Managen Sie den Dateizugriff über NFS

ONTAP 9

NetApp
February 12, 2026

Inhalt

Managen Sie den Dateizugriff über NFS

Aktivieren oder Deaktivieren von NFSv3 für ONTAP SVMs

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

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Aktivieren Sie NFSv3	`vserver nfs modify -vserver vserver_name -v3 enabled`
Deaktivieren Sie NFSv3	`vserver nfs modify -vserver vserver_name -v3 disabled`

Aktivieren oder Deaktivieren von NFSv4.0 für ONTAP SVMs

Sie können NFSv4.0 durch Ändern der `-v4.0` Option aktivieren oder deaktivieren. So ist der Dateizugriff für Clients möglich, die das NFSv4.0-Protokoll verwenden. In ONTAP 9.9 ist NFSv4.0 standardmäßig aktiviert; in früheren Versionen ist er standardmäßig deaktiviert.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	**Geben Sie den folgenden Befehl ein…**
Aktivieren Sie NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 enabled`
Deaktivieren Sie NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 disabled`

Aktivieren oder Deaktivieren von NFSv4.1 für ONTAP SVMs

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

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Aktivieren Sie NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 enabled`
Deaktivieren Sie NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 disabled`

Verwalten der ONTAP NFSv4 Storepool-Limits

Ab ONTAP 9.13 können Administratoren ihre NFSv4-Server aktivieren, um Ressourcen für NFSv4-Clients zu verweigern, wenn sie die Grenzen für die einzelnen Client-Speicherpools-Ressourcen erreicht haben. Wenn Clients zu viele NFSv4-Speicherpool-Ressourcen verbrauchen, kann dies dazu führen, dass andere NFSv4-Clients blockiert werden, weil die NFSv4-Speicherpool-Ressourcen nicht verfügbar sind.

Durch Aktivieren dieser Funktion können Kunden auch den aktiven Ressourcenverbrauch des Speicherpools für jeden Client anzeigen. Dies erleichtert die Identifizierung von Clients, die zu viel Systemressourcen benötigen, und ermöglicht das Aufzwingen von Ressourcenbeschränkungen pro Client.

Anzeige der belegten Speicherpools

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

Schritt

1. Führen Sie als Administrator den `vserver nfs storepool show` Befehl aus, um die Storepool-Informationen von NFSv4-Clients anzuzeigen.

Beispiel

Dieses Beispiel zeigt die Speicherpools-Informationen der 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 Sie die Steuerelemente für die Speicherpool-Begrenzung

Administratoren können die folgenden Befehle verwenden, um die Steuerelemente für die Speicherpool-Begrenzung zu aktivieren oder zu deaktivieren.

Schritt

1. Führen Sie als Administrator eine der folgenden Aktionen durch:

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Steuerelemente für die Speicherpool-Begrenzung aktivieren	`vserver nfs storepool config modify -limit-enforce enabled`
Steuerelemente für die Speicherpool-Begrenzung deaktivieren	`vserver nfs storepool config modify -limit-enforce disabled`

Eine Liste der blockierten Clients anzeigen

Wenn die Speicherpoolgrenze aktiviert ist, können Administratoren sehen, welche Clients beim Erreichen ihrer Ressourcenschwelle pro Client blockiert wurden. Administratoren können den folgenden Befehl verwenden, um zu sehen, welche Clients als blockierte Clients markiert wurden.

Schritte

1. Verwenden Sie den `vserver nfs storepool blocked-client show` Befehl, um die Liste der blockierten NFSv4-Clients anzuzeigen.

Entfernen Sie einen Client aus der Liste der blockierten Clients

Clients, die ihren Schwellenwert pro Client erreichen, werden getrennt und dem Block-Client-Cache hinzugefügt. Administratoren können den Client mit dem folgenden Befehl aus dem Block-Client-Cache entfernen. Dadurch kann der Client eine Verbindung zum ONTAP NFSV4-Server herstellen.

Schritte

1. Verwenden Sie den `vserver nfs storepool blocked-client flush -client-ip <ip address>` Befehl, um den Cache des blockierten Storepool-Clients zu leeren.
2. `vserver nfs storepool blocked-client show`Überprüfen Sie mit dem Befehl, ob der Client aus dem Block-Client-Cache entfernt wurde.

