Konfigurieren des NFS-Zugriffs auf eine SVM

ONTAP 9

NetApp
October 15, 2024

Inhalt

Konfigurieren des NFS-Zugriffs auf eine SVM . . . 1
Erstellen Sie ein SVM . . . 1
Vergewissern Sie sich, dass das NFS-Protokoll auf der SVM aktiviert ist . . . 2
Öffnen Sie die Exportrichtlinie für das SVM-Root-Volume . . . 3
Erstellen Sie einen NFS-Server . . . 4
Erstellen Sie eine LIF . . . 6
Aktivieren Sie DNS für die Auflösung des Host-Namens . . . 10
Konfigurieren Sie Name Services . . . 12
Hohe Sicherheit durch Kerberos mit NFS . . . 30
Hohe Sicherheit durch Verwendung von TLS mit NFS . . . 37

Konfigurieren des NFS-Zugriffs auf eine SVM

Erstellen Sie ein SVM

Wenn nicht bereits mindestens eine SVM in einem Cluster vorhanden ist, um den Datenzugriff für NFS-Clients zu ermöglichen, muss eine SVM erstellt werden.

Bevor Sie beginnen

- Ab ONTAP 9.13.1 können Sie die maximale Kapazität für eine Storage-VM festlegen. Sie können außerdem Warnmeldungen konfigurieren, wenn sich die SVM einem Kapazitätsschwellenwert nähert. Weitere Informationen finden Sie unter Management der SVM-Kapazität.

Schritte

1. 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`*

   - Verwenden Sie die UNIX-Einstellung für die `-rootvolume-security-style` Option.
   - Verwenden Sie die Standardoption C.UTF-8 `-language`.
   - Die `ipspace` Einstellung ist optional.

2. Konfiguration und Status der neu erstellten SVM überprüfen:

   `vserver show -vserver` *`vserver_name`*

   Das `Allowed Protocols` Feld muss NFS enthalten. Sie können diese Liste später bearbeiten.

   Das `Vserver Operational State` Feld muss den `running` Status anzeigen. Wenn auf der Statusanzeige der `initializing` Status angezeigt wird, ist ein Zwischenvorgang wie das Erstellen des Root-Volumes fehlgeschlagen, und Sie müssen die SVM löschen und neu erstellen.

Beispiele

Mit dem folgenden Befehl wird eine SVM für den Datenzugriff im IPspace ipspace A erstellt:

```
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
```

Mit dem folgenden Befehl wird angezeigt, dass eine SVM mit einem 1-GB-Root-Volume erstellt wurde und dieses automatisch gestartet wurde und sich im `running` Status befindet. Das Root-Volume verfügt über eine standardmäßige Exportrichtlinie, 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 können Sie eine Vorlage für anpassungsfähige QoS-Richtliniengruppen festlegen und dabei einen Durchsatz- und Höchstwert für Volumes in dieser SVM anwenden. Sie können diese Richtlinie nur anwenden, nachdem Sie die SVM erstellt haben. Weitere Informationen zu diesem Prozess finden Sie unter Legen Sie eine Vorlage für adaptive Richtliniengruppen fest.

Vergewissern Sie sich, dass das NFS-Protokoll auf der SVM aktiviert ist

Bevor Sie NFS auf SVMs konfigurieren und verwenden können, müssen Sie sicherstellen, dass das Protokoll aktiviert ist.

Über diese Aufgabe

Dies geschieht normalerweise während des SVM Setups. Wenn Sie das Protokoll jedoch während des Setups nicht aktiviert haben, können Sie es später über den `vserver add-protocols` Befehl aktivieren.

> Sobald ein Protokoll erstellt wurde, können Sie es nicht mehr zu einem LIF hinzufügen oder daraus entfernen.

Sie können auch Protokolle für SVMs mit dem `vserver remove-protocols` Befehl deaktivieren.

Schritte

1. Überprüfen Sie, welche Protokolle derzeit für die SVM aktiviert und deaktiviert sind:

   `vserver show -vserver vserver_name -protocols`

   Außerdem können Sie mit dem `vserver show-protocols` Befehl die derzeit aktivierten Protokolle auf allen SVMs im Cluster anzeigen.

2. Aktivieren oder deaktivieren Sie gegebenenfalls ein Protokoll:
   - So aktivieren Sie das NFS-Protokoll:
     `vserver add-protocols -vserver vserver_name -protocols nfs`
   - So deaktivieren Sie ein Protokoll:
     `vserver remove-protocols -vserver vserver_name -protocols protocol_name [,protocol_name,…]`
3. Vergewissern Sie sich, dass die aktivierten und deaktivierten Protokolle korrekt aktualisiert wurden:

   `vserver show -vserver vserver_name -protocols`

Beispiel

Mit dem folgenden Befehl werden auf der SVM namens vs1 angezeigt, welche Protokolle derzeit aktiviert bzw. deaktiviert (zulässig und nicht zulässig) sind:

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

Mit dem folgenden Befehl können Sie auf NFS zugreifen, indem Sie `nfs` der Liste der aktivierten Protokolle auf der SVM mit dem Namen vs1 hinzufügen:

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

Öffnen Sie die Exportrichtlinie für das SVM-Root-Volume

Die standardmäßige Exportrichtlinie für das SVM-Root-Volume muss eine Regel enthalten, um allen Clients einen offenen Zugriff über NFS zu ermöglichen. Ohne diese Regel erhält jeder NFS-Client Zugriff auf die SVM und ihre Volumes.

