendet wird und welche Zugriffstyp der Client als Ergebnis hat.

3. Gegebenenfalls die Regeln für die Exportrichtlinie neu konfigurieren.

Testen Sie den NFS-Zugriff von Client-Systemen

Nachdem Sie den NFS-Zugriff auf das neue Storage-Objekt überprüft haben, sollten Sie die Konfiguration testen. Dazu müssen Sie sich bei einem NFS-Administrationshost anmelden und die Daten von der SVM lesen und auf die SVM schreiben. Anschließend sollten Sie den Prozess als nicht-Root-Benutzer in einem Client-System wiederholen.

Was Sie benötigen

- Das Clientsystem muss über eine IP-Adresse verfügen, die durch die zuvor angegebene Exportregel zulässig ist.
- Sie müssen die Anmeldedaten für den Root-Benutzer haben.

Schritte

1. Überprüfen Sie im Cluster die IP-Adresse der logischen Schnittstelle, die das neue Volume hostet:

   `network interface show –vserver svm_name`

2. Melden Sie sich als Root-Benutzer beim Administrationshost-Client-System an.
3. Ändern Sie das Verzeichnis in den Mount-Ordner:

   `cd /mnt/`

4. Erstellen und Mounten eines neuen Ordners unter Verwendung der IP-Adresse der SVM:

   a. Erstellen Sie einen neuen Ordner:
   `mkdir /mnt/folder`

   b. Mounten Sie das neue Volume in diesem neuen Verzeichnis:
   `mount -t nfs -o hard IPAddress:/volume_name /mnt/folder`

   c. Ändern Sie das Verzeichnis in den neuen Ordner:
   `cd folder`

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

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

5. Erstellen Sie eine neue Datei, überprüfen Sie, ob sie vorhanden ist, und schreiben Sie Text in die Datei:

   a. Testdatei erstellen:
   `touch filename`

   b. Überprüfen Sie, ob die Datei existiert.:
   `ls -l filename`

   c. Geben Sie: + Ein `cat > filename`

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

d. Zeigt den Inhalt der Testdatei an.
`cat filename`

e. Entfernen Sie die Testdatei:
`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. Legen Sie als Root alle gewünschten UNIX-Eigentumsrechte und Berechtigungen auf dem gemounteten Volume fest.
7. Melden Sie sich auf einem UNIX-Client-System an, das in Ihren Exportregeln festgelegt ist, als einer der autorisierten Benutzer an, die nun Zugriff auf das neue Volume haben, und wiederholen Sie die Schritte in Schritt 3 bis 5, um zu überprüfen, ob Sie das Volume mounten und eine Datei erstellen können.