Beispiel

In diesem Beispiel wird ein blockierter Client mit der IP-Adresse „10.2.1.1“ angezeigt, der von allen Knoten gespült 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.
```

Aktivieren oder Deaktivieren von pNFS für ONTAP SVMs

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

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

Bevor Sie beginnen

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

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

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

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Aktivieren Sie pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled`
Deaktivieren Sie pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled`

Verwandte Informationen

- Übersicht über NFS Trunking

Steuern Sie den NFS-Zugriff über TCP und UDP für ONTAP SVMs

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

Über diese Aufgabe

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

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

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

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

Steuern Sie NFS-Anfragen von nicht reservierten Ports für ONTAP SVMs

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

Über diese Aufgabe

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

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

Diese Optionen gelten nicht für das Null-Verfahren.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Zulassen von NFS-Mount-Anforderungen von nicht reservierten Ports	`vserver nfs modify -vserver vserver_name -mount -rootonly disabled`
NFS-Mount-Anforderungen von nicht reservierten Ports ablehnen	`vserver nfs modify -vserver vserver_name -mount -rootonly enabled`
Erlauben Sie alle NFS-Anfragen von nicht reservierten Ports	`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`

Verwalten Sie den NFS-Zugriff auf ONTAP NTFS-Volumes oder Qtrees für unbekannte UNIX-Benutzer

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

- Zugriff auf unbekannte UNIX-Benutzer verweigern.

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

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

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

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie den standardmäßigen Windows-Benutzer für unbekannte UNIX-Benutzer wünschen…	Geben Sie den Befehl ein…
Aktiviert	`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 Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Überlegungen für Clients, die ONTAP NFS-Exporte auf nicht reservierten Ports mounten

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

Wenn die `-mount-rootonly` Option aktiviert ist, ermöglicht ONTAP NFS-Clients, die nicht reservierte Ports verwenden, nicht das Mounten von NFS-Exporten, d. h. Ports mit Zahlen über 1,023.

Führen Sie strengere Zugriffsprüfungen für Netzgruppen durch, indem Sie Domänen für ONTAP NFS SVMs überprüfen

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

Über diese Aufgabe

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

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

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

Diese Überprüfung ist standardmäßig aktiviert. Sie können sie verwalten, indem Sie den `-netgroup-dns -domain-search` Parameter ändern, der auf der erweiterten Berechtigungsebene verfügbar ist.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Führen Sie die gewünschte Aktion aus:

Wenn Sie möchten, dass die Domänenüberprüfung für Netzgruppen…	Eingeben…
Aktiviert	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled`
Deaktiviert	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled`

3. Legen Sie die Berechtigungsebene auf admin fest:

   ```
   set -privilege admin
   ```

Ändern Sie die für NFSv3-Dienste für ONTAP SVMs verwendeten Ports

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Zugriff auf NFS deaktivieren:

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

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

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

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

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

4. Zugriff auf NFS aktivieren:

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

5. `network connections listening show`Überprüfen Sie mit dem Befehl die Änderungen der Port-Nummer.

   Erfahren Sie mehr über `network connections listening show` in der "ONTAP-Befehlsreferenz".

6. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Beispiel

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

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

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

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

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

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

ONTAP-Befehle zum Managen von NFS-Servern

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

Ihr Ziel ist	Befehl
Erstellen Sie einen NFS-Server	`vserver nfs create`

Zeigen Sie NFS-Server an	`vserver nfs show`
Ändern eines NFS-Servers	`vserver nfs modify`
Löschen Sie einen NFS-Server	`vserver nfs delete`
Ausblenden Sie die `.snapshot` Verzeichnisliste unter NFSv3-Mount-Punkten Der explizite Zugriff auf das `.snapshot` Verzeichnis ist auch dann noch erlaubt, wenn die Option aktiviert ist.	`vserver nfs` Befehle mit der `-v3-hide-snapshot` Option aktiviert

Erfahren Sie mehr über `vserver nfs` in der "ONTAP-Befehlsreferenz".

Beheben von Name-Service-Problemen für ONTAP NAS SVMs

Wenn auf Clients aufgrund von Problemen mit dem Namensdienst Zugriffsfehler auftreten, können Sie mithilfe der `vserver services name-service getxxbyyy` Befehlfamilie manuell verschiedene Namendienstuchabfragen durchführen und die Details und Ergebnisse der Suche untersuchen, um die Fehlerbehebung zu erleichtern.

Über diese Aufgabe

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

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

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Um den abzurufen…	Verwenden Sie den Befehl…

IP-Adresse eines Host-Namens	`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 Benutzernamen	`vserver services name-service getxxbyyy getpwbyname` Sie können die Namensauflösung von RBAC-Benutzern testen, indem Sie den `-use-rbac` Parameter als angeben `true`.
Benutzerinformationen nach Benutzer-ID	`vserver services name-service getxxbyyy getpwbyuid` Sie können die Namensauflösung von RBAC-Benutzern testen, indem Sie den `-use-rbac` Parameter als angeben `true`.
Netzgruppenmitgliedschaft eines Clients	`vserver services name-service getxxbyyy netgrp`
Netzwerkgruppenmitgliedschaft eines Clients mit der Suche nach Netgroup-by-Host	`vserver services name-service getxxbyyy netgrpbyhost`

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

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

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

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvc2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

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

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

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

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

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

Wenn der…	**Überprüfen Sie…**
Die Suche nach Host-Name oder IP-Adresse ist fehlgeschlagen oder hat falsche Ergebnisse angezeigt	DNS-Konfiguration

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

Verwandte Informationen

"NetApp Technical Report 4668: Name Services Best Practices Guide"

Überprüfen der Name-Service-Verbindungen für ONTAP NAS SVMs

Sie können DNS- und Lightweight Directory Access Protocol (LDAP)-Nameserver überprüfen, um sicherzustellen, dass sie mit ONTAP verbunden sind. Diese Befehle sind auf der Administrator-Berechtigungsebene verfügbar.

Über diese Aufgabe

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

Für DNS-Konfigurationen werden alle Server getestet und müssen funktionieren, damit die Konfiguration als gültig erachtet wird. Bei LDAP-Konfigurationen ist die Konfiguration gültig, solange ein Server aktiv ist. Die Befehle für den Namendienst wenden die Konfigurationsprüfung an, sofern das `skip-config-validation` Feld nicht wahr ist (die Standardeinstellung ist false).

Schritt

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

Prüfung…	Befehl
DNS-Konfigurationsstatus	`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 der Dienst bereitgestellt wird. Wenn einige Server nicht erreichbar sind, wird eine Warnung angezeigt.

ONTAP-Befehle zum Verwalten von NAS-Name-Service-Switch-Einträgen

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

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

Erfahren Sie mehr über `vserver services name-service ns-switch` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

"NetApp Technical Report 4668: Name Services Best Practices Guide"

ONTAP-Befehle zur Verwaltung des NAS-Namensdienst-Cache

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

Wenn Sie den TTL-Wert ändern möchten für…	Befehl
UNIX-Benutzer	`vserver services name-service cache unix-user settings`
UNIX-Gruppen	`vserver services name-service cache unix-group settings`
UNIX-Netzwerkgruppen	`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 zum Managen von NFS-Namenszuordnungen

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

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