Über diese Aufgabe

Wenn eine neue SVM erstellt wird, wird automatisch eine standardmäßige Exportrichtlinie (Standard) für das Root-Volume der SVM erstellt. Sie müssen eine oder mehrere Regeln für die Standard-Exportrichtlinie erstellen, bevor Clients auf Daten auf der SVM zugreifen können.

Sie sollten überprüfen, ob der Zugriff für alle NFS Clients in der Standard-Exportrichtlinie zugänglich ist, und

Sie später den Zugriff auf einzelne Volumes beschränken, indem Sie benutzerdefinierte Exportrichtlinien für einzelne Volumes oder qtrees erstellen.

Schritte

1. Wenn Sie eine vorhandene SVM verwenden, prüfen Sie die standardmäßige Root Volume-Exportrichtlinie:

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

   Die Befehlsausgabe sollte wie die folgenden sein:

   ```
   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
   ```

   Wenn eine solche Regel vorhanden ist, die einen offenen Zugriff ermöglicht, ist diese Aufgabe abgeschlossen. Falls nicht, fahren Sie mit dem nächsten Schritt fort.

2. 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 durch Kerberos gesicherte Volumes enthält, können Sie die Optionen `-rorule` `-rwrule` `-superuser` für die Exportregel , und für das Root-Volume auf `krb5` oder festlegen `krb5i`. Beispiel:

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

3. Überprüfen Sie die Regelerstellung mit dem `vserver export-policy rule show` Befehl.

Ergebnis

Jeder NFS-Client kann jetzt auf alle Volumes oder qtree zugreifen, die auf der SVM erstellt wurden.

Erstellen Sie einen NFS-Server

Nachdem Sie die Überprüfung durchgeführt `vserver nfs create` haben, ob NFS auf Ihrem Cluster lizenziert ist, können Sie mit dem Befehl einen NFS-Server auf der SVM

erstellen und die unterstützten NFS-Versionen angeben.

Über diese Aufgabe

Die SVM kann so konfiguriert werden, dass eine oder mehrere NFS-Versionen unterstützt werden. Wenn Sie NFSv4 oder höher unterstützen:

- Der NFSv4-Benutzer-ID-Domänenname muss auf dem NFSv4-Server und den Ziel-Clients derselbe sein.

  Der Name eines LDAP- oder NIS-Domain muss nicht unbedingt identisch sein, solange der NFSv4-Server und die Clients den gleichen Namen verwenden.

- Die Ziel-Clients müssen die Einstellung für die numerische NFSv4-ID unterstützen.
- Aus Sicherheitsgründen sollten Sie LDAP für Namensdienste in NFSv4-Bereitstellungen verwenden.

Bevor Sie beginnen

Die SVM muss für die Unterstützung des NFS-Protokolls konfiguriert worden sein.

Schritte

1. Vergewissern Sie sich, dass NFS für Ihr Cluster lizenziert ist:

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

   Falls nicht, wenden Sie sich an Ihren Vertriebsmitarbeiter.

2. Erstellen eines NFS-Servers:

   ```
   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 die beliebige Kombination von NFS-Versionen aktivieren. Wenn Sie pNFS unterstützen möchten, müssen Sie beide `-v4.1 -v4.1-pnfs` Optionen aktivieren.

   Wenn Sie Version 4 oder höher aktivieren, sollten Sie auch sicher sein, dass die folgenden Optionen richtig eingestellt sind:

   - `-v4-id-domain`

     Dieser optionale Parameter gibt den Domain-Teil des String-Formteils von Benutzer- und Gruppennamen an, wie durch das NFSv4-Protokoll definiert. Standardmäßig verwendet ONTAP die NIS-Domäne, wenn eine festgelegt ist; wenn nicht, wird die DNS-Domäne verwendet. Sie müssen einen Wert angeben, der dem von den Zielclients verwendeten Domänennamen entspricht.

   - `-v4-numeric-ids`

     Dieser optionale Parameter gibt an, ob die Unterstützung für numerische String-IDs in NFSv4-Besitzattributen aktiviert ist. Die Standardeinstellung ist aktiviert, Sie sollten jedoch prüfen, ob die Zielclients sie unterstützen.

   Sie können zusätzliche NFS-Funktionen später mit dem `vserver nfs modify` Befehl aktivieren.

3. Überprüfen Sie, ob NFS ausgeführt wird:

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

4. Vergewissern Sie sich, dass NFS nach Bedarf konfiguriert ist:

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

Beispiele

Mit dem folgenden Befehl wird ein NFS-Server auf der SVM namens vs1 mit NFSv3 und NFSv4.0 aktiviert erstellt:

