Konfiguration des NFS-Zugriffs auf eine SVM

ONTAP 9

NetApp
October 08, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/nfs-config/create-svms-data-access-task.html on October 08, 2026. Always check docs.netapp.com for the latest.

Inhalt

Konfiguration des NFS-Zugriffs auf eine SVM . . . 1
- ONTAP SVMs für den NFS-Datenzugriff erstellen . . . 1
- Überprüfung der Aktivierung des NFS-Protokolls auf der ONTAP SVM . . . 2
- NFS-Client-Zugriff auf der ONTAP SVM öffnen . . . 3
- ONTAP NFS-Server erstellen . . . 4
- ONTAP NFS LIFs erstellen . . . 6
- DNS für die ONTAP NFS SVM-Hostnamensauflösung aktivieren . . . 10
- Namensdienste konfigurieren . . . 12
  - Informationen zu ONTAP NFS Namensdiensten . . . 12
  - Die ONTAP NFS Name-Service-Switch-Tabelle konfigurieren . . . 12
- Lokale UNIX-Benutzer und Gruppen konfigurieren . . . 13
  - Informationen zu lokalen UNIX-Benutzern und -Gruppen für ONTAP NFS SVMs . . . 13
  - Lokale UNIX-Benutzer auf ONTAP NFS SVMs erstellen . . . 13
  - Lokale UNIX-Benutzer aus URIs auf ONTAP NFS SVMs laden . . . 14
  - Lokale UNIX-Gruppen auf ONTAP NFS SVMs erstellen . . . 15
  - Benutzer zur lokalen UNIX-Gruppe auf ONTAP NFS SVMs hinzufügen . . . 15
  - Lokale UNIX-Gruppen von URIs auf ONTAP NFS SVMs laden . . . 16
- Mit Netzwerkgruppen arbeiten . . . 17
  - Informationen zu Netgroups auf ONTAP NFS SVMs . . . 17
  - Netzgruppen von URIs auf ONTAP NFS SVMs laden . . . 18
  - ONTAP NFS SVM-Netzgruppendefinitionen überprüfen . . . 19
  - NIS-Domänenkonfigurationen für ONTAP NFS SVMs erstellen . . . 20
- LDAP verwenden . . . 21
  - Informationen zur Verwendung von LDAP-Name-Services auf ONTAP NFS SVMs . . . 21
  - Neue LDAP-Client-Schemas für ONTAP NFS SVMs erstellen . . . 23
  - LDAP-Client-Konfigurationen für ONTAP NFS-Zugriff erstellen . . . 24
  - LDAP-Client-Konfigurationen mit ONTAP NFS SVMs verknüpfen . . . 28
  - LDAP-Quellen für ONTAP NFS SVMs verifizieren . . . 29
- Kerberos mit NFS für hohe Sicherheit verwenden . . . 29
  - Informationen zur Verwendung von Kerberos mit ONTAP NFS für eine starke Authentifizierung . . . 30
  - UNIX-Berechtigungen für NFS-Kerberos-Konfigurationen auf ONTAP SVMs überprüfen . . . 30
  - Erstellen von NFS Kerberos Realm-Konfigurationen auf ONTAP SVMs . . . 32
  - NFS-Kerberos zulässige Verschlüsselungstypen für ONTAP SVMs konfigurieren . . . 33
  - NFS Kerberos auf ONTAP LIFs aktivieren . . . 35

Konfiguration des NFS-Zugriffs auf eine SVM

ONTAP SVMs für den NFS-Datenzugriff erstellen

Wenn sich in einem Cluster noch keine SVM befindet, die NFS-Clients den Datenzugriff bereitstellt, ist eine SVM zu erstellen.

Bevor Sie beginnen

- Ab ONTAP 9.13.1 kann eine maximale Kapazität für eine Storage-VM festgelegt werden. Es besteht außerdem die Möglichkeit, Warnmeldungen zu konfigurieren, wenn die SVM einen Schwellenwert für die Kapazität erreicht. Weitere Informationen finden sich unter SVM Kapazität verwalten.

Schritte

1. Eine SVM erstellen:

   `vserver create -vserver` *`vserver_name`* `-rootvolume` *`root_volume_name`* `-aggregate` *`aggregate_name`* `-rootvolume-security-style unix -language C.UTF-8 -ipspace` *`ipspace_name`*

   - Die UNIX-Einstellung für die `-rootvolume-security-style` Option verwenden.
   - Die Standardoption C.UTF-8 `-language` kann verwendet werden.
   - Die `ipspace` Einstellung ist optional.

2. Die Konfiguration und der Status der neu erstellten SVM können überprüft werden:

   `vserver show -vserver` *`vserver_name`*

   Das `Allowed Protocols` Feld muss NFS enthalten. Diese Liste kann später bearbeitet werden.

   Das `Vserver Operational State`Feld muss den `running`Status anzeigen. Wenn es den `initializing`Status anzeigt, bedeutet dies, dass ein Zwischenvorgang wie die Erstellung des Root-Volumes fehlgeschlagen ist und die SVM gelöscht und neu erstellt werden muss.

Beispiele

Der folgende Befehl erstellt eine SVM für den Datenzugriff im IPspace ipspaceA:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

Der folgende Befehl zeigt, dass eine SVM mit einem Root-Volume von 1 GB erstellt wurde, das automatisch gestartet wurde und sich im `running` Status befindet. Das Root-Volume verfügt über eine Standard-Export-Richtlinie, die keine Regeln enthält, sodass das Root-Volume bei der Erstellung nicht exportiert wird.

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                                Vserver Type: data
                             Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                                Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                         Vserver Admin State: running
                   Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                           Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                        Disallowed Protocols: -
                            QoS Policy Group: -
                                 Config Lock: false
                                IPspace Name: ipspaceA
```

Ab ONTAP 9.13.1 kann eine adaptive QoS-Richtliniengruppenvorlage festgelegt werden, die eine Durchsatzuntergrenze und eine Obergrenze für Volumes in der SVM anwendet. Diese Richtlinie kann erst nach der Erstellung der SVM angewendet werden. Weitere Informationen zu diesem Vorgang finden sich unter Eine adaptive Richtliniengruppenvorlage festlegen.

Überprüfung der Aktivierung des NFS-Protokolls auf der ONTAP SVM

Bevor Sie NFS auf SVMs konfigurieren und verwenden können, muss überprüft werden, ob das Protokoll aktiviert ist.

Über diese Aufgabe

Dies geschieht üblicherweise während der SVM-Einrichtung, aber wenn das Protokoll während der Einrichtung nicht aktiviert wurde, kann es später mit dem `vserver add-protocols` Befehl aktiviert werden.

Sobald ein LIF erstellt wurde, kann kein Protokoll mehr hinzugefügt oder entfernt werden.

Protokolle auf SVMs lassen sich auch mit dem `vserver remove-protocols` Befehl deaktivieren.

Schritte

1. Es kann überprüft werden, welche Protokolle für die SVM aktuell aktiviert und deaktiviert sind:

   `vserver show -vserver vserver_name -protocols`

   Der `vserver show-protocols`Befehl kann ebenfalls verwendet werden, um die aktuell auf allen SVMs im Cluster aktivierten Protokolle anzuzeigen.

2. Gegebenenfalls kann ein Protokoll aktiviert oder deaktiviert werden:
   - Zum Aktivieren des NFS-Protokolls:
     `vserver add-protocols -vserver vserver_name -protocols nfs`
   - Ein Protokoll kann deaktiviert werden:
     `vserver remove-protocols -vserver vserver_name -protocols protocol_name [,protocol_name,…]`
3. Es wird bestätigt, dass die aktivierten und deaktivierten Protokolle korrekt aktualisiert wurden:

   `vserver show -vserver vserver_name -protocols`

Beispiel

Der folgende Befehl zeigt, welche Protokolle auf der SVM mit dem Namen vs1 aktuell aktiviert und deaktiviert (zugelassen und nicht zugelassen) sind:

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    -----------------------
vs1.example.com   nfs                       cifs, fcp, iscsi, ndmp
```

Der folgende Befehl ermöglicht den Zugriff über NFS, indem `nfs` zur Liste der aktivierten Protokolle auf der SVM mit dem Namen vs1 hinzugefügt wird:

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

NFS-Client-Zugriff auf der ONTAP SVM öffnen

Die Standardexportrichtlinie des SVM-Root-Volumes muss eine Regel enthalten, die allen Clients den offenen Zugriff über NFS ermöglicht. Ohne eine solche Regel wird allen NFS-Clients der Zugriff auf die SVM und ihre Volumes verweigert.

Über diese Aufgabe

Wenn eine neue SVM erstellt wird, wird automatisch eine Standard-Exportregel (genannt default) für das Root-Volume der SVM erstellt. Es müssen eine oder mehrere Regeln für die Standard-Exportregel erstellt werden, bevor Clients auf Daten auf der SVM zugreifen können.

Es empfiehlt sich zu überprüfen, ob der Zugriff für alle NFS-Clients in der Standard-Exportregel offen ist; anschließend kann der Zugriff auf einzelne Volumes eingeschränkt werden, indem benutzerdefinierte Exportregeln für einzelne Volumes oder qtrees erstellt werden.

Schritte

1. Wenn Sie eine vorhandene SVM verwenden, überprüfen Sie die Standard-Exportregel für das Root-Volume:

   ```
   vserver export-policy rule show
   ```

   Die Ausgabe des Befehls sollte in etwa wie folgt aussehen:

   ```
   cluster::> vserver export-policy rule show -vserver vs1.example.com
   -policyname default -instance

                                      Vserver: vs1.example.com
                                  Policy Name: default
                                   Rule Index: 1
                              Access Protocol:  nfs
   Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                                RO Access Rule: any
                                RW Access Rule: any
   User ID To Which Anonymous Users Are Mapped: 65534
                     Superuser Security Types: any
                 Honor SetUID Bits in SETATTR: true
                    Allow Creation of Devices: true
   ```

   Existiert eine solche Regel, die offenen Zugang erlaubt, ist diese Aufgabe abgeschlossen. Falls nicht, folgt der nächste Schritt.