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

Erfahren Sie mehr über `vserver name-mapping` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zum Verwalten lokaler NAS-UNIX-Benutzer

Es gibt bestimmte ONTAP Befehle zum Management lokaler UNIX Benutzer.

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

Erfahren Sie mehr über `vserver services name-service unix-user` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zum Verwalten lokaler NAS-UNIX-Gruppen

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

Ihr Ziel ist	Befehl

Erstellen Sie eine lokale UNIX-Gruppe	`vserver services name-service unix-group create`
Fügen Sie einen Benutzer zu einer lokalen UNIX-Gruppe hinzu	`vserver services name-service unix-group adduser`
Laden Sie lokale UNIX-Gruppen von einem URI	`vserver services name-service unix-group load-from-uri`
Zeigen Sie lokale UNIX-Gruppen an	`vserver services name-service unix-group show`
Ändern einer lokalen UNIX-Gruppe	`vserver services name-service unix-group modify`
Löschen Sie einen Benutzer aus einer lokalen UNIX-Gruppe	`vserver services name-service unix-group deluser`
Löschen Sie eine lokale UNIX-Gruppe	`vserver services name-service unix-group delete`

Erfahren Sie mehr über `vserver services name-service unix-group` in der "ONTAP-Befehlsreferenz".

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

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

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

Datenbank	Standardlimit	Harte Grenze
Lokale UNIX-Benutzer	32.768	65.536
Lokale UNIX-Gruppen und Gruppenmitglieder	32.768	65.536

Verwalten Sie Limits für lokale UNIX-Benutzer und -Gruppen für ONTAP NFS SVMs

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

Über diese Aufgabe

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

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Verwenden Sie den Befehl…
Informationen zu lokalen UNIX-Benutzerlimits anzeigen	`vserver services unix-user max-limit show`
Zeigen Sie Informationen über die Grenzwerte der lokalen UNIX-Gruppen an	`vserver services unix-group max-limit show`
Ändern Sie die lokalen UNIX-Benutzergrenzen	`vserver services unix-user max-limit modify`
Ändern Sie die Grenzwerte für lokale UNIX-Gruppen	`vserver services unix-group max-limit modify`

Erfahren Sie mehr über `vserver services unix` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zum Verwalten lokaler NFS-Netzgruppen

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

Ihr Ziel ist	Verwenden Sie den Befehl…
Laden von Netzgruppen aus einem URI	`vserver services name-service netgroup load`
Überprüfen Sie den Status von Netzgruppen über Knoten hinweg	`vserver services name-service netgroup status` Verfügbar auf der erweiterten Berechtigungsebene und höher.
Zeigen Sie lokale Netzgruppen an	`vserver services name-service netgroup file show`

Lokale Netzwerkgruppe löschen	`vserver services name-service netgroup file delete`

Erfahren Sie mehr über `vserver services name-service netgroup file` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zum Verwalten von NFS-NIS-Domänenkonfigurationen

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

Ihr Ziel ist	Befehl
Erstellen Sie eine NIS-Domänenkonfiguration	`vserver services name-service nis-domain create`
Anzeige der NIS-Domänenkonfigurationen	`vserver services name-service nis-domain show`
Anzeige des Bindungsstatus einer NIS-Domain-Konfiguration	`vserver services name-service nis-domain show-bound`
Zeigt die NIS-Statistiken an	`vserver services name-service nis-domain show-statistics` Verfügbar auf der erweiterten Berechtigungsebene und höher.
Löschen Sie NIS-Statistiken	`vserver services name-service nis-domain clear-statistics` Verfügbar auf der erweiterten Berechtigungsebene und höher.
Ändern Sie eine NIS-Domänenkonfiguration	`vserver services name-service nis-domain modify`
Löschen Sie eine NIS-Domänenkonfiguration	`vserver services name-service nis-domain delete`
Aktivieren Sie das Caching für Netzgruppensuche nach Host	`vserver services name-service nis-domain netgroup-database config modify` Verfügbar auf der erweiterten Berechtigungsebene und höher.

Erfahren Sie mehr über `vserver services name-service nis-domain` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zum Verwalten von NFS-LDAP-Clientkonfigurationen

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

Befehle.

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

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

Erfahren Sie mehr über `vserver services name-service ldap client` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zum Verwalten von NFS-LDAP-Konfigurationen

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

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

Erfahren Sie mehr über `vserver services name-service ldap` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zum Verwalten von NFS-LDAP-Clientschemavorlagen

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

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

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

Erfahren Sie mehr über `vserver services name-service ldap client schema` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zum Verwalten von NFS Kerberos-Schnittstellenkonfigurationen

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

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

Erfahren Sie mehr über `vserver nfs kerberos interface` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zum Verwalten von NFS Kerberos-Realm-Konfigurationen

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

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

Erfahren Sie mehr über `vserver nfs kerberos realm` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zur Verwaltung von Exportrichtlinien

Zum Management von Exportrichtlinien gibt es bestimmte ONTAP-Befehle.

Ihr Ziel ist	Befehl
Informationen zu Exportrichtlinien anzeigen	`vserver export-policy show`
Benennen Sie eine Exportrichtlinie um	`vserver export-policy rename`
Exportrichtlinie kopieren	`vserver export-policy copy`
Löschen Sie eine Exportrichtlinie	`vserver export-policy delete`

Erfahren Sie mehr über `vserver export-policy` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zum Verwalten von Exportregeln

Zum Management von Exportregeln gibt es bestimmte ONTAP-Befehle.

Ihr Ziel ist	Befehl

Erstellen Sie eine Exportregel	`vserver export-policy rule create`
Informationen zu Exportregeln anzeigen	`vserver export-policy rule show`
Exportregel ändern	`vserver export-policy rule modify`
Exportregel löschen	`vserver export-policy rule delete`

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

Erfahren Sie mehr über `vserver export-policy` in der "ONTAP-Befehlsreferenz".

Konfigurieren Sie den NFS-Anmeldeinformationscache

Gründe für die Änderung der Time-to-Live des NFS-Anmeldeinformationscache für ONTAP SVMs

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

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

Gründe

Unter folgenden Umständen sollte die Standard-TTL geändert werden:

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

Problem	Korrekturmaßnahmen
Der Name-Server-Administrator hat Änderungen vorgenommen, um den Zugriff auf NFS-Benutzer zu verweigern, die zuvor zugelassen waren.	Reduzieren Sie die TTL für positive Anmeldeinformationen im Cache, um die Zeit zu verkürzen, bevor ONTAP neue Zugangsdaten von externen Name-Servern anfordert, damit NFS-Benutzer jetzt keinen Zugriff haben.

Konsequenzen

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

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

Konfigurieren Sie die Lebensdauer für zwischengespeicherte NFS-Benutzeranmeldeinformationen für ONTAP SVMs

Sie können die Länge der Zeit konfigurieren, die ONTAP Anmeldedaten für NFS-Benutzer in seinem internen Cache speichert (time-to-live oder TTL), indem Sie den NFS-Server der SVM (Storage Virtual Machine) ändern. So werden bestimmte Probleme entschärft, die bei hoher Belastung des Name Servers oder bei Änderungen der Zugangsdaten, die sich auf den Zugriff von NFS-Benutzern auswirken, auftreten können.

Über diese Aufgabe

Diese Parameter sind auf der erweiterten Berechtigungsebene verfügbar.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Führen Sie die gewünschte Aktion aus:

Wenn Sie die TTL für den Cache ändern möchten…	Verwenden Sie den Befehl…
Positive Referenzen	`vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live` Die TTL wird in Millisekunden gemessen. Ab ONTAP 9.10.1 ist der Standardwert 1 Stunde (3,600,000 Millisekunden). In ONTAP 9.9.1 und früheren Versionen beträgt der Standardwert 24 Stunden (86,400,000 Millisekunden). Der zulässige Bereich für diesen Wert beträgt 1 Minute (60000 Millisekunden) bis 7 Tage (604,800,000 Millisekunden).
Negative Anmeldeinformationen	`vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live` Die TTL wird in Millisekunden gemessen. Der Standardwert ist 2 Stunden (7,200,000 Millisekunden). Der zulässige Bereich für diesen Wert beträgt 1 Minute (60000 Millisekunden) bis 7 Tage (604,800,000 Millisekunden).

3. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

Management von Caches für Exportrichtlinien

Leeren Sie die Exportrichtlinien-Caches für ONTAP NAS SVMs

ONTAP nutzt mehrere Exportrichtlinien-Caches, um Informationen im Zusammenhang mit Exportrichtlinien zu speichern, um schnelleren Zugriff zu ermöglichen. Export Policy Caches manuell (`vserver export-policy cache flush`löschen) entfernt potenziell veraltete Informationen und zwingt ONTAP, aktuelle Informationen aus den entsprechenden externen Ressourcen abzurufen. Dies kann dabei helfen, eine Vielzahl von Problemen im Zusammenhang mit dem Client-Zugriff auf NFS-Exporte zu lösen.