```
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 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
...
```

Erstellen Sie eine LIF

Ein LIF ist eine IP-Adresse, die einem physischen oder logischen Port zugewiesen ist. Falls eine Komponente ausfällt, kann ein LIF ein Failover auf einen anderen physischen Port durchführen oder zu einem anderen migrieren, sodass weiterhin mit dem Netzwerk kommunizieren wird.

Was Sie benötigen

- Der zugrunde liegende physische oder logische Netzwerkport muss im Administratorstatus konfiguriert worden `up` sein.
- Wenn Sie planen, einen Subnetznamen zu verwenden, um die IP-Adresse und den Netzwerkmaskenwert für eine LIF zuzuweisen, muss das Subnetz bereits vorhanden sein.

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

- Der Mechanismus zur Angabe der von einem LIF bearbeiteten Traffic-Art ist geändert. Für ONTAP 9.5 und früher verwendeten LIFs Rollen, um den Typ des Datenverkehrs anzugeben, den er verarbeiten würde. Ab ONTAP 9.6 verwenden LIFs Service-Richtlinien, um den Typ des Datenverkehrs anzugeben, den es verarbeiten würde.

Über diese Aufgabe

- Sie können am gleichen Netzwerkport IPv4- und IPv6-LIFs erstellen.
- Wenn Sie Kerberos-Authentisierung verwenden, aktivieren Sie Kerberos auf mehreren LIFs.
- Wenn Sie im Cluster eine große Anzahl von LIFs enthalten sind, können Sie die auf dem Cluster unterstützte LIF- `network interface capacity show`Kapazität überprüfen. Verwenden Sie dazu den Befehl und die auf jedem Node unterstützte LIF-Kapazität. Hierzu können Sie mit dem `network interface capacity details show` Befehl (auf der erweiterten Berechtigungsebene) nachprüfen.
- Wenn bereits ab ONTAP 9.7 andere LIFs für die SVM im selben Subnetz vorhanden sind, müssen Sie den Home Port der LIF nicht angeben. ONTAP wählt automatisch einen zufälligen Port auf dem angegebenen Home-Node in derselben Broadcast-Domäne wie die anderen LIFs, die bereits im selben Subnetz konfiguriert sind.

Ab ONTAP 9.4 wird FC-NVMe unterstützt. Wenn Sie eine FC-NVMe-LIF erstellen, sollten Sie Folgendes 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 eine logische Schnittstelle für den Management-Datenverkehr konfiguriert werden.
- NVMe LIFs und Namespaces müssen auf demselben Node gehostet werden.
- Pro SVM kann nur eine NVMe-LIF konfiguriert werden, die den Datenverkehr verarbeitet

Schritte

1. 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}
   ```

Option	Beschreibung
ONTAP 9.5 und früher	`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 ein LIF mithilfe einer Service-Richtlinie erstellt wird (ab ONTAP 9.6).
- Der `-data-protocol` Parameter muss bei der Erstellung der LIF angegeben werden. Eine spätere Änderung ist nur dann möglich, wenn die Daten-LIF zerstört und neu erstellt wird.

  Der `-data-protocol` Parameter ist nicht erforderlich, wenn eine LIF mithilfe einer Service-Richtlinie erstellt wird (beginnend mit ONTAP 9.6).

- `-home-node` Ist der Node, zu dem das LIF zurückgibt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.

  Sie können außerdem angeben, ob die LIF mithilfe der `-auto-revert` Option automatisch zum Home Node und Home Port zurückgesetzt werden soll.

- `-home-port` Ist der physische oder logische Port, zu dem die LIF zurückgibt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.
- Sie können eine IP-Adresse mit den `-address -netmask` Optionen und angeben oder die Zuweisung aus einem Subnetz mit der `-subnet_name` Option aktivieren.
- Wenn Sie zur Versorgung der IP-Adresse und Netzwerkmaske ein Subnetz verwenden, wird bei einem Gateway automatisch eine Standardroute zu diesem Gateway zur SVM hinzugefügt, wenn mithilfe dieses Subnetzes eine LIF erstellt wird.
- Wenn Sie IP-Adressen manuell zuweisen (ohne ein Subnetz zu verwenden), müssen Sie möglicherweise eine Standardroute zu einem Gateway konfigurieren, wenn Clients oder Domänen-Controller in einem anderen IP-Subnetz vorhanden sind. Die `network route create` man-Page enthält Informationen zum Erstellen einer statischen Route innerhalb einer SVM.
- `-firewall-policy`Verwenden Sie für die Option denselben Standard `data` wie die LIF-Rolle.

  Sie können bei Bedarf später eine benutzerdefinierte Firewallrichtlinie erstellen und hinzufügen.

  > Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und werden vollständig durch LIF-Servicerichtlinien ersetzt. Weitere Informationen finden Sie unter "Konfigurieren Sie Firewallrichtlinien für LIFs".

- `-auto-revert` Ermöglicht Ihnen die Angabe, ob eine Daten-LIF automatisch auf ihren Home Node zurückgesetzt wird, wenn beispielsweise ein Start erfolgt, Änderungen am Status der Managementdatenbank oder die Netzwerkverbindung hergestellt wird. Die Standardeinstellung ist `false`, Sie können sie jedoch `false` abhängig von den Netzwerkverwaltungsrichtlinien in Ihrer Umgebung auf festlegen.

2. Überprüfen Sie mit dem `network interface show` Befehl, ob das LIF erfolgreich erstellt wurde.
3. Vergewissern Sie sich, dass die konfigurierte IP-Adresse erreichbar ist:

Überprüfen einer…	Verwenden…
IPv4-Adresse	`network ping`
IPv6-Adresse	`network ping6`

4. Wenn Sie Kerberos verwenden, wiederholen Sie die Schritte 1 bis 3, um weitere LIFs zu erstellen.

   Kerberos muss auf jedem dieser LIFs separat aktiviert werden.