2. Eine Exportregel für das SVM-Root-Volume erstellen:

   ```
   vserver export-policy rule create -vserver vserver_name -policyname default
   -ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any
   -superuser any
   ```

   Wenn die SVM nur Volumes enthält, die durch Kerberos gesichert sind, können die Exportregeloptionen `-rorule`, `-rwrule` und `-superuser` für das Root-Volume auf `krb5` oder `krb5i` gesetzt werden. Beispiel:

   ```
   -rorule krb5i -rwrule krb5i -superuser krb5i
   ```

3. Die Regelerstellung kann mithilfe des `vserver export-policy rule show` Befehls überprüft werden.

Ergebnis

Jeder NFS-Client kann nun auf jedes Volume oder jeden Qtree zugreifen, der auf der SVM erstellt wurde.

ONTAP NFS-Server erstellen

Nachdem überprüft wurde, dass NFS auf Ihrem Cluster lizenziert ist, kann mit dem `vserver nfs create` Befehl ein NFS-Server auf der SVM erstellt und die unterstützten NFS-Versionen angegeben werden.

Über diese Aufgabe

Die SVM kann so konfiguriert werden, dass eine oder mehrere Versionen von NFS unterstützt werden. Falls NFSv4 oder höher unterstützt wird:

- Der Domänenname für die NFSv4-Benutzer-ID-Zuordnung muss auf dem NFSv4-Server und den Ziel-Clients identisch sein.

  Es muss nicht unbedingt mit einem LDAP- oder NIS-Domänennamen übereinstimmen, solange der NFSv4-Server und die Clients denselben Namen verwenden.

- Zielclients müssen die NFSv4-Einstellung für numerische IDs unterstützen.
- Aus Sicherheitsgründen empfiehlt sich in NFSv4-Bereitstellungen die Verwendung von LDAP für Namensdienste.

Bevor Sie beginnen

Die SVM muss so konfiguriert sein, dass das NFS-Protokoll zulässig ist.

Schritte

1. Es sollte überprüft werden, ob NFS auf Ihrem Cluster lizenziert ist:

   ```
   system license show -package nfs
   ```

   Falls dies nicht der Fall ist, kontaktieren Sie Ihren Vertriebsmitarbeiter.

2. Einen NFS-Server erstellen:

   ```
   vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0
   {enabled|disabled} -v4-id-domain nfsv4_id_domain -v4-numeric-ids
   {enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
   ```

   Sie können beliebige Kombinationen von NFS-Versionen aktivieren. Wenn pNFS unterstützt werden soll, müssen sowohl `-v4.1` als auch `-v4.1-pnfs` Optionen aktiviert werden.

   Wenn Sie Version 4 oder höher aktivieren, sollte außerdem sichergestellt sein, dass die folgenden Optionen korrekt eingestellt sind:

   - `-v4-id-domain`

     Dieser optionale Parameter legt den Domänenanteil der Zeichenfolgenform von Benutzer- und Gruppennamen gemäß dem NFSv4-Protokoll fest. Standardmäßig verwendet ONTAP die NIS-Domäne, sofern eine konfiguriert ist; andernfalls wird die DNS-Domäne verwendet. Es ist ein Wert anzugeben, der mit dem von den Zielclients verwendeten Domänennamen übereinstimmt.

   - `-v4-numeric-ids`

     Dieser optionale Parameter legt fest, ob die Unterstützung für numerische Zeichenfolgenbezeichner in NFSv4-Besitzerattributen aktiviert ist. Die Standardeinstellung ist aktiviert, jedoch sollte überprüft werden, ob die Zielclients dies unterstützen.

   Zusätzliche NFS-Funktionen lassen sich später mit dem `vserver nfs modify` Befehl aktivieren.

3. Es sollte überprüft werden, ob NFS ausgeführt wird:

```
vserver nfs status -vserver vserver_name
```

4. Es sollte überprüft werden, ob NFS wie gewünscht konfiguriert ist:

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

Beispiele

Der folgende Befehl erstellt einen NFS-Server auf der SVM namens vs1 mit aktivierten NFSv3 und NFSv4.0:

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id
-domain my_domain.com
```

Die folgenden Befehle überprüfen den Status und die Konfigurationswerte des neuen NFS-Servers mit dem Namen vs1:

```
vs1::> vserver nfs status -vserver vs1
The NFS server is running on Vserver "vs1".

vs1::> vserver nfs show -vserver vs1

                              Vserver: vs1
                 General NFS Access: true
                              NFS v3: enabled
                            NFS v4.0: enabled
                         UDP Protocol: enabled
                         TCP Protocol: enabled
                Default Windows User: -
                 NFSv4.0 ACL Support: disabled
    NFSv4.0 Read Delegation Support: disabled
   NFSv4.0 Write Delegation Support: disabled
             NFSv4 ID Mapping Domain: my_domain.com
...
```

ONTAP NFS LIFs erstellen

Eine LIF ist eine IP-Adresse, die einem physischen oder logischen Port zugeordnet ist. Bei einem Komponentenausfall kann eine LIF auf einen anderen physischen Port umgeschaltet oder dorthin migriert werden, wodurch die Kommunikation mit dem Netzwerk aufrechterhalten wird.

Bevor Sie beginnen

- Der zugrunde liegende physische oder logische Netzwerkport muss auf den administrativen `up` Status konfiguriert sein.
- Wenn geplant ist, einen Subnetznamen zu verwenden, um die IP-Adresse und den Netzwerkmaskenwert für ein LIF zuzuweisen, muss das Subnetz bereits existieren.

Subnetze enthalten einen Pool von IP-Adressen, die zum selben Layer-3-Subnetz gehören. Sie werden mit dem `network subnet create` Befehl erstellt.

Weitere Informationen zu `network subnet create` finden sich in der "ONTAP-Befehlsreferenz".

- Der Mechanismus zur Festlegung des von einem LIF verarbeiteten Datenverkehrstyps hat sich geändert. Für ONTAP 9.5 und frühere Versionen verwendeten LIFs Rollen, um den Typ des zu verarbeitenden Datenverkehrs festzulegen. Ab ONTAP 9.6 verwenden LIFs Dienstrichtlinien, um den Typ des zu verarbeitenden Datenverkehrs festzulegen.

Über diese Aufgabe

- Sowohl IPv4- als auch IPv6-LIFs können auf demselben Netzwerkport erstellt werden.
- Wenn die Kerberos-Authentifizierung verwendet wird, sollte Kerberos auf mehreren LIFs aktiviert sein.
- Wenn Sie eine große Anzahl von LIFs in Ihrem Cluster haben, kann die vom Cluster unterstützte LIF-Kapazität mit dem `network interface capacity show` Befehl und die von jedem Knoten unterstützte LIF-Kapazität mit dem `network interface capacity details show` Befehl (auf der erweiterten Berechtigungsstufe) überprüft werden.

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

- Ab ONTAP 9.7 ist es nicht mehr nötig, den Heimatport einer LIF anzugeben, wenn bereits andere LIFs für die SVM im selben Subnetz vorhanden sind. ONTAP wählt automatisch einen zufälligen Port auf dem angegebenen Heimatknoten in derselben Broadcast-Domäne wie die anderen bereits im selben Subnetz konfigurierten LIFs.

Ab ONTAP 9.4 wird FC-NVMe unterstützt. Bei der Erstellung einer FC-NVMe LIF sind die folgenden Punkte zu beachten:

- Das NVMe-Protokoll muss vom FC-Adapter unterstützt werden, auf dem die LIF erstellt wird.
- FC-NVMe kann das einzige Datenprotokoll auf Daten-LIFs sein.
- Für jede Storage Virtual Machine (SVM), die SAN unterstützt, muss ein LIF für die Verwaltung des Datenverkehrs konfiguriert werden.
- NVMe LIFs und Namespaces müssen auf demselben Knoten gehostet werden.
- Pro SVM kann nur eine NVMe-LIF für den Datenverkehr konfiguriert werden.

Schritte

1. Eine LIF erstellen:

   ```
   network interface create -vserver vserver_name -lif lif_name -role data -data
   -protocol nfs -home-node node_name -home-port port_name {-address IP_address
   -netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
   -revert {true|false}
   ```

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

Option	Beschreibung

ONTAP 9.5 und älter	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`
ONTAP 9.6 und höher	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`

- Der `-role`Parameter ist nicht erforderlich, wenn eine LIF mithilfe einer Dienstrichtlinie erstellt wird (beginnend mit ONTAP 9.6).
- Der `-data-protocol`Parameter muss bei der Erstellung der LIF angegeben werden und kann später nicht mehr geändert werden, ohne die Daten-LIF zu löschen und neu zu erstellen.

  Der `-data-protocol` Parameter ist nicht erforderlich, wenn eine LIF mithilfe einer Dienstrichtlinie erstellt wird (ab ONTAP 9.6).

- `-home-node` ist der Knoten, zu dem die LIF zurückkehrt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.

  Sie können auch angeben, ob die LIF mit der `-auto-revert` Option automatisch auf den Home-Node und Home-Port zurückkehren soll.

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

- `-home-port` ist der physische oder logische Port, zu dem die LIF zurückkehrt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.
- Sie können eine IP-Adresse mit den `-address` und `-netmask` Optionen angeben oder die Zuweisung aus einem Subnetz mit der `-subnet_name` Option ermöglichen.
- Wird ein Subnetz zur Bereitstellung der IP-Adresse und der Netzwerkmaske verwendet, wird, falls das Subnetz mit einem Gateway definiert wurde, beim Erstellen eines LIF mit diesem Subnetz automatisch eine Standardroute zu diesem Gateway zur SVM hinzugefügt.
- Wenn Sie IP-Adressen manuell zuweisen (ohne Verwendung eines Subnetzes), müssen Sie möglicherweise eine Standardroute zu einem Gateway konfigurieren, falls sich Clients oder Domänencontroller in einem anderen IP-Subnetz befinden. Weitere Informationen zu `network route create` und zum Erstellen einer statischen Route innerhalb einer SVM finden sich im "ONTAP-Befehlsreferenz".
- Für die `-firewall-policy` Option sollte derselbe Standardwert `data` wie für die LIF-Rolle verwendet werden.

  Bei Bedarf kann später eine benutzerdefinierte Firewall-Richtlinie erstellt und hinzugefügt werden.

  Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und vollständig durch LIF-Dienstrichtlinien ersetzt. Weitere Informationen finden sich unter "Firewall-Richtlinien für LIFs konfigurieren".

- `-auto-revert`Hiermit kann festgelegt werden, ob ein Daten-LIF unter Umständen wie Systemstart, Änderungen am Status der Management-Datenbank oder beim Herstellen einer Netzwerkverbindung automatisch auf seinen Heimatknoten zurückkehrt. Die Standardeinstellung ist `false`, sie kann jedoch je nach Netzwerkverwaltungsrichtlinien in Ihrer Umgebung auf `false` gesetzt werden.

  a. Es kann mit dem `network interface show` Befehl überprüft werden, ob die LIF erfolgreich erstellt wurde.

  b. Es sollte überprüft werden, ob die konfigurierte IP-Adresse erreichbar ist:

Zur Überprüfung einer…	Verwenden…
IPv4-Adresse	`network ping`
IPv6-Adresse	`network ping6`

  c. Wenn Sie Kerberos verwenden, sind die Schritte 1 bis 3 zu wiederholen, um zusätzliche LIFs zu erstellen.

     Kerberos muss auf jedem dieser LIFs separat aktiviert werden.

Beispiele

Der folgende Befehl erstellt eine LIF und gibt die Werte für IP-Adresse und Netzwerkmaske mithilfe der `-address` und `-netmask` Parameter an:

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

Der folgende Befehl erstellt eine LIF und weist ihr IP-Adresse und Netzwerkmaskenwerte aus dem angegebenen Subnetz (mit dem Namen client1_sub) zu:

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

Der folgende Befehl zeigt alle LIFs in cluster-1 an. Die Data LIFs datalif1 und datalif3 sind mit IPv4-Adressen konfiguriert, und datalif4 ist mit einer IPv6-Adresse konfiguriert:

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
```

```
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

Der folgende Befehl zeigt, wie ein NAS-Daten-LIF erstellt wird, dem die `default-data-files` Dienstrichtlinie zugewiesen ist:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

Verwandte Informationen

- "Netzwerk-Ping"
- "Netzwerkschnittstelle"

DNS für die ONTAP NFS SVM-Hostnamensauflösung aktivieren

Sie können den `vserver services name-service dns` Befehl verwenden, um DNS auf einer SVM zu aktivieren und sie so zu konfigurieren, dass sie DNS für die Hostnamensauflösung verwendet. Hostnamen werden mithilfe externer DNS-Server aufgelöst.

Bevor Sie beginnen

Für die Auflösung von Hostnamen muss ein standortweiter DNS-Server verfügbar sein.

Es empfiehlt sich, mehr als einen DNS-Server zu konfigurieren, um einen Single Point of Failure zu vermeiden. Der `vserver services name-service dns create` Befehl gibt eine Warnung aus, wenn nur ein DNS-Servername eingegeben wird.

Über diese Aufgabe

Weitere Informationen zu "Konfiguration von dynamischem DNS auf der SVM".

Schritte

1. DNS auf der SVM aktivieren:

   `vserver services name-service dns create -vserver` *`vserver_name`* `-domains` *`domain_name`* `-name-servers` *`ip_addresses`* `-state enabled`

   Der folgende Befehl aktiviert externe DNS-Server auf der SVM vs1:

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   Der `vserver services name-service dns create` Befehl führt eine automatische Konfigurationsprüfung durch und gibt eine Fehlermeldung aus, wenn ONTAP den Nameserver nicht erreichen kann.

2. Die DNS-Domänenkonfigurationen werden mit dem `vserver services name-service dns show` Befehl angezeigt.

   Der folgende Befehl zeigt die DNS-Konfigurationen für alle SVMs im Cluster an:

   ```
   vserver services name-service dns show
                                                Name
   Vserver           State     Domains             Servers
   ----------------- --------- ------------------- -------------
   cluster1          enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   vs1.example.com   enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   ```