Über diese Aufgabe

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

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

Schritte

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

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

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

Wenn Sie spülen möchten…	Geben Sie den Befehl ein…
Die Exportrichtlinie regeln den Zugriff auf den Cache	`vserver export-policy cache flush -vserver vserver_name -cache access` Sie können den optionalen `-node` Parameter hinzufügen, um den Node anzugeben, auf dem Sie den Zugriffs-Cache leeren möchten.
Der Host-Name-Cache	`vserver services name-service cache hosts forward-lookup delete-all`

Wenn Sie spülen möchten…	Geben Sie den Befehl ein…
Der Netzwerk-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. Sie sollten den Netgroup-Cache nur dann leeren, wenn Sie versuchen, ein Problem mit dem Clientzugriff zu lösen, das durch eine veraltete Netzwerkgruppe verursacht wird.
Der showmount-Cache	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

Zeigen Sie die Netgroup-Warteschlange und den Cache der Exportrichtlinie für ONTAP NFS SVMs an

ONTAP verwendet die Netzwerkgruppewarteschlange beim Importieren und Auflösen von Netzgruppen und verwendet den Netzwerkgruppecache, um die resultierenden Informationen zu speichern. Wenn Sie Probleme mit der Exportrichtlinie Netzgruppen beheben, können Sie mit den `vserver export-policy netgroup queue show` `vserver export-policy netgroup cache show` Befehlen und den Status der Netzgruppenwarteschlange und den Inhalt des Netzgruppencaches anzeigen.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

So zeigen Sie die Netzwerkgruppe der Exportrichtlinie an:	Geben Sie den Befehl ein…
Warteschlange	`vserver export-policy netgroup queue show`
Cache	`vserver export-policy netgroup cache show -vserver vserver_name`

Erfahren Sie mehr über `vserver export-policy netgroup` in der "ONTAP-Befehlsreferenz".

Überprüfen Sie, ob eine Client-IP-Adresse Mitglied einer ONTAP NFS-Netzgruppe ist

Wenn Sie Probleme mit dem NFS-Client-Zugriff `vserver export-policy netgroup check-membership` in Verbindung mit Netzwerkgruppen beheben, können Sie mit dem Befehl ermitteln, ob eine Client-IP Mitglied einer bestimmten Netzwerkgruppe ist.

Über diese Aufgabe

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

Schritt

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

   Der Befehl kann die folgenden Ergebnisse zurückgeben:

   - Der Client ist Mitglied der Netzwerkgruppe.

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

   - Der Client ist Mitglied der Netzwerkgruppe.

     Sie wurde im ONTAP Netzwerkgruppecache gefunden.

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

     Bis zu diesem Zeitpunkt kann die Mitgliedschaft nicht explizit in oder aus ausgeschlossen werden. Verwenden Sie den `vserver export-policy netgroup queue show` Befehl, um das Laden der Netzgruppe zu überwachen, und versuchen Sie die Prüfung erneut, nachdem sie abgeschlossen ist.

Beispiel

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

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

Optimieren Sie die Zugriffscache-Leistung für ONTAP NFS SVMs

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

Über diese Aufgabe

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

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

  Der Vorteil ist eine bessere Performance, weil ONTAP weniger Ressourcen für die Aktualisierung von Zugriffs-Cache-Einträgen ausgibt. Der Nachteil besteht darin, dass eine Aktualisierung der Regeln für die

Exportrichtlinie und die Einträge für den Zugriffs-Cache veraltet ist. Dies führt dazu, dass Clients, die Zugriff erhalten sollen, möglicherweise verweigert werden und Clients, die verweigert werden sollten, möglicherweise Zugriff erhalten.

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

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

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Führen Sie die gewünschte Aktion aus:

So ändern Sie die…	Eingeben…
Zeitraum für positive Einträge aktualisieren	`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`
Timeout-Zeitraum für alte Einträge	`vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value`

3. Überprüfen Sie die neuen Parametereinstellungen:

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

4. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Verwalten von Dateisperren

Erfahren Sie mehr über die Dateisperre zwischen Protokollen für ONTAP NFS SVMs

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

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

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

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

- In gemischten oder NTFS-Volumes `rm` `rmdir` `mv` können Dateimanipulationsvorgänge wie, und dazu führen, dass die NFS-Anwendung fehlschlägt.
- Lese- und Schreibvorgänge für NFS werden vom SMB Deny-read- bzw. Deny-Write-Open-Modus verweigert.
- NFS-Schreibvorgänge schlagen fehl, wenn der geschriebene Bereich der Datei durch einen exklusiven SMB-Bytelock gesperrt ist.

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

Erfahren Sie mehr über schreibgeschützte Bits für ONTAP NFS SVMs

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

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

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

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

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

Das Nur-Lese-Bit interagiert mit den ACL- und Unix-Modus-Bits auf folgende Weise:

Wenn das Schreibschutzbit für eine Datei gesetzt ist:

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

Wenn das Schreibschutzbit für eine Datei nicht gesetzt ist:

- ONTAP bestimmt den Zugriff basierend auf den ACL- und 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-Modus-Bits den Schreibzugriff verweigern, können NFS- und SMB-Clients die Datei ändern.

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

Erfahren Sie, wie sich ONTAP NFS und Windows bei der Handhabung von Sperren für Share-Path-Komponenten unterscheiden

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

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

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

Erfahren Sie mehr über "So verhindern Sie, dass Verzeichnisse umbenannt werden, während Clients auf sie zugreifen".

Informationen zu Sperren für ONTAP NFS SVMs anzeigen

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

Über diese Aufgabe

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

Standardmäßig werden mit dem Befehl Informationen zu allen Sperren angezeigt. Mit den Befehlsparametern

können Informationen über Sperren für eine bestimmte Storage Virtual Machine (SVM) angezeigt oder die Ausgabe des Befehls nach anderen Kriterien gefiltert werden.

Mit dem `vserver locks show` Befehl werden Informationen zu vier Arten von Sperren angezeigt:

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

Durch die Angabe optionaler Parameter können Sie wichtige Informationen zu jedem Sperrtyp ermitteln. Erfahren Sie mehr über `vserver locks show` in der "ONTAP-Befehlsreferenz".

Schritt

1. Mit dem `vserver locks show` Befehl werden Informationen über Sperren angezeigt.

Beispiele

Das folgende Beispiel zeigt zusammenfassende Informationen für eine NFSv4-Sperre auf einer Datei mit dem Pfad an `/vol1/file1`. Der Zugriffsmodus für sharlock ist write-Deny_none, und die Sperre wurde mit der Schreibdelegation gewährt:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
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 über die SMB-Sperre in einer Datei mit dem Pfad `/data2/data2_2/intro.pptx`. Ein dauerhafter Handle wird auf der Datei mit einem Zugriffsmodus für die Freigabesperre von write-Deny_none einem Client mit einer IP-Adresse von 10.3.1.3 gewährt. Ein Lease Oplock wird mit einem Batch-Oplock-Niveau gewährt:

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

                  Vserver: vs1
                   Volume: data2_2
        Logical Interface: lif2
              Object Path: /data2/data2_2/intro.pptx
                Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
            Lock Protocol: cifs
                Lock Type: share-level
   Node Holding Lock State: node3
```

```
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

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

Aufheben von Dateisperren für ONTAP NFS SVMs

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

Über diese Aufgabe

Der `vserver locks break` Befehl ist nur auf der erweiterten Berechtigungsebene und höher verfügbar. Erfahren Sie mehr über `vserver locks break` in der "ONTAP-Befehlsreferenz".

Schritte

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

   Erfahren Sie mehr über `vserver locks show` in der "ONTAP-Befehlsreferenz".

2. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

3. Führen Sie eine der folgenden Aktionen aus:

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

4. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Erfahren Sie, wie ONTAP FPolicy First-Read- und First-Write-Filter mit NFS funktionieren

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

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

Anforderungen erzeugt werden, kann dies zu folgenden Problemen führen:

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

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

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

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

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

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

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

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

Ändern Sie die NFSv4.1-Serverimplementierungs-ID für ONTAP SVMs

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

Über diese Aufgabe

Die Standardwerte für die drei Optionen lauten wie folgt:

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

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie die NFSv4.1 Implementierungs-ID ändern möchten…	Geben Sie den Befehl ein…
Domäne	`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 Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Managen Sie NFSv4-ACLs

Erfahren Sie mehr über die Vorteile der Aktivierung von NFSv4-ACLs für ONTAP SVMs

Die Aktivierung von NFSv4-ACLs bietet viele Vorteile.

Die Aktivierung von NFSv4-ACLs bietet folgende Vorteile:

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

Erfahren Sie mehr über NFSv4-ACLs für ONTAP SVMs

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

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

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

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

- Wenn die Anforderung nur standardmäßige UNIX-Dateizugriffsberechtigungen enthält und das übergeordnete Verzeichnis keine ACL besitzt, wird der Client-Dateimodus verwendet, um standardmäßige UNIX-Dateizugriffsberechtigungen festzulegen.
- Wenn die Anforderung nur Standardberechtigungen für den UNIX-Dateizugriff enthält und das übergeordnete Verzeichnis über eine nicht vererbbare ACL verfügt, wird das neue Objekt nur mit Modus-Bits erstellt.

Wenn der `-chown-mode` Parameter `restricted` mit Befehlen in den `vserver nfs` oder-`vserver export-policy rule`Familien auf gesetzt wurde, kann die Dateieigentümerschaft nur vom Superuser geändert werden, selbst wenn die mit NFSv4-ACLs festgelegten Berechtigungen auf der Festplatte einem nicht-Root-Benutzer erlauben, die Dateieigentümerschaft zu ändern. Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "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 erhält, wird die ACL standardmäßig beibehalten und geändert, um die Änderung des Modus-Bits widerzuspiegeln. Sie können den `-v4-acl-preserve` Parameter zum Ändern des Verhaltens deaktivieren, wenn Sie stattdessen die ACL entfernen möchten.

Über diese Aufgabe

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

Die Standardeinstellung für diesen Parameter ist aktiviert.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

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

3. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Erfahren Sie, wie ONTAP NFSv4-ACLs verwendet, um zu bestimmen, ob Dateien gelöscht werden können.

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

Aktivieren oder Deaktivieren von NFSv4-ACLs für ONTAP SVMs

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

Über diese Aufgabe

Die `-v4.0-acl -v4.1-acl` Option oder steuert die Einstellung und Anzeige von NFSv4-ACLs; sie kontrolliert nicht die Durchsetzung dieser ACLs zur Zugriffsprüfung.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Dann…
Aktivieren Sie NFSv4.0 ACLs	Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`

Deaktivieren Sie NFSv4.0 ACLs	Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
Aktivieren Sie NFSv4.1 ACLs	Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`
Deaktivieren Sie NFSv4.1 ACLs	Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

Ändern Sie das maximale ACE-Limit für NFSv4-ACLs für ONTAP SVMs

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

Über diese Aufgabe

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

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   `set -privilege advanced`

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

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

   Der gültige Bereich von

   `max_ace_limit` Ist `192` an `1024`.

3. Zurück zur Administratorberechtigungsebene:

   `set -privilege admin`

Managen der NFSv4-Dateidelegationen

Aktivieren oder Deaktivieren von NFSv4-Lesedateidelegierungen für ONTAP SVMs

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

Über diese Aufgabe

Standardmäßig sind Lesedatei-Delegationen deaktiviert.

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

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

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

Ergebnis

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

Aktivieren oder Deaktivieren von NFSv4-Schreibdateidelegierungen für ONTAP SVMs

Zum Aktivieren oder Deaktivieren der Dateidelegationen können Sie die `-v4.0-write -delegation`Option oder ändern. Durch die Aktivierung von Write-File-Delegationen

können Sie einen Großteil des Nachrichtenüberaufwands, der mit der Datei- und Datensatzsperrung verbunden ist, sowie das Öffnen und Schließen von Dateien eliminieren.

Über diese Aufgabe

Standardmäßig sind die Delegierungen der Schreibledatei deaktiviert.

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

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Dann…
Aktivieren Sie NFSv4-Schreibdateidelegationen	Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled`
Aktivieren Sie NFSv4.1-Schreibdateidelegationen	Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled`
Deaktivieren Sie NFSv4 „Write File Delegationen“	Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled`
Deaktivieren Sie NFSv4.1 „Write File Delegationen“	Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled`

Ergebnis

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

Konfigurieren der NFSv4-Datei und der Datensatzsperrung

Erfahren Sie mehr über NFSv4-Datei- und Datensatzsperren für ONTAP SVMs

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

"Technischer Bericht von NetApp 3580: NFSv4 Enhancements and Best Practices Guide Data ONTAP Implementation"

Geben Sie die NFSv4-Sperr-Lease-Periode für ONTAP SVMs an

Um den Leasing-Zeitraum für die NFSv4-Sperrung anzugeben (d. h. den Zeitraum, in dem ONTAP einem Client unwiderruflich eine Sperre gewährt), können Sie die `-v4-lease-seconds` Option ändern. Durch kürzere Leasing-Zeiten wird die Server-Recovery beschleunigt, während längere Leasing-Zeiten für Server mit einer sehr großen Anzahl von Clients von Vorteil sind.

Über diese Aufgabe

Standardmäßig ist diese Option auf eingestellt `30`. Der Mindestwert für diese Option ist `10`. Der maximale Wert für diese Option ist die Sperrfrist, die Sie mit der `locking.lease_seconds` Option einstellen können.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Geben Sie den folgenden Befehl ein:

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

3. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Festlegen der NFSv4-Sperrfrist für ONTAP SVMs

Um die NFSv4-Sperrfrist (d. h. den Zeitraum, in dem Clients versuchen, während der Serverwiederherstellung ihren Sperrstatus aus ONTAP zurückzugewinnen) anzugeben, können Sie die `-v4-grace-seconds` Option ändern.

Über diese Aufgabe

Standardmäßig ist diese Option auf eingestellt `45`.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Geben Sie den folgenden Befehl ein:

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

3. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Erfahren Sie mehr über NFSv4-Empfehlungen für ONTAP SVMs

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

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

Aktivieren oder Deaktivieren von NFSv4-Verweise für ONTAP SVMs

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

Bevor Sie beginnen

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

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

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

Deaktivieren Sie NFSv4.1 Empfehlungen	`vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled`

3. Zurück zur Administratorberechtigungsebene:

   `set -privilege admin`

Statistiken für ONTAP NFS SVMs anzeigen

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

Schritte

1. Verwenden Sie den `statistics catalog object show` Befehl, um die NFS-Objekte zu identifizieren, aus denen Sie Daten anzeigen können.

   `statistics catalog object show -object nfs*`

2. Verwenden Sie die `statistics start` `statistics stop` Befehle und optional, um ein Datenbeispiel von einem oder mehreren Objekten zu erfassen.
3. `statistics show`Die Beispieldaten mit dem Befehl anzeigen.

Beispiel: Monitoring der NFSv3 Performance

Das folgende Beispiel zeigt die Performance-Daten für das NFSv3-Protokoll.

Mit dem folgenden Befehl wird die Datenerfassung für einen neuen Probe gestartet:

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

Der folgende Befehl zeigt die Daten aus der Probe an, indem Zähler angegeben werden, die die Anzahl der erfolgreichen Lese- und Schreibanforderungen gegenüber der Gesamtzahl der Lese- und Schreibanforderungen anzeigen:

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                     Value
    -------------------------- ----------------------------
    read_success                                40042
    read_total                                  40042
    write_success                             1492052
    write_total                               1492052
```