Beispiele

Mit dem folgenden Befehl wird eine LIF erstellt und die Werte der IP-Adresse und Netzwerkmaske anhand der `-address -netmask` Parameter und angegeben:

```
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
```

Mit dem folgenden Befehl wird eine LIF erstellt und dem angegebenen Subnetz (namens client1_sub) IP-Adresse und Netzwerkmaskenwerte zugewiesen:

```
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
```

Mit dem folgenden Befehl werden alle LIFs in Cluster-1 angezeigt. Datenschnittstellen Datenschnittstellen Datenverbund Daten3 werden mit IPv4-Adressen konfiguriert und Daten3 wird 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 eine NAS-Daten-LIF erstellt wird, die der `default-data-files` Service-Richtlinie zugewiesen ist:

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

Aktivieren Sie DNS für die Auflösung des Host-Namens

Sie können mit dem `vserver services name-service dns` Befehl DNS auf einer SVM aktivieren und für die Verwendung von DNS für die Auflösung von Host-Namen

konfigurieren. Host-Namen werden mithilfe externer DNS-Server aufgelöst.

Was Sie benötigen

Ein standortweiter DNS-Server muss für die Suche nach Hostnamen verfügbar sein.

Sie sollten mehrere DNS-Server konfigurieren, um Single Point of Failure zu vermeiden. `vserver services name-service dns create`Wenn Sie nur einen DNS-Servernamen eingeben, gibt der Befehl eine Warnung aus.

Über diese Aufgabe

Der *Network Management Guide* enthält Informationen zur 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`

   Mit dem folgenden Befehl werden externe DNS-Server auf der SVM vs1 aktiviert:

   ```
   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
   ```

   > Ab ONTAP 9.2 `vserver services name-service dns create` führt der Befehl eine automatische Konfigurationsprüfung durch und meldet eine Fehlermeldung, wenn ONTAP den Name Server nicht kontaktieren kann.

2. Zeigen Sie die DNS-Domänenkonfigurationen mit dem `vserver services name-service dns show` Befehl an.

   Mit dem folgenden Befehl werden die DNS-Konfigurationen für alle SVMs im Cluster angezeigt:

   ```
   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
   ```

   Mit dem folgenden Befehl werden detaillierte DNS-Konfigurationsinformationen für SVM vs1 angezeigt:

```
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. Überprüfen Sie den Status der Namensserver mit dem `vserver services name-service dns check` Befehl.

   Der `vserver services name-service dns check` Befehl ist ab ONTAP 9.2 verfügbar.

```
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
```

Konfigurieren Sie Name Services

Name Services – Übersicht konfigurieren

Je nach der Konfiguration Ihres Storage-Systems muss ONTAP in der Lage sein, Host-, Benutzer-, Gruppen- oder Netzwerkgruppeninformationen zu suchen, um Clients ordnungsgemäßen Zugriff zu ermöglichen. Sie müssen Name Services konfigurieren, damit ONTAP auf lokale oder externe Namensservices zugreifen kann, um diese Informationen abzurufen.

Sie sollten einen Namensdienst wie NIS oder LDAP verwenden, um die Suche nach Namen während der Client-Authentifizierung zu erleichtern. Für mehr Sicherheit empfiehlt es sich, LDAP nach Möglichkeit zu verwenden, insbesondere bei der Bereitstellung von NFSv4 oder neuer. Sie sollten auch lokale Benutzer und Gruppen konfigurieren, falls keine externen Namensserver verfügbar sind.

Informationen zum Namensdienst müssen auf allen Quellen synchronisiert bleiben.

Konfigurieren Sie die Tabelle Service Switch Name

Sie müssen die Switch-Tabelle für den Namensdienst richtig konfigurieren, damit ONTAP Informationen zur Zuordnung von Host-, Benutzer-, Gruppen-, Netzwerkgruppen- oder Namenszuordnungen abrufen kann.

Was Sie benötigen

Sie müssen entschieden haben, welche Namensdienste Sie für die Zuordnung von Host, Benutzer, Gruppe, Netzgruppe oder Name verwenden möchten, je nachdem, welche für Ihre Umgebung relevant sind.

Wenn Sie Netzgruppen verwenden möchten, müssen alle in Netzgruppen angegebenen IPv6-Adressen gekürzt und komprimiert werden, wie in RFC 5952 angegeben.

Über diese Aufgabe

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

Schritte

1. Fügen Sie die erforderlichen Einträge zur Tabelle des Namensdienstschalters hinzu:

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

2. Vergewissern Sie sich, dass die Tabelle des Namensdienstschalters 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` `vserver services name-service ns-switch delete` Befehle oder verwenden.

Beispiel

Im folgenden Beispiel wird ein neuer Eintrag in der Namensservice-Switch-Tabelle erstellt, in der die SVM vs1 die lokale netgroup-Datei und ein externer NIS-Server zum Nachsuchen von Netzgruppeninformationen in dieser Reihenfolge verwendet:

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

Nachdem Sie fertig sind

- Sie müssen die von Ihnen angegebenen Namensservices konfigurieren, damit die SVM den Datenzugriff ermöglicht.
- Wenn Sie einen Namensservice für die SVM löschen, müssen Sie ihn auch aus der Name Service Switch-Tabelle entfernen.

  Der Client-Zugriff auf das Storage-System funktioniert möglicherweise nicht wie erwartet, wenn Sie den Namensservice aus der Switch-Tabelle namens Service nicht löschen können.

Konfigurieren Sie lokale UNIX-Benutzer und -Gruppen

Lokale UNIX-Benutzer und Gruppen – Übersicht konfigurieren

Zur Authentifizierung und Namenszuordnungen können lokale UNIX Benutzer und Gruppen auf der SVM verwendet werden. Sie können UNIX-Benutzer und -Gruppen manuell erstellen oder eine Datei mit UNIX-Benutzern oder -Gruppen von einer einheitlichen Ressourcen-ID (URI) laden.

Es gibt eine standardmäßige Maximalgrenze von 32,768 lokalen UNIX-Benutzergruppen und Gruppenmitgliedern, die im Cluster kombiniert wurden. Der Cluster-Administrator kann diesen Grenzwert ändern.

Erstellen Sie einen lokalen UNIX-Benutzer

Mit dem `vserver services name-service unix-user create` Befehl können Sie lokale UNIX-Benutzer erstellen. Ein lokaler UNIX-Benutzer ist ein UNIX-Benutzer, den Sie auf der SVM als UNIX Name Services-Option erstellen, der bei der Verarbeitung von Namenszuordnungen verwendet werden soll.

Schritt

1. Erstellen Sie einen lokalen UNIX-Benutzer:

   `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 muss mindestens 64 Zeichen lang sein.

   `-id` *`integer`* Gibt die Benutzer-ID an, die Sie zuweisen.

   `-primary-gid` *`integer`* Gibt die primäre Gruppen-ID an. Dadurch wird der Benutzer zur primären Gruppe hinzugefügt. Nach dem Erstellen des Benutzers können Sie den Benutzer manuell zu jeder gewünschten zusätzlichen Gruppe hinzufügen.

Beispiel

Mit dem folgenden Befehl wird ein lokaler UNIX-Benutzer namens johnm (voller Name „John Miller“) auf der SVM mit dem Namen vs1 erstellt. 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"
```