   Der folgende Befehl zeigt detaillierte DNS-Konfigurationsinformationen für SVM vs1 an:

   ```
   vserver services name-service dns show -vserver vs1.example.com
                  Vserver: vs1.example.com
                  Domains: example.com
             Name Servers: 192.0.2.201, 192.0.2.202
       Enable/Disable DNS: enabled
   ```

```
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. Der Status der Nameserver kann mit dem `vserver services name-service dns check` Befehl validiert werden.

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

Namensdienste konfigurieren

Informationen zu ONTAP NFS Namensdiensten

Abhängig von der Konfiguration Ihres Speichersystems muss ONTAP Host-, Benutzer-, Gruppen- oder Netzgruppeninformationen abrufen können, um den Clients den korrekten Zugriff zu ermöglichen. Namensdienste müssen so konfiguriert werden, dass ONTAP auf lokale oder externe Namensdienste zugreifen kann, um diese Informationen zu erhalten.

Es empfiehlt sich, einen Namensdienst wie NIS oder LDAP zu verwenden, um Namensauflösungen während der Client-Authentifizierung zu erleichtern. Nach Möglichkeit sollte LDAP für eine höhere Sicherheit eingesetzt werden, insbesondere bei der Bereitstellung von NFSv4 oder höher. Lokale Benutzer und Gruppen sollten ebenfalls konfiguriert werden, falls externe Namensserver nicht verfügbar sind.

Namensdienstinformationen müssen auf allen Quellen synchron gehalten werden.

Die ONTAP NFS Name-Service-Switch-Tabelle konfigurieren

Die Namensdienst-Switchtabelle muss korrekt konfiguriert sein, damit ONTAP lokale oder externe Namensdienste konsultieren kann, um Host-, Benutzer-, Gruppen-, Netzgruppen- oder Namenszuordnungsinformationen abzurufen.

Bevor Sie beginnen

Es muss festgelegt sein, welche Namensdienste für Host-, Benutzer-, Gruppen-, Netzgruppen- oder Namenszuordnung in Ihrer Umgebung verwendet werden sollen.

Wenn die Verwendung von Netgroups vorgesehen ist, müssen alle in Netgroups angegebenen IPv6-Adressen gemäß RFC 5952 gekürzt und komprimiert werden.

Über diese Aufgabe

Geben Sie keine Informationsquellen an, die nicht verwendet werden. Wenn NIS beispielsweise in Ihrer Umgebung nicht verwendet wird, geben Sie die `-sources nis` Option nicht an.

Schritte

1. Die erforderlichen Einträge zur Name-Service-Switch-Tabelle hinzufügen:

   `vserver services name-service ns-switch create -vserver` *`vserver_name`* `-database` *`database_name`* `-sources` *`source_names`*

2. Es sollte sichergestellt werden, dass die Namensdienst-Switch-Tabelle die erwarteten Einträge in der gewünschten Reihenfolge enthält:

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

   Wenn Sie Korrekturen vornehmen möchten, müssen Sie die `vserver services name-service ns-switch modify` oder `vserver services name-service ns-switch delete` Befehle verwenden.

Beispiel

Das folgende Beispiel erstellt einen neuen Eintrag in der Name-Service-Switch-Tabelle für die SVM vs1, sodass die lokale Netgroup-Datei und ein externer NIS-Server in dieser Reihenfolge zur Suche nach Netgroup-Informationen verwendet werden:

```
cluster::> vserver services name-service ns-switch create -vserver vs1
-database netgroup -sources files,nis
```

Nachdem Sie fertig sind

- Die angegebenen Namensdienste müssen für die SVM so konfiguriert werden, dass der Datenzugriff bereitgestellt wird.
- Wenn Sie einen Namendienst für die SVM löschen, müssen Sie ihn auch aus der Namendienst-Switchtabelle entfernen.

  Der Clientzugriff auf das Speichersystem funktioniert möglicherweise nicht wie erwartet, wenn der Namensdienst nicht aus der Namensdienst-Umschalttabelle gelöscht wird.

Lokale UNIX-Benutzer und Gruppen konfigurieren

Informationen zu lokalen UNIX-Benutzern und -Gruppen für ONTAP NFS SVMs

Sie können lokale UNIX-Benutzer und -Gruppen auf der SVM für die Authentifizierung und Namenszuordnungen verwenden. Sie können UNIX-Benutzer und -Gruppen manuell erstellen oder eine Datei mit UNIX-Benutzern oder -Gruppen von einem Uniform Resource Identifier (URI) laden.

Im Cluster gilt standardmäßig eine maximale Anzahl von 32.768 lokalen UNIX-Benutzergruppen und Gruppenmitgliedern zusammen. Der Clusteradministrator kann dieses Limit anpassen.

Lokale UNIX-Benutzer auf ONTAP NFS SVMs erstellen

Der `vserver services name-service unix-user create` Befehl kann verwendet werden, um lokale UNIX-Benutzer zu erstellen. Ein lokaler UNIX-Benutzer ist ein UNIX-Benutzer, der auf der SVM als Option für UNIX-Name Services erstellt wird und

bei der Verarbeitung von Namenszuordnungen verwendet werden kann.

Schritt

1. Einen lokalen UNIX-Benutzer erstellen:

   `vserver services name-service unix-user create -vserver vserver_name -user user_name -id integer -primary-gid integer -full-name full_name`

   `-user user_name`Gibt den Benutzernamen an. Der Benutzername darf maximal 64 Zeichen lang sein.

   `-id integer` gibt die von Ihnen zugewiesene Benutzer-ID an.

   `-primary-gid integer` Gibt die primäre Gruppen-ID an. Dadurch wird der Benutzer zur primären Gruppe hinzugefügt. Nach der Erstellung des Benutzers ist eine manuelle Hinzufügung zu jeder gewünschten weiteren Gruppe möglich.

Beispiel

Der folgende Befehl erstellt einen lokalen UNIX-Benutzer namens johnm (vollständiger Name "John Miller") auf der SVM namens vs1. Der Benutzer hat die ID 123 und die primäre Gruppen-ID 100.