Verwandte Informationen

- "Einrichtung der Performance-Überwachung"
- "Statistik Katalog Objekt anzeigen"
- "Statistiken zeigen"
- "Statistikstart"
- "Statistikstopp"

DNS-Statistiken für ONTAP NFS SVMs anzeigen

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

Schritte

1. `statistics catalog object show`Identifizieren Sie mit dem Befehl die DNS-Objekte, aus denen Sie Daten anzeigen können.

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

2. Verwenden Sie die `statistics start` `statistics stop` Befehle und, um ein Datenbeispiel von einem oder mehreren Objekten zu erfassen.
3. `statistics show`Die Beispieldaten mit dem Befehl anzeigen.

Überwachen der DNS-Statistiken

Die folgenden Beispiele zeigen Performance-Daten für DNS-Abfragen. Die folgenden Befehle starten die Datenerfassung für eine neue Probe:

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

Mit dem folgenden Befehl werden die Daten aus der Probe angezeigt, indem Sie Zähler angeben, die die Anzahl der gesendeten DNS-Abfragen im Vergleich zur Anzahl der empfangenen, fehlgeschlagenen oder Timeout-DNS-Abfragen anzeigen:

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            0
    num_requests_sent                                               1
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

Mit dem folgenden Befehl werden Daten aus der Probe angezeigt, indem Zähler angegeben werden, die die Anzahl der Male anzeigen, die ein bestimmter Fehler für eine DNS-Abfrage auf dem jeweiligen Server empfangen wurde:

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                             NXDOMAIN
    server_ip_address                                   10.72.219.109
3 entries were displayed.
```

Verwandte Informationen

- "Einrichtung der Performance-Überwachung"
- "Statistik Katalog Objekt anzeigen"
- "Statistiken zeigen"
- "Statistikstart"
- "Statistikstopp"

NIS-Statistiken für ONTAP NFS SVMs anzeigen

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

Schritte

1. Verwenden Sie den `statistics catalog object show` Befehl, um die NIS-Objekte zu identifizieren, aus denen Sie Daten anzeigen können.

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

2. Verwenden Sie die `statistics start` `statistics stop` Befehle und, um ein Datenbeispiel von einem oder mehreren Objekten zu erfassen.
3. `statistics show`Die Beispieldaten mit dem Befehl anzeigen.

Überwachen der NIS-Statistiken

In den folgenden Beispielen werden Performancedaten für NIS-Abfragen angezeigt. Die folgenden Befehle starten die Datenerfassung für eine neue Probe:

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

Mit dem folgenden Befehl werden die Daten aus der Probe angezeigt, indem Sie Zähler angeben, die die Anzahl der gesendeten NIS-Abfragen im Vergleich zur Anzahl der empfangenen, fehlgeschlagenen oder Zeitüberschreitung bei NIS-Abfragen anzeigen:

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            1
    num_requests_sent                                               2
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

Mit dem folgenden Befehl werden Daten aus der Probe angezeigt, indem Zähler angegeben werden, die die Anzahl der Male anzeigen, an denen ein bestimmter Fehler bei einer NIS-Abfrage auf dem jeweiligen Server empfangen wurde:

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                           YP_NOTFOUND
    server_ip_address                                   10.227.13.221
3 entries were displayed.
```

Verwandte Informationen

- "Einrichtung der Performance-Überwachung"
- "Statistik Katalog Objekt anzeigen"
- "Statistiken zeigen"
- "Statistikstart"
- "Statistikstopp"

Erfahren Sie mehr über die Unterstützung für VMware vStorage über ONTAP NFS

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

Unterstützte Funktionen

Folgende Funktionen werden unterstützt:

- Copy-Offload

  Ermöglicht es einem ESXi Host, Virtual Machines oder Virtual Machine Disks (VMDKs) direkt zwischen dem Quell- und Zielspeicherort zu kopieren, ohne den Host zu involvieren. Dies spart ESXi Host-CPU-Zyklen und Netzwerkbandbreite. Der Copy-Offload behält die Platzeffizienz bei, wenn das Quell-Volume nur wenige Ressourcen beansprucht.