Laden Sie lokale UNIX-Benutzer von einem URI

Als Alternative zur manuellen Erstellung einzelner lokaler UNIX-Benutzer in SVMs können Sie diese Aufgabe vereinfachen, indem Sie eine Liste lokaler UNIX-Benutzer aus einer Uniform Resource Identifier (URI) in SVMs laden(`vserver services name-service unix-user load-from-uri`.

Schritte

1. Erstellen Sie eine Datei mit der Liste der lokalen UNIX-Benutzer, die Sie laden möchten.

   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. Vergewissern Sie sich, dass die Liste keine doppelten Informationen enthält.

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

3. Kopieren Sie die Datei auf einen Server.

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

4. Legen Sie fest, was der URI für die Datei ist.

   Der URI ist die Adresse, die Sie dem Speichersystem zur Angabe des Speicherortes angeben.

5. Laden Sie die Datei mit der Liste der lokalen UNIX-Benutzer von der URI in SVMs:

   `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 sollen. Der Standardwert ist `false`.

Beispiel

Mit dem folgenden Befehl `ftp://ftp.example.com/passwd` wird eine Liste lokaler UNIX-Benutzer aus dem URI in die SVM mit dem Namen vs1 geladen. Vorhandene Benutzer auf dem SVM werden nicht durch die Informationen des URI überschrieben.

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

Erstellen Sie eine lokale UNIX-Gruppe

Mit dem `vserver services name-service unix-group create` Befehl können Sie UNIX-Gruppen erstellen, die in der SVM lokal sind. Lokale UNIX Gruppen werden mit lokalen UNIX Benutzern verwendet.

Schritt

1. Erstellen einer lokalen UNIX-Gruppe:

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

   `-name` *`group_name`* Gibt den Gruppennamen an. Der Gruppenname muss mindestens 64 Zeichen lang sein.

   `-id` *`integer`* Gibt die Gruppen-ID an, die Sie zuweisen.

Beispiel

Mit dem folgenden Befehl wird eine lokale Gruppe mit dem Namen „eng“ auf der SVM „vs1“ erstellt. Die Gruppe hat die ID 101.

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

Fügen Sie einen Benutzer zu einer lokalen UNIX-Gruppe hinzu

Mit dem `vserver services name-service unix-group adduser` Befehl können Sie einen Benutzer zu einer ergänzenden UNIX-Gruppe hinzufügen, die sich lokal in der SVM befindet.

Schritt

1. 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, der der Benutzer zusätzlich zur primären Gruppe des Benutzers hinzugefügt werden soll.

Beispiel

Mit dem folgenden Befehl wird eine lokale UNIX-Gruppe mit dem Namen „eng“ auf der SVM „vs1“ mit dem Namen „max“ hinzugefügt:

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

Laden Sie lokale UNIX-Gruppen von einem URI

Alternativ zum manuellen Erstellen einzelner lokaler UNIX-Gruppen können Sie mit dem `vserver services name-service unix-group load-from-uri` Befehl eine Liste lokaler UNIX-Gruppen aus einer Uniform Resource Identifier (URI) in SVMs laden.

Schritte

1. Erstellen Sie eine Datei mit der Liste der lokalen UNIX-Gruppen, die Sie laden möchten.

   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. Vergewissern Sie sich, dass die Liste keine doppelten Informationen enthält.

   Die Liste darf keine doppelten Einträge enthalten, sonst schlägt das Laden der Liste fehl. Wenn bereits Einträge in der SVM vorhanden sind, müssen Sie entweder den `-overwrite` Parameter `true` so einstellen, dass alle vorhandenen Einträge mit der neuen Datei überschrieben werden, oder sicherstellen, dass die neue Datei keine Einträge enthält, die vorhandene Einträge duplizieren.

3. Kopieren Sie die Datei auf einen Server.

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

4. Legen Sie fest, was der URI für die Datei ist.

   Der URI ist die Adresse, die Sie dem Speichersystem zur Angabe des Speicherortes angeben.

5. Laden Sie die Datei mit der Liste der lokalen UNIX-Gruppen von der URI in die SVM:

   `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 sollen. Der Standardwert ist `false`. Wenn Sie diesen Parameter als angeben `true`, ersetzt ONTAP die gesamte vorhandene lokale UNIX-Gruppendatenbank der angegebenen SVM durch die Einträge aus der zu ladenen Datei.