```
node::> vserver services name-service unix-user create -vserver vs1 -user
johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

Lokale UNIX-Benutzer aus URIs auf ONTAP NFS SVMs laden

Alternativ zur manuellen Erstellung einzelner lokaler UNIX-Benutzer in SVMs lässt sich die Aufgabe vereinfachen, indem eine Liste lokaler UNIX-Benutzer aus einem Uniform Resource Identifier (URI (`vserver services name-service unix-user load-from-uri`) in SVMs geladen wird.

Schritte

1. Eine Datei mit der Liste der lokalen UNIX-Benutzer, die geladen werden sollen, erstellen.

   Die Datei muss Benutzerinformationen im UNIX `/etc/passwd`-Format enthalten:

   `user_name: password: user_ID: group_ID: full_name`

   Der Befehl verwirft den Wert des *`password`* Feldes und die Werte der Felder nach dem *`full_name`* Feld(*`home_directory`* und *`shell`*).

   Die maximal unterstützte Dateigröße beträgt 2,5 MB.

2. Es ist sicherzustellen, dass die Liste keine doppelten Einträge enthält.

   Enthält die Liste doppelte Einträge, schlägt das Laden der Liste mit einer Fehlermeldung fehl.

3. Kopieren Sie die Datei auf einen Server.

   Der Server muss vom Speichersystem über HTTP, HTTPS, FTP oder FTPS erreichbar sein.

4. Ermittelt wird, welcher URI für die Datei gilt.

   Der URI ist die Adresse, die Sie dem Speichersystem angeben, um den Speicherort der Datei zu kennzeichnen.

5. Die Datei mit der Liste der lokalen UNIX-Benutzer wird aus der URI in die SVMs geladen:

   `vserver services name-service unix-user load-from-uri -vserver` *`vserver_name`* `-uri {ftp|http|ftps|https}://`*`uri`* `-overwrite {true|false}`

   `-overwrite {true false}` gibt an, ob Einträge überschrieben werden. Der Standardwert ist `false`.

Beispiel

Der folgende Befehl lädt eine Liste lokaler UNIX-Benutzer aus der URI `ftp://ftp.example.com/passwd` in die SVM mit dem Namen vs1. Vorhandene Benutzer auf der SVM werden durch die Informationen aus der URI nicht überschrieben.

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

Lokale UNIX-Gruppen auf ONTAP NFS SVMs erstellen

Der `vserver services name-service unix-group create` Befehl kann verwendet werden, um UNIX-Gruppen zu erstellen, die lokal für die SVM sind. Lokale UNIX-Gruppen werden mit lokalen UNIX-Benutzern verwendet.

Schritt

1. Eine lokale UNIX-Gruppe erstellen:

   `vserver services name-service unix-group create -vserver` *`vserver_name`* `-name` *`group_name`* `-id` *`integer`*

   `-name` *`group_name`* Gibt den Gruppennamen an. Die Länge des Gruppennamens darf 64 Zeichen nicht überschreiten.

   `-id` *`integer`*`gibt die zugewiesene Gruppen-ID an.

Beispiel

Der folgende Befehl erstellt eine lokale Gruppe namens eng auf der SVM namens vs1. Die Gruppe hat die ID 101.

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name
eng -id 101
```

Benutzer zur lokalen UNIX-Gruppe auf ONTAP NFS SVMs hinzufügen

Mit dem `vserver services name-service unix-group adduser` Befehl kann ein Benutzer zu einer zusätzlichen UNIX-Gruppe hinzugefügt werden, die lokal zur SVM

gehört.

Schritt

1. Einen Benutzer zu einer lokalen UNIX-Gruppe hinzufügen:

`vserver services name-service unix-group adduser -vserver` *`vserver_name`* `-name` *`group_name`* `-username` *`user_name`*

`-name` `*group_name*`Gibt den Namen der UNIX-Gruppe an, zu der der Benutzer zusätzlich zu seiner primären Gruppe hinzugefügt wird.

Beispiel

Der folgende Befehl fügt einen Benutzer namens max zu einer lokalen UNIX-Gruppe namens eng auf der SVM namens vs1 hinzu:

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name
eng
-username max
```

Lokale UNIX-Gruppen von URIs auf ONTAP NFS SVMs laden

Alternativ zur manuellen Erstellung einzelner lokaler UNIX-Gruppen kann eine Liste lokaler UNIX-Gruppen mithilfe des `vserver services name-service unix-group load-from-uri` Befehls aus einem Uniform Resource Identifier (URI) in SVMs geladen werden.

Schritte

1. Erstellen Sie eine Datei mit der Liste der lokalen UNIX-Gruppen, die geladen werden sollen.

   Die Datei muss Gruppeninformationen im UNIX `/etc/group`-Format enthalten:

   `group_name: password: group_ID: comma_separated_list_of_users`

   Der Befehl verwirft den Wert des *`password`* Feldes.

   Die maximal unterstützte Dateigröße beträgt 1 MB.

   Die maximale Länge jeder Zeile in der Gruppendatei beträgt 32.768 Zeichen.

2. Es ist sicherzustellen, dass die Liste keine doppelten Einträge enthält.

   Die Liste darf keine doppelten Einträge enthalten, da sonst das Laden fehlschlägt. Sind bereits Einträge in der SVM vorhanden, muss entweder der `-overwrite` Parameter auf `true` gesetzt werden, um alle vorhandenen Einträge mit der neuen Datei zu überschreiben, oder es muss sichergestellt werden, dass die neue Datei keine Einträge enthält, die vorhandene Einträge duplizieren.

3. Kopieren Sie die Datei auf einen Server.

   Der Server muss vom Speichersystem über HTTP, HTTPS, FTP oder FTPS erreichbar sein.

4. Ermittelt wird, welcher URI für die Datei gilt.

   Der URI ist die Adresse, die Sie dem Speichersystem angeben, um den Speicherort der Datei zu kennzeichnen.

5. Die Datei mit der Liste der lokalen UNIX-Gruppen wird aus dem URI in die SVM geladen:

   `vserver services name-service unix-group load-from-uri -vserver` *vserver_name* `-uri {ftp|http|ftps|https}://`*uri* `-overwrite {true|false}`

   `-overwrite true false`} gibt an, ob Einträge überschrieben werden. Der Standardwert ist `false`. Wird dieser Parameter als `true` angegeben, ersetzt ONTAP die gesamte vorhandene lokale UNIX-Gruppendatenbank der angegebenen SVM durch die Einträge aus der Datei, die geladen wird.

Beispiel

Der folgende Befehl lädt eine Liste lokaler UNIX-Gruppen aus dem URI `ftp://ftp.example.com/group` in die SVM mit dem Namen vs1. Vorhandene Gruppen auf der SVM werden durch die Informationen aus dem URI nicht überschrieben.

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

Mit Netzwerkgruppen arbeiten

Informationen zu Netgroups auf ONTAP NFS SVMs

Sie können Netzgruppen zur Benutzerauthentifizierung und zum Abgleich von Clients in Exportrichtlinienregeln verwenden. Der Zugriff auf Netzgruppen kann von externen Namensservern (LDAP oder NIS) bereitgestellt werden, oder Netzgruppen können mithilfe des `vserver services name-service netgroup load` Befehls aus einem Uniform Resource Identifier (URI) in SVMs geladen werden.

Bevor Sie beginnen

Bevor Sie mit Netgroups arbeiten, muss sichergestellt sein, dass die folgenden Bedingungen erfüllt sind:

- Alle Hosts in Netgroups, unabhängig von der Quelle (NIS, LDAP oder lokale Dateien), müssen sowohl Forward- (A) als auch Reverse- (PTR) DNS-Einträge besitzen, um konsistente Forward- und Reverse-DNS-Lookups bereitzustellen.

  Wenn eine IP-Adresse eines Clients über mehrere PTR-Einträge verfügt, müssen außerdem alle diese Hostnamen Mitglieder der Netgroup sein und über entsprechende A-Einträge verfügen.

- Die Namen aller Hosts in Netgroups müssen, unabhängig von ihrer Quelle (NIS, LDAP oder lokale Dateien), korrekt geschrieben sein und die richtige Groß-/Kleinschreibung aufweisen. Inkonsistenzen bei der Groß-/Kleinschreibung von Hostnamen in Netgroups können zu unerwartetem Verhalten führen, wie zum Beispiel zu fehlgeschlagenen Exportprüfungen.
- Alle in Netzgruppen angegebenen IPv6-Adressen müssen gemäß RFC 5952 gekürzt und komprimiert sein.

  Beispielsweise muss 2011:hu9:0:0:0:0:3:1 zu 2011:hu9::3:1 verkürzt werden.

Über diese Aufgabe

Bei der Arbeit mit Netzwerkgruppen können die folgenden Operationen durchgeführt werden:

- Der `vserver export-policy netgroup check-membership`Befehl kann verwendet werden, um festzustellen, ob eine Client-IP-Adresse Mitglied einer bestimmten Netzgruppe ist.
- Mit dem `vserver services name-service getxxbyyy netgrp` Befehl lässt sich überprüfen, ob ein Client Teil einer Netgroup ist.

  Der für die Namensauflösung zugrunde liegende Dienst wird basierend auf der konfigurierten Reihenfolge des Name Service Switch ausgewählt.

Netzgruppen von URIs auf ONTAP NFS SVMs laden

Eine der Methoden, mit denen Sie Clients in Exportrichtlinienregeln abgleichen können, ist die Verwendung von Hosts, die in Netzgruppen aufgeführt sind. Netzgruppen können als Alternative zur Verwendung von Netzgruppen, die auf externen Namensservern gespeichert sind (`vserver services name-service netgroup load`, über einen Uniform Resource Identifier (URI) in SVMs geladen werden.