- Speicherplatzreservierung

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

Einschränkungen

VMware vStorage via NFS weist folgende Einschränkungen auf:

- Offload-Vorgänge für Kopien können in den folgenden Szenarien fehlschlagen:
  - Während der Ausführung von Wafliron auf dem Quell- oder Ziel-Volume, da es das Volume vorübergehend offline nimmt
  - Während Sie das Quell- oder Ziel-Volume verschieben
  - Während Sie die Quell- oder Ziel-LIF verschieben
  - Während der Durchführung von Takeover- oder Giveback-Vorgängen
  - Während Switchover- oder Switchback-Vorgänge durchgeführt werden
- Serverseitige Kopien können aufgrund von Formatunterschieden bei Datei-Handle im folgenden Szenario fehlschlagen:

  Sie versuchen, Daten von SVMs zu kopieren, die derzeit oder zuvor qtrees in SVMs exportiert hatten, die in noch nie qtrees exportiert hatten. Um diese Einschränkung zu umgehen, können Sie mindestens einen qtree auf der Ziel-SVM exportieren.

Verwandte Informationen

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

Aktivieren oder Deaktivieren von VMware vStorage über ONTAP NFS

Sie können `vserver nfs modify` die Unterstützung für VMware vStorage über NFS auf Storage Virtual Machines (SVMs) mit dem Befehl aktivieren oder deaktivieren.

Über diese Aufgabe

Standardmäßig ist die Unterstützung für VMware vStorage via NFS deaktiviert.

Schritte

1. Zeigen Sie den aktuellen vStorage Support-Status für SVMs an:

   ```
   vserver nfs show -vserver vserver_name -instance
   ```

2. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Aktivieren Sie den VMware vStorage Support	`vserver nfs modify -vserver vserver_name -vstorage enabled`
Deaktivieren Sie die VMware vStorage Unterstützung	`vserver nfs modify -vserver vserver_name -vstorage disabled`

Nachdem Sie fertig sind

Bevor Sie diese Funktion nutzen können, müssen Sie das NFS-Plug-in für VMware VAAI installieren. Weitere

Informationen finden Sie unter *Installation des NetApp NFS Plug-ins für VMware VAAI*.

Verwandte Informationen

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

Aktivieren oder Deaktivieren der rquota-Unterstützung auf ONTAP NFS SVMs

Mit dem Remote Quota Protocol (rquota) können NFS-Clients Kontingentinformationen für Benutzer von einem Remote-Computer abrufen. Die Unterstützung für rquota-Versionen hängt von Ihrer Version von ONTAP ab.

- Rquota v1 wird in ONTAP 9 und höher unterstützt.
- Rquota v2 wird ab ONTAP 9.12.1 unterstützt.

  Wenn Sie von rquota v1 auf rquota v2 aktualisieren, stellen Sie möglicherweise eine unerwartete Änderung Ihres Benutzerkontingentlimits fest. Diese Änderung ist auf die unterschiedliche Berechnungsweise der Quote zwischen rquota v1 und rquota v2 zurückzuführen. Weitere Informationen finden Sie im"NetApp Knowledge Base: Warum hat sich das Benutzerkontingentlimit unerwartet geändert?" .

Über diese Aufgabe

Standardmäßig ist rquota deaktiviert.

Schritt

1. Aktivieren oder Deaktivieren von rquota:

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Rquota-Unterstützung für SVMs aktivieren	`vserver nfs modify -vserver vserver_name -rquota enable`
Deaktivieren Sie rquota-Unterstützung für SVMs	`vserver nfs modify -vserver vserver_name -rquota disable`

   Weitere Informationen zu Quoten finden Sie unter "Logisches Storage-Management".

Erfahren Sie mehr über Leistungsverbesserungen bei NFSv3 und NFSv4 sowie die TCP-Übertragungsgröße für ONTAP SVMs

Sie können die Performance von NFSv3- und NFSv4-Clients verbessern, die über ein Netzwerk mit hoher Latenz mit Storage-Systemen verbunden sind, indem Sie die maximale TCP-Übertragungsgröße ändern.

Wenn Clients über ein Netzwerk mit hoher Latenz auf Storage-Systeme zugreifen, z. B. ein Wide Area Network (WAN) oder ein Metro Area Network (MAN) mit einer Latenz über 10 Millisekunden. Können Sie die Verbindungs-Performance möglicherweise verbessern, indem Sie die maximale TCP-Übertragungsgröße ändern. Clients, die in einem Netzwerk mit niedriger Latenz auf Storage-Systeme zugreifen, wie z. B. LAN (Local Area Network), können von der Änderung dieser Parameter kaum oder gar nicht profitieren. Wenn die Durchsatzverbesserung die Auswirkung auf die Latenz nicht überwiegt, sollten Sie diese Parameter nicht verwenden.

Um zu ermitteln, ob Ihre Storage-Umgebung von der Änderung dieser Parameter profitieren würde, sollten Sie zunächst eine umfassende Performance-Bewertung eines NFS-Clients mit schlechter Performance durchführen. Prüfen Sie, ob die geringe Performance auf eine übermäßige Paketumlauflatenz und kleine Anfragen beim Client zurückzuführen ist. Unter diesen Bedingungen können Client und Server die verfügbare Bandbreite nicht vollständig nutzen, da sie die meisten Arbeitszyklen verwenden, die darauf warten, dass kleine Anfragen und Antworten über die Verbindung übertragen werden.

Durch Erhöhung der Anfragegröße für NFSv3 und NFSv4 kann der Client und Server die verfügbare Bandbreite effektiver nutzen, um mehr Daten pro Einheit zu verschieben. Dadurch wird die Gesamteffizienz der Verbindung erhöht.

Beachten Sie, dass die Konfiguration zwischen dem Storage-System und dem Client variieren kann. Das Speichersystem und der Client unterstützen bei Übertragungsvorgängen eine maximale Größe von 1 MB. Wenn Sie jedoch das Speichersystem so konfigurieren, dass es maximal 1 MB Übertragungsgröße unterstützt, aber der Client nur 64 KB unterstützt, ist die Mount-Transfergröße auf 64 KB oder weniger begrenzt.

Bevor Sie diese Parameter ändern, müssen Sie beachten, dass dies zu einem zusätzlichen Speicherverbrauch auf dem Speichersystem für den Zeitraum führt, der für die Montage und Übertragung einer großen Reaktion erforderlich ist. Je mehr latenzarme Verbindungen zum Storage-System, desto höher ist der zusätzliche Speicherverbrauch. Bei Storage-Systemen mit hoher Speicherkapazität kann diese Änderung nur sehr geringe Auswirkungen haben. Bei Storage-Systemen mit niedriger Speicherkapazität kann es zu einer merklichen Verschlechterung der Performance kommen.