Beispiel

Mit dem folgenden Befehl `ftp://ftp.example.com/group` wird eine Liste der lokalen UNIX-Gruppen aus dem URI in die SVM mit dem Namen vs1 geladen. Vorhandene Gruppen auf der SVM werden nicht durch die Informationen des URI überschrieben.

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

Arbeiten Sie mit Netzgruppen

Arbeiten mit Netzgruppen Übersicht

Sie können Netzgruppen zur Benutzerauthentifizierung verwenden und Clients in den Regeln für Exportrichtlinien zuordnen. Sie können den Zugriff auf Netzwerkgruppen von externen Namensservern (LDAP oder NIS) aus ermöglichen oder Sie können mit dem `vserver services name-service netgroup load` Befehl Netzgruppen von einer einheitlichen Ressourcen-ID (URI) in SVMs laden.

Was Sie benötigen

Bevor Sie mit Netzgruppen arbeiten, müssen Sie sicherstellen, dass die folgenden Bedingungen erfüllt sind:

- Alle Hosts in Netgroups, unabhängig von den Quelldateien (NIS, LDAP oder lokale Dateien), müssen sowohl vorwärts (A) als auch rückwärts (PTR) DNS-Einträge enthalten, um eine konsistente vorwärts- und rückwärts-DNS-Suche zu ermöglichen.

  Wenn zudem eine IP-Adresse eines Clients mehrere PTR-Datensätze hat, müssen alle diese Hostnamen

Mitglieder der Netzwerkgruppe sein und entsprechende Datensätze haben.

- Die Namen aller Hosts in Netzwerkgruppen müssen unabhängig von ihrer Quelle (NIS, LDAP oder lokale Dateien) korrekt geschrieben werden und den richtigen Fall verwenden. Falls Inkonsistenzen bei in Netzgruppen verwendeten Hostnamen zu unerwarteten Verhaltensweisen führen können, z. B. fehlgeschlagene Exportprüfungen.
- Alle IPv6-Adressen, die in Netzgruppen angegeben sind, müssen gekürzt und komprimiert werden, wie in RFC 5952 angegeben.

  Beispiel: 2011:hu9:0:0:0:0:3:1 muss verkürzt werden auf 2011:hu9::3:1.

Über diese Aufgabe

Wenn Sie mit Netzgruppen arbeiten, können Sie die folgenden Vorgänge ausführen:

- Mit dem `vserver export-policy netgroup check-membership` Befehl können Sie feststellen, ob eine Client-IP Mitglied einer bestimmten Netzgruppe ist.
- Mit dem `vserver services name-service getxxbyyy netgrp` Befehl können Sie überprüfen, ob ein Client Teil einer Netzgruppe ist.

  Der zugrunde liegende Service für die Suche wird basierend auf der konfigurierten Name-Service-Switch-Reihenfolge ausgewählt.

Laden Sie Netzgruppen in SVMs

Eine der Methoden, die Sie verwenden können, um Clients in den Regeln der Exportrichtlinie zu entsprechen, ist die Verwendung von Hosts, die in netgroups aufgeführt sind. Sie können Netzgruppen aus einer einheitlichen Ressourcen-Kennung (URI) in SVMs laden(`vserver services name-service netgroup load`, als Alternative zur Verwendung von Netzwerkgruppen, die in externen Namensservern gespeichert sind.

Was Sie benötigen

Netzwerkgruppendateien müssen die folgenden Anforderungen erfüllen, bevor sie in eine SVM geladen werden:

- Die Datei muss dasselbe Netgroup-Textdateiformat verwenden, das zum Befüllen von NIS verwendet wird.

  ONTAP überprüft das Format der netgroup-Textdatei, bevor sie geladen wird. Wenn die Datei Fehler enthält, wird sie nicht geladen und es wird eine Meldung angezeigt, die die Korrekturen anzeigt, die Sie in der Datei vornehmen müssen. Nach der Behebung der Fehler können Sie die Netzwerkgruppendatei erneut in die angegebene SVM laden.

- Alle alphabetischen Zeichen in den Hostnamen in der Netzwerkgruppedatei müssen klein geschrieben werden.
- Die maximal unterstützte Dateigröße beträgt 5 MB.
- Die maximal unterstützte Stufe für das Nesting von Netzgruppen ist 1000.
- Bei der Definition von Hostnamen in der Netzwerkgruppendatei können nur primäre DNS-Hostnamen verwendet werden.

  Um Probleme beim Export von Zugriffsrechten zu vermeiden, sollten Hostnamen nicht mithilfe von DNS

CNAME- oder Round-Robin-Datensätzen definiert werden.

- Der Benutzer- und Domain-Anteil von Dreieckskomponenten in der netgroup-Datei sollte leer bleiben, da ONTAP sie nicht unterstützt.

  Es wird nur der Host/IP-Teil unterstützt.

Über diese Aufgabe

ONTAP unterstützt die Suche nach der lokalen Netzwerkgruppedatei von Netgroup zu Host. Nachdem Sie die netgroup-Datei geladen haben, erstellt ONTAP automatisch eine netgroup.byhost-Zuordnung, um netgroup-by-Host-Suchen zu aktivieren. Dies kann die Suche lokaler Netzgruppen erheblich beschleunigen, wenn die Regeln für Exportrichtlinien verarbeitet werden, um den Client-Zugriff zu bewerten.