Bevor Sie beginnen

Netgroup-Dateien müssen die folgenden Anforderungen erfüllen, bevor sie in eine SVM geladen werden:

- Die Datei muss das gleiche korrekte Netgroup-Textdateiformat verwenden, das auch zur Befüllung von NIS verwendet wird.

  ONTAP prüft das Format der Netgroup-Textdatei vor dem Laden. Enthält die Datei Fehler, wird sie nicht geladen und eine Meldung zeigt die Korrekturen an, die Sie in der Datei vornehmen müssen. Nach der Korrektur der Fehler kann die Netgroup-Datei in die angegebene SVM erneut geladen werden.

- Alle alphabetischen Zeichen in den Hostnamen in der Netgroup-Datei sollten Kleinbuchstaben sein.
- Die maximal unterstützte Dateigröße beträgt 5 MB.
- Die maximal unterstützte Verschachtelungsebene für Netzgruppen beträgt 1000.
- Beim Definieren von Hostnamen in der Netgroup-Datei können nur primäre DNS-Hostnamen verwendet werden.

  Um Probleme beim Exportzugriff zu vermeiden, sollten Hostnamen nicht mittels DNS CNAME- oder Round-Robin-Einträgen definiert werden.

- Die Benutzer- und Domänenteile der Tripel in der Netgroup-Datei sollten leer bleiben, da ONTAP diese nicht unterstützt.

  Es wird nur der Host/IP-Teil unterstützt.

Über diese Aufgabe

ONTAP unterstützt netgroup-by-host-Suchen für die lokale netgroup-Datei. Nach dem Laden der netgroup-Datei erstellt ONTAP automatisch eine netgroup.byhost-Zuordnung, um netgroup-by-host-Suchen zu ermöglichen. Dies kann lokale netgroup-Suchen bei der Verarbeitung von Export-Policy-Regeln zur Bewertung des Clientzugriffs erheblich beschleunigen.

Schritt

1. Netzgruppen aus einer URI in SVMs laden:

   `vserver services name-service netgroup load -vserver vserver_name -source {ftp|http|ftps|https}://uri`

   Das Laden der Netgroup-Datei und das Erstellen der Netgroup.byhost-Zuordnung kann mehrere Minuten dauern.

   Wenn Sie die Netzgruppen aktualisieren möchten, kann die Datei bearbeitet und die aktualisierte Netzgruppendatei in die SVM geladen werden.

Beispiel

Der folgende Befehl lädt Netzgruppendefinitionen in die SVM mit dem Namen vs1 von der HTTP-URL `http://intranet/downloads/corp-netgroup`:

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

ONTAP NFS SVM-Netzgruppendefinitionen überprüfen

Nach dem Laden der Netzgruppen in die SVM kann mit dem `vserver services name-service netgroup status` Befehl der Status der Netzgruppendefinitionen überprüft werden. So lässt sich feststellen, ob die Netzgruppendefinitionen auf allen Knoten, die die SVM unterstützen, konsistent sind.

Schritte

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

   `set -privilege advanced`

2. Status der Netzgruppendefinitionen überprüfen:

   `vserver services name-service netgroup status`

   Zusätzliche Informationen werden in einer detaillierteren Ansicht angezeigt.

3. Zurück zur Administrator-Privilegstufe:

   `set -privilege admin`

Beispiel

Nachdem die Berechtigungsstufe festgelegt wurde, zeigt der folgende Befehl den Netgroup-Status für alle SVMs an:

```
vs1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when
         directed to do so by technical support.
```

```
Do you wish to continue? (y or n): y

vs1::*> vserver services name-service netgroup status
Virtual
Server    Node            Load Time           Hash Value
--------- --------------- -------------------
--------------------------------
vs1
          node1           9/20/2006 16:04:53
e6cb38ec1396a280c0d2b77e3a84eda2
          node2           9/20/2006 16:06:26
e6cb38ec1396a280c0d2b77e3a84eda2
          node3           9/20/2006 16:08:08
e6cb38ec1396a280c0d2b77e3a84eda2
          node4           9/20/2006 16:11:33
e6cb38ec1396a280c0d2b77e3a84eda2
```

NIS-Domänenkonfigurationen für ONTAP NFS SVMs erstellen

Wenn in Ihrer Umgebung ein Network Information Service (NIS) für Namensdienste verwendet wird, muss eine NIS-Domänenkonfiguration für die SVM mithilfe des `vserver services name-service nis-domain create` Befehls erstellt werden.

Bevor Sie beginnen

Alle konfigurierten NIS-Server müssen verfügbar und erreichbar sein, bevor die NIS-Domäne auf der SVM konfiguriert wird.

Wenn Sie NIS für Verzeichnissuchen verwenden möchten, dürfen die Zuordnungen auf Ihren NIS-Servern maximal 1.024 Zeichen pro Eintrag enthalten. Ein NIS-Server, der diese Beschränkung nicht einhält, sollte nicht angegeben werden. Andernfalls kann der Clientzugriff, der von NIS-Einträgen abhängt, fehlschlagen.

Über diese Aufgabe

Wenn Ihre NIS-Datenbank eine `netgroup.byhost` Zuordnung enthält, kann ONTAP diese für schnellere Suchvorgänge nutzen. Die `netgroup.byhost`- und `netgroup`-Zuordnungen im Verzeichnis müssen jederzeit synchron gehalten werden, um Zugriffsprobleme für Clients zu vermeiden. Ab ONTAP 9.7 können NIS- `netgroup.byhost`-Einträge mithilfe der `vserver services name-service nis-domain netgroup-database` Befehle zwischengespeichert werden.

Die Verwendung von NIS zur Hostnamensauflösung wird nicht unterstützt.

Schritte

1. Erstellen einer NIS-Domänenkonfiguration:

   ```
   vserver services name-service nis-domain create -vserver vs1 -domain
   <domain_name> -nis-servers <IP_addresses>
   ```

   Sie können bis zu 10 NIS Server angeben.

Das `-nis-servers` Feld ersetzt das `-servers` Feld. Das `-nis-servers` Feld kann verwendet werden, um entweder einen Hostnamen oder eine IP-Adresse für den NIS-Server anzugeben.

2. Überprüfen, ob die Domain erstellt wurde:

```
vserver services name-service nis-domain show
```

Beispiel

Der folgende Befehl erstellt eine NIS-Domänenkonfiguration für eine NIS-Domäne namens `nisdomain` auf der SVM mit dem Namen `vs1` mit einem NIS-Server unter der IP-Adresse `192.0.2.180`:

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -nis-servers 192.0.2.180
```

LDAP verwenden

Informationen zur Verwendung von LDAP-Name-Services auf ONTAP NFS SVMs

Wenn in Ihrer Umgebung LDAP für Namensdienste verwendet wird, ist eine Zusammenarbeit mit Ihrem LDAP-Administrator erforderlich, um die Anforderungen und geeigneten Speichersystemkonfigurationen zu bestimmen und anschließend die SVM als LDAP-Client zu aktivieren.

Ab ONTAP 9.10.1 wird die LDAP-Kanalbindung standardmäßig sowohl für Active Directory- als auch für Name Services-LDAP-Verbindungen unterstützt. ONTAP versucht die Kanalbindung mit LDAP-Verbindungen nur, wenn Start-TLS oder LDAPS aktiviert ist und die Sitzungssicherheit entweder auf Signieren oder Versiegeln eingestellt ist. Zum Deaktivieren oder erneuten Aktivieren der LDAP-Kanalbindung mit Nameservern kann der `-try-channel-binding` Parameter mit dem `ldap client modify` Befehl verwendet werden.

Weitere Informationen finden sich unter "LDAP-Kanalbindungs- und LDAP-Signaturanforderungen für Windows 2020".

- Bevor Sie LDAP für ONTAP konfigurieren, sollte überprüft werden, ob Ihre Standortbereitstellung den Best Practices für die Konfiguration von LDAP-Server und -Client entspricht. Insbesondere müssen die folgenden Bedingungen erfüllt sein:
  - Der Domänenname des LDAP-Servers muss mit dem Eintrag auf dem LDAP-Client übereinstimmen.
  - Die vom LDAP-Server unterstützten LDAP-Benutzerpasswort-Hash-Typen müssen diejenigen einschließen, die von ONTAP unterstützt werden:
    - CRYPT (alle Typen) und SHA-1 (SHA, SSHA).
    - Ab ONTAP 9.8 werden auch SHA-2-Hashes (SHA-256, SHA-384, SHA-512, SSHA-256, SSHA-384 und SSHA-512) unterstützt.
  - Wenn der LDAP-Server Sitzungssicherheitsmaßnahmen erfordert, müssen diese im LDAP-Client konfiguriert werden.

    Folgende Sitzungssicherheitsoptionen stehen zur Verfügung:

        - LDAP-Signierung (bietet Datenintegritätsprüfung) und LDAP-Signierung und Versiegelung (bietet Datenintegritätsprüfung und Verschlüsselung)
        - START TLS
        - LDAPS (LDAP über TLS oder SSL)
    - Um signierte und versiegelte LDAP-Abfragen zu ermöglichen, müssen die folgenden Dienste konfiguriert werden:
        - LDAP-Server müssen den GSSAPI (Kerberos) SASL-Mechanismus unterstützen.
        - LDAP-Server müssen sowohl DNS-A/AAAA-Einträge als auch PTR-Einträge auf dem DNS-Server haben.
        - Kerberos-Server müssen SRV-Einträge auf dem DNS-Server haben.
    - Um START TLS oder LDAPS zu aktivieren, sind die folgenden Punkte zu berücksichtigen.
        - Es ist eine NetApp Best Practice, Start TLS anstelle von LDAPS zu verwenden.
        - Wenn LDAPS verwendet wird, muss der LDAP-Server in ONTAP 9.5 und höher für TLS oder für SSL aktiviert sein. SSL wird in ONTAP 9.0-9.4 nicht unterstützt.
        - In der Domäne muss bereits ein Zertifikatsserver konfiguriert sein.
    - Damit LDAP-Referral-Chasing (in ONTAP 9.5 und höher) aktiviert werden kann, müssen die folgenden Bedingungen erfüllt sein:
        - Beide Domänen sollten mit einer der folgenden Vertrauensbeziehungen konfiguriert sein:
            - Zweiwege
            - Einseitig, wobei die primäre Domain der Referral-Domain vertraut.
            - Parent-Child
        - DNS muss so konfiguriert sein, dass alle referenzierten Servernamen aufgelöst werden.
        - Domänenpasswörter müssen identisch sein, um die Authentifizierung zu ermöglichen, wenn --bind -as-cifs-server auf true gesetzt ist.



Die folgenden Konfigurationen werden bei LDAP-Referral-Chasing nicht unterstützt.

- Für alle ONTAP Versionen:
    - LDAP-Clients auf einer Admin-SVM
- Für ONTAP 9.8 und frühere Versionen (sie werden in ONTAP 9.9.1 und später unterstützt):
    - LDAP-Signierung und Versiegelung (die `-session-security` Option)
    - Verschlüsselte TLS-Verbindungen (die `-use-start-tls` Option)
    - Kommunikation über den LDAPS-Port 636 (die `-use-ldaps-for-ad-ldap` Option)

- Ein LDAP-Schema ist bei der Konfiguration des LDAP-Clients auf der SVM anzugeben.

  In den meisten Fällen ist eines der Standard-ONTAP-Schemas geeignet. Weicht das LDAP-Schema in Ihrer Umgebung jedoch davon ab, muss vor der Erstellung des LDAP-Clients ein neues LDAP-Client-Schema für ONTAP erstellt werden. Bezüglich der Anforderungen in Ihrer Umgebung empfiehlt sich eine Rücksprache mit Ihrem LDAP-Administrator.

- Die Verwendung von LDAP zur Hostnamensauflösung wird nicht unterstützt.

Für weitere Informationen

- "NetApp Technischer Bericht 4835: Konfiguration von LDAP in ONTAP"
- "Selbstsignierte Root-CA-Zertifikate auf der ONTAP SMB SVM installieren"

Neue LDAP-Client-Schemas für ONTAP NFS SVMs erstellen

Wenn das LDAP-Schema in Ihrer Umgebung von den ONTAP-Standardeinstellungen abweicht, muss ein neues LDAP-Client-Schema für ONTAP erstellt werden, bevor die LDAP-Client-Konfiguration erstellt wird.

Über diese Aufgabe

Die meisten LDAP-Server können die von ONTAP bereitgestellten Standardschemas verwenden:

- MS-AD-BIS (das bevorzugte Schema für die meisten Windows 2012 und späteren AD-Server)
- AD-IDMU (Windows 2008, Windows 2012 und spätere AD-Server)
- AD-SFU (Windows 2003 und ältere AD-Server)
- RFC-2307 (UNIX LDAP-Server)

Wenn ein nicht standardmäßiges LDAP-Schema verwendet werden soll, muss dieses vor der Erstellung der LDAP-Client-Konfiguration erstellt werden. Vor der Erstellung eines neuen Schemas sollte Rücksprache mit dem LDAP-Administrator gehalten werden.

Die von ONTAP bereitgestellten Standard-LDAP-Schemas können nicht geändert werden. Zum Erstellen eines neuen Schemas wird eine Kopie erstellt und anschließend entsprechend angepasst.

Schritte

1. Die vorhandenen LDAP-Client-Schemavorlagen werden angezeigt, um diejenige zu identifizieren, die kopiert werden soll:

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

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

   ```
   set -privilege advanced
   ```

3. Eine Kopie eines vorhandenen LDAP-Client-Schemas erstellen:

   ```
   vserver services name-service ldap client schema copy -vserver vserver_name
   -schema existing_schema_name -new-schema-name new_schema_name
   ```

4. Das neue Schema kann geändert und an die eigene Umgebung angepasst werden:

   ```
   vserver services name-service ldap client schema modify
   ```

5. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

LDAP-Client-Konfigurationen für ONTAP NFS-Zugriff erstellen

Wenn ONTAP auf die externen LDAP- oder Active Directory-Dienste in Ihrer Umgebung zugreifen soll, muss zunächst ein LDAP-Client auf dem Speichersystem eingerichtet werden.

Bevor Sie beginnen

Einer der ersten drei Server in der aufgelösten Liste der Active Directory-Domäne muss betriebsbereit sein und Daten bereitstellen. Andernfalls schlägt diese Aufgabe fehl.

> Es gibt mehrere Server, von denen zu jedem Zeitpunkt mehr als zwei Server ausgefallen sind.

Schritte

1. Konsultieren Sie Ihren LDAP-Administrator, um die geeigneten Konfigurationswerte für den `vserver services name-service ldap client create` Befehl zu bestimmen:

   a. Eine domänenbasierte oder eine adressbasierte Verbindung zu LDAP-Servern angeben.

      Die `-ad-domain`- und `-servers`-Optionen schließen sich gegenseitig aus.

      - Die `-ad-domain` Option ermöglicht die Aktivierung der LDAP-Servererkennung in der Active Directory-Domäne.
        - Sie können die `-restrict-discovery-to-site` Option verwenden, um die LDAP-Serverermittlung auf den CIFS-Standardstandort für die angegebene Domäne zu beschränken. Wenn Sie diese Option verwenden, müssen Sie auch den CIFS-Standardstandort mit `-default-site` angeben.
      - Sie können die `-preferred-ad-servers` Option verwenden, um einen oder mehrere bevorzugte Active Directory Server anhand ihrer IP-Adressen in einer durch Kommas getrennten Liste anzugeben. Nach der Erstellung des Clients kann diese Liste mit dem `vserver services name-service ldap client modify` Befehl geändert werden.
      - Mit der `-servers` Option kann ein oder können mehrere LDAP-Server (Active Directory oder UNIX) anhand ihrer IP-Adresse in einer durch Kommas getrennten Liste angegeben werden.

        > Die `-servers` Option ist veraltet. Das `-ldap-servers` Feld ersetzt das `-servers` Feld. Dieses Feld kann entweder einen Hostnamen oder eine IP-Adresse für den LDAP-Server annehmen.

   b. Ein Standard- oder ein benutzerdefiniertes LDAP-Schema kann angegeben werden.

      Die meisten LDAP-Server können die von ONTAP bereitgestellten schreibgeschützten Standardschemas verwenden. Es empfiehlt sich, diese Standardschemas zu nutzen, sofern keine anderen Anforderungen bestehen. In diesem Fall kann ein eigenes Schema erstellt werden, indem ein Standardschema kopiert wird (diese sind schreibgeschützt) und die Kopie anschließend angepasst wird.

      Standardschemas:

      - MS-AD-BIS

        Basierend auf RFC-2307bis ist dies das bevorzugte LDAP-Schema für die meisten Standard-

Windows 2012 und späteren LDAP-Bereitstellungen.

- `AD-IDMU`

  Dieses Schema basiert auf Active Directory Identity Management für UNIX und eignet sich für die meisten Windows 2008, Windows 2012 und späteren AD-Server.

- `AD-SFU`

  Basierend auf Active Directory Services für UNIX ist dieses Schema für die meisten Windows 2003 und frühere AD-Server geeignet.

- `RFC-2307`

  Basierend auf RFC-2307 (*An Approach for Using LDAP as a Network Information Service*) ist dieses Schema für die meisten UNIX AD Server geeignet.

c. Bindungswerte auswählen.

- `-min-bind-level {anonymous|simple|sasl}` gibt die minimale Bindungs-Authentifizierungsebene an.

  Der Standardwert ist **`anonymous`**.

- `-bind-dn *LDAP_DN*` gibt den Bind-Benutzer an.

  Für Active Directory-Server muss der Benutzer im Kontoformat (DOMAIN\user) oder im Principal-Format (user@domain.com) angegeben werden. Andernfalls muss der Benutzer im Format individueller Name (CN=user,DC=domain,DC=com) angegeben werden.

- `-bind-password *password*` gibt das Bind-Passwort an.

d. Sicherheitsoptionen für die Sitzung können bei Bedarf ausgewählt werden.

Sie können entweder LDAP-Signierung und -Versiegelung oder LDAP über TLS aktivieren, falls dies vom LDAP-Server erforderlich ist.

- `--session-security {none|sign|seal}`

  Sie können Signieren (`sign`, Datenintegrität, Signieren und Versiegeln (`seal`, Datenintegrität und Verschlüsselung oder keines von beidem `none`, keine Signierung oder Versiegelung, aktivieren. Der Standardwert ist `none`.

  Sie sollten außerdem `-min-bind-level {sasl}` festlegen, es sei denn, Sie möchten, dass die Bind-Authentifizierung auf **`anonymous`** oder **`simple`** zurückgreift, falls die Signierungs- und Versiegelungsbindung fehlschlägt.

- `-use-start-tls {true|false}`

  Wenn auf **`true`** gesetzt und der LDAP-Server dies unterstützt, verwendet der LDAP-Client eine verschlüsselte TLS-Verbindung zum Server. Der Standardwert ist **`false`**. Zum Verwenden dieser Option ist die Installation eines selbstsignierten Root-CA-Zertifikats des LDAP-Servers erforderlich.

> Wenn der Storage-VM ein SMB-Server hinzugefügt wurde, der einer Domäne zugeordnet ist, und der LDAP-Server einer der Domänencontroller der Heimatdomäne

des SMB-Servers ist, kann die `-session-security-for-ad-ldap` Option mit dem `vserver cifs security modify` Befehl geändert werden.

e. Port-, Abfrage- und Basiswerte auswählen.

Die Standardwerte werden empfohlen, jedoch sollte mit dem LDAP-Administrator überprüft werden, ob sie für Ihre Umgebung geeignet sind.

- `-port *port*` gibt den LDAP-Server-Port an.

  Der Standardwert ist `389`.

Wenn Sie Start TLS zur Sicherung der LDAP-Verbindung verwenden möchten, müssen Sie den Standardport 389 nutzen. Start TLS beginnt als unverschlüsselte Verbindung über den LDAP-Standardport 389, und diese Verbindung wird anschließend auf TLS umgestellt. Wenn Sie den Port ändern, schlägt Start TLS fehl.

- `-query-timeout *integer*` gibt die Abfrage-Zeitüberschreitung in Sekunden an.

  Der zulässige Bereich liegt zwischen 1 und 10 Sekunden. Der Standardwert beträgt `3` Sekunden.

- `-base-dn *LDAP_DN*` Gibt den Basis-DN an.

  Bei Bedarf können mehrere Werte eingegeben werden (z. B. wenn das LDAP-Referral-Chasing aktiviert ist). Der Standardwert ist `""` (root).

- `-base-scope` {`base`|`onelevel`|`subtree`} gibt den Basissuchbereich an.

  Der Standardwert ist `subtree`.

- `-referral-enabled` {`true`|`false`} gibt an, ob die LDAP-Referral-Verfolgung aktiviert ist.

  Ab ONTAP 9.5 ermöglicht dies dem ONTAP LDAP-Client, Suchanfragen an andere LDAP-Server weiterzuleiten, wenn der primäre LDAP-Server eine LDAP-Verweisantwort zurückgibt, die angibt, dass die gewünschten Datensätze auf den referenzierten LDAP-Servern vorhanden sind. Der Standardwert ist **`false`**.

Um nach Datensätzen auf den referenzierten LDAP-Servern zu suchen, muss der Basis-DN der referenzierten Datensätze im Rahmen der LDAP-Client-Konfiguration zum Basis-DN hinzugefügt werden.

2. Eine LDAP-Client-Konfiguration auf der Storage-VM erstellen:

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```

Beim Erstellen einer LDAP-Client-Konfiguration muss der Name der Storage-VM angegeben werden.

3. Es sollte überprüft werden, ob die LDAP-Client-Konfiguration erfolgreich erstellt wurde:

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

Beispiele

Der folgende Befehl erstellt eine neue LDAP-Client-Konfiguration namens ldap1 für die Storage-VM vs1 zur Zusammenarbeit mit einem Active Directory Server für LDAP:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

Der folgende Befehl erstellt eine neue LDAP-Clientkonfiguration namens ldap1 für die Storage-VM vs1, um mit einem Active Directory Server für LDAP zu arbeiten, auf dem Signierung und Versiegelung erforderlich sind und die LDAP-Servererkennung auf einen bestimmten Standort für die angegebene Domäne beschränkt ist:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

Der folgende Befehl erstellt eine neue LDAP-Client-Konfiguration namens ldap1 für die Storage-VM vs1, um mit einem Active Directory Server für LDAP zu arbeiten, wobei LDAP-Referral-Chasing erforderlich ist:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

Der folgende Befehl ändert die LDAP-Client-Konfiguration mit dem Namen ldap1 für die Storage-VM vs1, wobei der Basis-DN angegeben wird:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

Der folgende Befehl ändert die LDAP-Client-Konfiguration mit dem Namen ldap1 für die Storage-VM vs1, indem das Referral-Chasing aktiviert wird:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com"  -referral-enabled true
```