Die erfolgreiche Verwendung dieser Parameter hängt von der Fähigkeit ab, Daten von mehreren Nodes eines Clusters abzurufen. Die inhärente Latenz des Cluster-Netzwerks erhöht möglicherweise die gesamte Latenz der Antwort. Die gesamte Latenz erhöht sich bei der Verwendung dieser Parameter normalerweise. Daher können latenzkritische Workloads negative Auswirkungen haben.

Ändern Sie die maximale TCP-Übertragungsgröße für NFSv3 und NFSv4 für ONTAP SVMs

Sie können die `-tcp-max-xfer-size` Option ändern, um die maximale Übertragungsgröße für alle TCP-Verbindungen mithilfe der Protokolle NFSv3 und NFSv4.x zu konfigurieren.

Über diese Aufgabe

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

Ab ONTAP 9 `v3-tcp-max-read-size` `v3-tcp-max-write-size` sind die Optionen und veraltet. Sie müssen `-tcp-max-xfer-size` stattdessen die Option verwenden.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Ändern Sie die maximale Übertragungsgröße von NFSv3 oder NFSv4 TCP	`vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size`

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

Die maximale Übertragungsgröße, die Sie eingeben, muss ein Vielfaches von 4 KB (4096 Byte) sein. Anfragen, die nicht richtig ausgerichtet sind, wirken sich negativ auf die Performance aus.

3. `vserver nfs show -fields tcp-max-xfer-size`Überprüfen Sie die Änderungen mit dem Befehl.
4. Wenn Clients statische Mounts verwenden, heben Sie die Bereitstellung ab und montieren Sie sie neu, damit die neue Parametergröße wirksam wird.

Beispiel

Mit dem folgenden Befehl wird die maximale Übertragungsgröße von NFSv3 und NFSv4.x TCP auf 1048576 Byte auf der SVM mit dem Namen vs1 festgelegt:

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

Konfigurieren Sie die Anzahl der für NFS-Benutzer zulässigen Gruppen-IDs für ONTAP SVMs

Standardmäßig unterstützt ONTAP bis zu 32 Gruppen-IDs beim Umgang mit NFS-Anmeldedaten über Kerberos (RPCSEC_GSS) Authentifizierung. Bei Verwendung der AUTH_SYS-Authentifizierung beträgt die standardmäßige maximale Anzahl von Gruppen-IDs 16, wie in RFC 5531 definiert. Sie können das Maximum auf 1,024 erhöhen, wenn Sie Benutzer haben, die mehr als die Standardanzahl von Gruppen sind.

Über diese Aufgabe

Wenn ein Benutzer mehr als die Standardanzahl von Gruppen-IDs in seinen Anmeldedaten hat, werden die übrigen Gruppen-IDs abgeschnitten und der Benutzer erhält beim Versuch, auf Dateien vom Speichersystem zuzugreifen, möglicherweise Fehler. Sie sollten die maximale Anzahl an Gruppen pro SVM auf eine Zahl festlegen, die die maximalen Gruppen in Ihrer Umgebung repräsentiert.

Um die AUTH_SYS-Authentifizierungsvoraussetzungen für die Aktivierung erweiterter Gruppen zu verstehen(`-auth-sys-extended-groups`), die Gruppen-IDs über das Standardmaximum von 16 hinaus verwenden, finden Sie im"NetApp Knowledge Base: Was sind die Voraussetzungen für die Aktivierung von auth-sys-extended-groups?"

In der folgenden Tabelle werden die beiden Parameter des `vserver nfs modify` Befehls aufgeführt, mit denen die maximale Anzahl von Gruppen-IDs in drei Beispielkonfigurationen festgelegt wird:

Parameter	Einstellungen	Resultierende Gruppen-IDs Limit

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`32`
	
	`disabled`
	
	Dies sind die Standardeinstellungen.
		RPCSEC_GSS: 32
		
		AUTH_SYS: 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`256`
	
	`disabled`
		RPCSEC_GSS: 256
		
		AUTH_SYS: 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`512`
	
	`enabled`
		RPCSEC_GSS: 512
		
		AUTH_SYS: 512

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Führen Sie die gewünschte Aktion aus:

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

3. Überprüfen Sie den `-extended-groups-limit` Wert und überprüfen Sie, ob AUTH_SYS erweiterte Gruppen verwendet: `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`

4. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

Beispiel

Das folgende Beispiel ermöglicht erweiterte Gruppen für die AUTH_SYS-Authentifizierung und setzt die maximale Anzahl erweiterter Gruppen für AUTH_SYS- und RPCSEC_GSS-Authentifizierung auf 512. Diese Änderungen werden nur für Clients vorgenommen, die auf die SVM mit dem Namen vs1 zugreifen:

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

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
------- ------------------------ ---------------------
vs1     enabled                  512

vs1::*> set -privilege admin
```

Verwandte Informationen

- "NetApp Knowledge Base: AUTH_SYS Extended Groups-Änderungen für die NFS-Authentifizierung für ONTAP 9"

Kontrollieren Sie den Root-Benutzerzugriff auf Daten im NTFS-Sicherheitsstil für ONTAP SVMs

Sie können ONTAP so konfigurieren, dass NFS-Clients Zugriff auf NTFS-Sicherheitsdaten und NTFS-Clients auf die Daten im NFS-Sicherheitsstil erhalten. Wenn Sie den NTFS-Sicherheitsstil bei einem NFS-Datenspeicher verwenden, müssen Sie entscheiden, wie der Root-Benutzer den Zugriff behandelt und die SVM (Storage Virtual Machine) entsprechend konfiguriert.

Über diese Aufgabe

Wenn ein Root-Benutzer auf NTFS-Sicherheitsdaten zugreift, haben Sie zwei Optionen:

- Ordnen Sie den Root-Benutzer wie jeder andere NFS-Benutzer einem Windows-Benutzer zu und verwalten Sie den Zugriff nach NTFS ACLs.
- Ignorieren Sie NTFS ACLs und bieten Sie vollständigen Zugriff auf das Root.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Führen Sie die gewünschte Aktion aus:

Wenn der Root-Benutzer…	Geben Sie den Befehl ein…
Werden einem Windows-Benutzer zugeordnet	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled`
Umgehen Sie die NT-ACL-Prüfung	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled`

   Dieser Parameter ist standardmäßig deaktiviert.

   Wenn dieser Parameter aktiviert ist, aber keine Namenszuweisung für den Root-Benutzer vorhanden ist, verwendet ONTAP für die Prüfung eine standardmäßige SMB-Administratoranmeldungs-Berechtigung.

3. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```