Schritt

1. Laden Sie Netzgruppen aus einem URI in SVMs:

   `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-Karte kann mehrere Minuten dauern.

   Wenn Sie die Netzgruppen aktualisieren möchten, können Sie die Datei bearbeiten und die aktualisierte Netzwerkgruppendatei in die SVM laden.

Beispiel

Mit dem folgenden Befehl werden Netzgruppen-Definitionen von der HTTP-URL in die SVM namens vs1 geladen `http://intranet/downloads/corp-netgroup`:

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

Überprüfen Sie den Status der Netgroup-Definitionen

Nachdem Sie netgroups in die SVM geladen haben, können Sie mit dem `vserver services name-service netgroup status` Befehl den Status der netgroup-Definitionen überprüfen. So können Sie feststellen, ob für alle Nodes, die die SVM zurückgeben, Netgroup-Definitionen konsistent sind.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   `set -privilege advanced`

2. Überprüfen Sie den Status der Netgroup-Definitionen:

   `vserver services name-service netgroup status`

   Sie können zusätzliche Informationen in einer detaillierteren Ansicht anzeigen.

3. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

Beispiel

Nachdem die Berechtigungsebene festgelegt wurde, wird mit dem folgenden Befehl der Status als netgroup für alle SVMs angezeigt:

```
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
```

Erstellen Sie eine NIS-Domänenkonfiguration

Wenn in Ihrer Umgebung ein Network Information Service (NIS) für Namensdienste verwendet wird, müssen Sie mit dem `vserver services name-service nis-domain create` Befehl eine NIS-Domänenkonfiguration für die SVM erstellen.

Bevor Sie beginnen

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

Wenn Sie NIS für die Verzeichnissuchung verwenden möchten, dürfen die Karten in Ihren NIS-Servern nicht mehr als 1,024 Zeichen für jeden Eintrag enthalten. Geben Sie den NIS-Server nicht an, der dieser Beschränkung nicht entspricht. Andernfalls kann der Client-Zugriff, der von NIS-Einträgen abhängig ist, fehlschlagen.

Über diese Aufgabe

Wenn Ihre NIS-Datenbank eine `netgroup.byhost` Karte enthält, kann ONTAP sie für schnellere Suchvorgänge verwenden. Die `netgroup.byhost` und- `netgroup`Zuordnungen im Verzeichnis müssen jederzeit synchron gehalten werden, um Probleme mit dem Client-Zugriff zu

vermeiden. Ab ONTAP 9.7 `netgroup.byhost` können NIS-Einträge mit den `vserver services name-service nis-domain netgroup-database` Befehlen zwischengespeichert werden.

Die Verwendung von NIS für die Auflösung des Host-Namens 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.

   > Ab ONTAP 9.2 `-nis-servers` ersetzt das Feld das Feld `-servers`. Dieses neue Feld kann entweder einen Hostnamen oder eine IP-Adresse für den NIS-Server enthalten.

2. Vergewissern Sie sich, dass die Domäne erstellt wurde:

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

Beispiel

Mit dem folgenden Befehl wird eine NIS-Domänenkonfiguration für eine NIS-Domäne erstellt, die auf der SVM `vs1` mit einem NIS-Server an der IP-Adresse `192.0.2.180` aufgerufen `nisdomain` wird:

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

LDAP verwenden

Überblick über die Verwendung von LDAP

Wenn in Ihrer Umgebung LDAP für Name-Services verwendet wird, müssen Sie gemeinsam mit Ihrem LDAP-Administrator die Anforderungen und die entsprechenden Speichersystemkonfigurationen ermitteln und die SVM als LDAP-Client aktivieren.

Ab ONTAP 9.10.1 wird die LDAP-Kanalbindung standardmäßig sowohl für LDAP-Verbindungen von Active Directory- als auch für Namensdienste unterstützt. ONTAP versucht die Channel-Bindung mit LDAP-Verbindungen nur dann, wenn Start-TLS oder LDAPS aktiviert ist und die Sitzungssicherheit entweder auf Signieren oder Seal gesetzt ist. Um `-try-channel-binding` `ldap client modify` die LDAP-Kanalbindung mit Nameservern zu deaktivieren oder wieder zu aktivieren, verwenden Sie den Parameter mit dem Befehl.

Weitere Informationen finden Sie unter "2020 LDAP-Channel-Binding und LDAP-Signing-Anforderungen für Windows".

- Bevor Sie LDAP für ONTAP konfigurieren, sollten Sie überprüfen, ob die Standortbereitstellung die Best Practices für die LDAP-Server- und Client-Konfiguration erfüllt. Insbesondere sind folgende Voraussetzungen zu erfüllen:
  - Der Domänenname des LDAP-Servers muss mit dem Eintrag auf dem LDAP-Client übereinstimmen.

- Die vom LDAP-Server unterstützten LDAP-Benutzerpasswort-Hash-Typen müssen die von ONTAP unterstützten LDAP-Benutzerpasswort-Typen enthalten:
  - CRYPT (alle Typen) und SHA-1 (SHA, SSHA).
  - Beginnend mit ONTAP 9.8, SHA-2-Hashes (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384 und SSHA-512) werden ebenfalls unterstützt.
- Wenn für den LDAP-Server Sitzungssicherheitsmaßnahmen erforderlich sind, müssen Sie diese im LDAP-Client konfigurieren.