LDAP-Client-Konfigurationen mit ONTAP NFS SVMs verknüpfen

Um LDAP auf einer SVM zu aktivieren, muss der `vserver services name-service ldap create` Befehl verwendet werden, um eine LDAP-Client-Konfiguration mit der SVM zu verknüpfen.

Bevor Sie beginnen

- Im Netzwerk muss bereits eine LDAP-Domäne vorhanden sein, die für den Cluster, auf dem sich die SVM befindet, zugänglich ist.
- Auf der SVM muss eine LDAP-Client-Konfiguration vorhanden sein.

Schritte

1. LDAP auf der SVM aktivieren:

   `vserver services name-service ldap create -vserver` *`vserver_name`* `-client-config` *`client_config_name`*

   > ⓘ Der `vserver services name-service ldap create` Befehl führt eine automatische Konfigurationsprüfung durch und gibt eine Fehlermeldung aus, wenn ONTAP den Nameserver nicht erreichen kann.

   Der folgende Befehl aktiviert LDAP auf der "vs1"SVM und konfiguriert sie so, dass sie die LDAP-Client-Konfiguration "ldap1" verwendet:

   ```
   cluster1::> vserver services name-service ldap create -vserver vs1
   -client-config ldap1 -client-enabled true
   ```

2. Der Status der Nameserver kann mit dem Befehl vserver services name-service ldap check validiert werden.

   Der folgende Befehl validiert LDAP-Server auf der SVM vs1.

   ```
   cluster1::> vserver services name-service ldap check -vserver vs1

   | Vserver: vs1                                                    |
   | Client Configuration Name: c1                                   |
   | LDAP Status: up                                                 |
   | LDAP Status Details: Successfully connected to LDAP server
   "10.11.12.13".                                                  |
   ```

LDAP-Quellen für ONTAP NFS SVMs verifizieren

Es ist zu überprüfen, ob die LDAP-Quellen für die Namensdienste in der Name-Service-Switch-Tabelle für die SVM korrekt aufgeführt sind.

Schritte

1. Aktueller Inhalt der Namensdienstumschaltertabelle anzeigen:

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

   Der folgende Befehl zeigt die Ergebnisse für die SVM My_SVM:

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
                                 Source
Vserver         Database         Order
--------------- ------------   ---------
My_SVM          hosts          files,
                               dns
My_SVM          group          files,ldap
My_SVM          passwd         files,ldap
My_SVM          netgroup       files
My_SVM          namemap        files
5 entries were displayed.
```

   `namemap` Gibt die Quellen an, in denen nach Namenszuordnungsinformationen gesucht wird, und in welcher Reihenfolge. In einer reinen UNIX-Umgebung ist dieser Eintrag nicht erforderlich. Eine Namenszuordnung ist nur in einer gemischten Umgebung mit UNIX und Windows erforderlich.

2. Der `ns-switch`Eintrag wird gegebenenfalls aktualisiert:

Wenn Sie den ns-switch-Eintrag für … aktualisieren möchten	Geben Sie den Befehl ein…
Benutzerinformationen	`vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files`
Gruppeninformationen	`vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files`
Netgroup-Informationen	`vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files`

Kerberos mit NFS für hohe Sicherheit verwenden

Informationen zur Verwendung von Kerberos mit ONTAP NFS für eine starke Authentifizierung

Wenn Kerberos in Ihrer Umgebung für die starke Authentifizierung verwendet wird, ist eine Zusammenarbeit mit Ihrem Kerberos-Administrator erforderlich, um die Anforderungen und geeigneten Speichersystemkonfigurationen zu bestimmen und anschließend die SVM als Kerberos-Client zu aktivieren.

Ihre Umgebung sollte die folgenden Richtlinien erfüllen:

- Die Standortbereitstellung sollte den Best Practices für die Konfiguration von Kerberos-Server und -Client entsprechen, bevor Kerberos für ONTAP konfiguriert wird.
- Wenn möglich, sollte NFSv4 oder höher verwendet werden, falls eine Kerberos-Authentifizierung erforderlich ist.

  NFSv3 kann mit Kerberos verwendet werden. Die vollen Sicherheitsvorteile von Kerberos kommen jedoch nur in ONTAP Deployments von NFSv4 oder höher vollständig zum Tragen.

- Um redundanten Serverzugriff zu fördern, sollte Kerberos auf mehreren Daten-LIFs auf mehreren Knoten im Cluster unter Verwendung desselben SPN aktiviert werden.
- Wenn Kerberos auf der SVM aktiviert ist, muss je nach Konfiguration Ihres NFS-Clients eine der folgenden Sicherheitsmethoden in den Exportrichtlinien für Volumes oder qtrees angegeben werden.
  - `krb5` (Kerberos v5-Protokoll)
  - `krb5i` (Kerberos v5-Protokoll mit Integritätsprüfung mittels Prüfsummen)
  - `krb5p` (Kerberos v5-Protokoll mit Datenschutzdienst)

Zusätzlich zum Kerberos-Server und den Clients müssen die folgenden externen Dienste für ONTAP konfiguriert werden, damit Kerberos unterstützt wird:

- Verzeichnisdienst

  In Ihrer Umgebung sollte ein sicherer Verzeichnisdienst wie Active Directory oder OpenLDAP verwendet werden, der für die Nutzung von LDAP über SSL/TLS konfiguriert ist. NIS sollte nicht verwendet werden, da dessen Anfragen im Klartext gesendet werden und daher nicht sicher sind.

- NTP

  Sie benötigen einen funktionierenden Zeitserver, auf dem NTP ausgeführt wird. Dies ist notwendig, um einen Fehler bei der Kerberos-Authentifizierung aufgrund von Zeitabweichungen zu verhindern.

- Domainnamensauflösung (DNS)

  Jeder UNIX-Client und jede SVM-LIF muss über einen gültigen Service Record (SRV) verfügen, der beim KDC in den Forward- und Reverse-Lookup-Zonen registriert ist. Alle Teilnehmer müssen über DNS auflösbar sein.

UNIX-Berechtigungen für NFS-Kerberos-Konfigurationen auf ONTAP SVMs überprüfen

Kerberos erfordert, dass bestimmte UNIX-Berechtigungen für das SVM Root-Volume sowie für lokale Benutzer und Gruppen festgelegt sind.

Schritte

1. Die relevanten Berechtigungen für das SVM-Root-Volume werden angezeigt:

   `volume show -volume root_vol_name-fields user,group,unix-permissions`

   Das Root-Volume der SVM muss folgende Konfiguration aufweisen:

Name…	Einstellung…
UID	Root-Benutzer oder ID 0
GID	Root-Benutzer oder ID 0
UNIX-Berechtigungen	755

   Falls diese Werte nicht angezeigt werden, kann der `volume modify` Befehl zur Aktualisierung verwendet werden.

2. Lokale UNIX-Benutzer werden angezeigt:

   `vserver services name-service unix-user show -vserver vserver_name`

   Die SVM muss über die folgenden UNIX-Benutzer verfügen:

Benutzername	Benutzer-ID	Primäre Gruppen-ID	Kommentar
NFS	500	0	Erforderlich für die GSS INIT-Phase. Die erste Komponente des NFS-Client-Benutzer-SPN wird als Benutzer verwendet. Der NFS-Benutzer ist nicht erforderlich, wenn eine Kerberos-UNIX-Namenszuordnung für den SPN des NFS-Client-Benutzers existiert.
root	0	0	Für das Mounten erforderlich.

   Falls diese Werte nicht angezeigt werden, kann der `vserver services name-service unix-user modify` Befehl verwendet werden, um sie zu aktualisieren.

3. Lokale UNIX-Gruppen werden angezeigt:

   `vserver services name-service unix-group show -vserver vserver _name`

   Die SVM muss mit den folgenden UNIX-Gruppen konfiguriert sein:

Gruppenname	Gruppen-ID
Daemon	1
root	0

Falls diese Werte nicht angezeigt werden, kann der `vserver services name-service unix-group modify` Befehl verwendet werden, um sie zu aktualisieren.

Erstellen von NFS Kerberos Realm-Konfigurationen auf ONTAP SVMs

Damit ONTAP auf externe Kerberos-Server in Ihrer Umgebung zugreifen kann, müssen Sie die SVM zunächst für die Verwendung eines vorhandenen Kerberos-Realms konfigurieren. Dazu benötigen Sie die Konfigurationswerte für den Kerberos-KDC-Server und verwenden dann den `vserver nfs kerberos realm create` Befehl, um die Kerberos-Realm-Konfiguration auf einer SVM zu erstellen.

Bevor Sie beginnen

Der Clusteradministrator sollte NTP auf dem Speichersystem, dem Client und dem KDC-Server konfiguriert haben, um Authentifizierungsprobleme zu vermeiden. Zeitunterschiede zwischen Client und Server (Uhrzeitabweichung) sind eine häufige Ursache für Authentifizierungsfehler.

Schritte

1. Mit dem Kerberos-Administrator kann bestimmt werden, welche geeigneten Konfigurationswerte für den `vserver nfs kerberos realm create` Befehl bereitzustellen sind.
2. Erstellen einer Kerberos Realm-Konfiguration auf der SVM:

   `vserver nfs kerberos realm create -vserver` *`vserver_name`* `-realm` *`realm_name`* *`{AD_KDC_server_values |AD_KDC_server_values}`* `-comment "`*`text`*`"`

3. Es wird überprüft, ob die Kerberos Realm-Konfiguration erfolgreich erstellt wurde:

   `vserver nfs kerberos realm show`

Beispiele

Der folgende Befehl erstellt eine NFS Kerberos Realm-Konfiguration für die SVM vs1, die einen Microsoft Active Directory Server als KDC-Server verwendet. Der Kerberos Realm ist AUTH.EXAMPLE.COM. Der Active Directory Server heißt ad-1 und hat die IP-Adresse 10.10.8.14. Die zulässige Zeitabweichung beträgt 300 Sekunden (Standardwert). Die IP-Adresse des KDC-Servers ist 10.10.8.14, und seine Portnummer ist 88 (Standardwert). Der Kommentar ist „Microsoft Kerberos config“.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

Der folgende Befehl erstellt eine NFS Kerberos Realm-Konfiguration für die SVM vs1, die einen MIT KDC verwendet. Das Kerberos Realm ist SECURITY.EXAMPLE.COM. Die zulässige Zeitabweichung beträgt 300 Sekunden. Die IP-Adresse des KDC-Servers ist 10.10.9.1, und seine Portnummer ist 88. Der KDC-Anbieter ist

Other, um einen UNIX-Anbieter anzuzeigen. Die IP-Adresse des Administrationsservers ist 10.10.9.1, und seine Portnummer ist 749 (Standard). Die IP-Adresse des Passwortservers ist 10.10.9.1, und seine Portnummer ist 464 (Standard). "UNIX Kerberos config" ist der Kommentar.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

NFS-Kerberos zulässige Verschlüsselungstypen für ONTAP SVMs konfigurieren

Standardmäßig unterstützt ONTAP die folgenden Verschlüsselungstypen für NFS Kerberos: DES, 3DES, AES-128 und AES-256. Die zulässigen Verschlüsselungstypen können für jede SVM entsprechend den Sicherheitsanforderungen der jeweiligen Umgebung mit dem `vserver nfs modify` Befehl und dem `-permitted-enc-types` Parameter konfiguriert werden.

Über diese Aufgabe

Für größtmögliche Client-Kompatibilität unterstützt ONTAP standardmäßig sowohl die schwache DES- als auch die starke AES-Verschlüsselung. Das bedeutet beispielsweise, dass, wenn eine Erhöhung der Sicherheit gewünscht ist und die Umgebung dies unterstützt, mit diesem Verfahren DES und 3DES deaktiviert werden können und Clients ausschließlich AES-Verschlüsselung verwenden müssen.

Sie sollten die stärkste verfügbare Verschlüsselung verwenden. Für ONTAP ist das AES-256. Es sollte mit Ihrem KDC-Administrator bestätigt werden, dass diese Verschlüsselungsstufe in Ihrer Umgebung unterstützt wird.

- Das vollständige Aktivieren oder Deaktivieren von AES (sowohl AES-128 als auch AES-256) auf SVMs ist störend, da dabei die ursprüngliche DES-Principal-/Keytab-Datei zerstört wird, wodurch die Kerberos-Konfiguration auf allen LIFs für die SVM deaktiviert werden muss.

  Vor dieser Änderung sollte überprüft werden, ob NFS Clients auf der SVM nicht auf AES Verschlüsselung angewiesen sind.

- Das Aktivieren oder Deaktivieren von DES oder 3DES erfordert keine Änderungen an der Kerberos-Konfiguration auf LIFs.

Schritt

1. Den gewünschten zulässigen Verschlüsselungstyp aktivieren oder deaktivieren:

Wenn Sie aktivieren oder deaktivieren möchten…	Folgen Sie diesen Schritten…

DES oder 3DES	a. Die zulässigen Verschlüsselungstypen für NFS Kerberos der SVM konfigurieren:
	`vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types`
	
	Mehrere Verschlüsselungstypen durch ein Komma trennen.
	
	b. Es sollte überprüft werden, ob die Änderung erfolgreich war:
	`vserver nfs show -vserver vserver_name -fields permitted-enc-types`

AES-128 oder AES-256	a. Ermitteln, auf welcher SVM und LIF Kerberos aktiviert ist:
	`vserver nfs kerberos interface show`
	
	b. Kerberos auf allen LIFs der SVM deaktivieren, deren NFS Kerberos zulässigen Verschlüsselungstyp Sie ändern möchten:
	`vserver nfs kerberos interface disable -lif lif_name`
	
	c. Die zulässigen Verschlüsselungstypen für NFS Kerberos der SVM konfigurieren:
	`vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types`
	
	Mehrere Verschlüsselungstypen durch ein Komma trennen.
	
	d. Es sollte überprüft werden, ob die Änderung erfolgreich war:
	`vserver nfs show -vserver vserver_name -fields permitted-enc-types`
	
	e. Kerberos auf allen LIFs auf der SVM wieder aktivieren:
	`vserver nfs kerberos interface enable -lif lif_name -spn service_principal_name`
	
	f. Es sollte überprüft werden, dass Kerberos auf allen LIFs aktiviert ist:
	`vserver nfs kerberos interface show`

NFS Kerberos auf ONTAP LIFs aktivieren

Sie können den `vserver nfs kerberos interface enable` Befehl verwenden, um Kerberos auf einer Daten-LIF zu aktivieren. Dadurch kann die SVM Kerberos-Sicherheitsdienste für NFS verwenden.

Über diese Aufgabe

Wenn Sie einen Active Directory KDC verwenden, müssen die ersten 15 Zeichen aller verwendeten SPNs innerhalb eines Realms oder einer Domäne über alle SVMs hinweg eindeutig sein.

Schritte

1. Die NFS-Kerberos-Konfiguration erstellen:

   `vserver nfs kerberos interface enable -vserver` *`vserver_name`* `-lif` *`logical_interface`* `-spn` *`service_principal_name`*

   ONTAP benötigt den geheimen Schlüssel für den SPN vom KDC, damit die Kerberos-Schnittstelle aktiviert werden kann.

   Bei Microsoft KDCs wird der KDC kontaktiert und über die CLI eine Benutzername- und Kennwortabfrage angezeigt, um den geheimen Schlüssel zu erhalten. Wenn der SPN in einer anderen Organisationseinheit (OU) des Kerberos-Bereichs erstellt werden soll, kann der optionale `-ou` Parameter angegeben werden.

   Für Nicht-Microsoft-KDCs kann der geheime Schlüssel auf eine von zwei Arten bezogen werden:

Wenn Sie…	Dem Befehl ist außerdem der folgende Parameter hinzuzufügen…
Die KDC-Administratoranmeldeinformationen sind erforderlich, um den Schlüssel direkt vom KDC abzurufen.	`-admin-username` *`kdc_admin_username`*
Sie besitzen nicht die KDC-Administratoranmeldeinformationen, haben aber eine Keytab-Datei vom KDC, die den Schlüssel enthält	`-keytab-uri` {ftp

2. Es sollte überprüft werden, ob Kerberos auf der LIF aktiviert ist:

   `vserver nfs kerberos-config show`

3. Schritte 1 und 2 werden wiederholt, um Kerberos auf mehreren LIFs zu aktivieren.

Beispiel

Der folgende Befehl erstellt und überprüft eine NFS-Kerberos-Konfiguration für die SVM mit dem Namen vs1 auf der logischen Schnittstelle ves03-d1 mit dem SPN nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM in der OU lab2ou:

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
```

```
         Logical
Vserver  Interface Address       Kerberos  SPN
-------  --------- -------       --------- --------------------------------
vs0      ves01-a1
                   10.10.10.30   disabled  -
vs2      ves01-d1
                   10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.