  Folgende Sicherheitsoptionen sind verfügbar:

  - LDAP-Signatur (bietet Datenintegritätsprüfung) und LDAP-Signing and Sealing (bietet Datenintegritätsprüfung und -Verschlüsselung)
  - STARTEN SIE TLS
  - LDAPS (LDAP über TLS oder SSL)
- Um signierte und versiegelte LDAP-Abfragen zu aktivieren, müssen die folgenden Dienste konfiguriert sein:
  - LDAP-Server müssen den GSSAPI (Kerberos) SASL-Mechanismus unterstützen.
  - LDAP-Server müssen DNS-A/AAAA-Datensätze sowie PTR-Datensätze auf dem DNS-Server eingerichtet haben.
  - Kerberos-Server müssen über SRV-Datensätze auf dem DNS-Server verfügen.
- Um TLS ODER LDAPS ZU STARTEN, sollten die folgenden Punkte berücksichtigt werden.
  - Es handelt sich hierbei um eine NetApp Best Practice, Start TLS statt LDAPS zu verwenden.
  - Bei Verwendung von LDAPS muss der LDAP-Server für TLS oder für SSL in ONTAP 9.5 und höher aktiviert sein. SSL wird in ONTAP 9.0-9.4 nicht unterstützt.
  - Ein Zertifikatsserver muss bereits in der Domäne konfiguriert sein.
- Um LDAP-Verweisungsjagd zu ermöglichen (in ONTAP 9.5 und höher), müssen die folgenden Bedingungen erfüllt sein:
  - Beide Domänen sollten mit einer der folgenden Vertrauensbeziehungen konfiguriert werden:
    - Zwei-Wege
    - Eine Möglichkeit, bei der der primäre vertraut auf die Empfehlungsdomäne
    - Elternteil-Kind
  - DNS muss so konfiguriert sein, dass alle genannten Servernamen aufgelöst werden.
  - Domänenpasswörter sollten für die Authentifizierung identisch sein, wenn --bind-as-cifs-Server auf true gesetzt ist.

Die folgenden Konfigurationen werden mit LDAP-Referenznachverfolgungsjagd nicht unterstützt.

- Für alle ONTAP-Versionen:
  - LDAP-Clients auf einer Administrator-SVM
- Für ONTAP 9.8 und frühere Versionen (unterstützt ab 9.9.1):
  - LDAP-Signing and Sealing (`-session-security`optional)
  - Verschlüsselte TLS-Verbindungen (`-use-start-tls`Option)
  - Kommunikation über LDAPS-Port 636 (`-use-ldaps-for-ad-ldap`optional)

- Sie müssen beim Konfigurieren des LDAP-Clients auf der SVM ein LDAP-Schema eingeben.

  In den meisten Fällen ist eines der Standard-ONTAP-Schemas angemessen. Wenn sich das LDAP-Schema in Ihrer Umgebung jedoch von diesen unterscheidet, müssen Sie ein neues LDAP-Client-Schema für ONTAP erstellen, bevor Sie den LDAP-Client erstellen. Wenden Sie sich an Ihren LDAP-Administrator, um die Anforderungen Ihrer Umgebung zu besprechen.

- Die Verwendung von LDAP für die Auflösung des Host-Namens wird nicht unterstützt.

Finden Sie weitere Informationen

- "Technischer Bericht von NetApp 4835: Konfigurieren von LDAP in ONTAP"
- "Installieren Sie das selbstsignierte Root-CA-Zertifikat auf der SVM"

Erstellen Sie ein neues LDAP-Client-Schema

Wenn sich das LDAP-Schema in Ihrer Umgebung von den ONTAP-Standardwerten unterscheidet, müssen Sie ein neues LDAP-Client-Schema für ONTAP erstellen, bevor Sie die LDAP-Client-Konfiguration erstellen.

Über diese Aufgabe

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

- MS-AD-bis (das bevorzugte Schema für die meisten Windows 2012- und späteren AD-Server)
- AD-IDMU (AD-Server Windows 2008, Windows 2012 und höher)
- AD-SFU (Windows 2003 und frühere AD-Server)
- RFC-2307 (UNIX LDAP-SERVER)

Wenn Sie ein nicht standardmäßiges LDAP-Schema verwenden müssen, müssen Sie es erstellen, bevor Sie die LDAP-Client-Konfiguration erstellen. Wenden Sie sich an Ihren LDAP-Administrator, bevor Sie ein neues Schema erstellen.

Die von ONTAP bereitgestellten Standard-LDAP-Schemata können nicht geändert werden. Zum Erstellen eines neuen Schemas erstellen Sie eine Kopie und ändern dann die Kopie entsprechend.

Schritte

1. Zeigen Sie die vorhandenen LDAP-Client-Schemavorlagen an, um die zu kopierende zu identifizieren:

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

2. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

3. 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. Ändern Sie das neue Schema und passen Sie es für Ihre Umgebung an:

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

5. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Erstellen Sie eine LDAP-Client-Konfiguration

Wenn ONTAP auf die externen LDAP- oder Active Directory-Dienste in Ihrer Umgebung zugreifen soll, müssen Sie zunächst einen LDAP-Client auf dem Speichersystem einrichten.

Was Sie benötigen

Einer der ersten drei Server in der Liste Active Directory Domain Resolved muss up sein und Daten bereitstellen. Andernfalls schlägt diese Aufgabe fehl.

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

Schritte

1. Wenden Sie sich an Ihren LDAP-Administrator, um die entsprechenden Konfigurationswerte für den `vserver services name-service ldap client create` folgenden Befehl zu ermitteln:

   a. Geben Sie eine domänenbasierte oder eine address-basierte Verbindung zu LDAP-Servern an.

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

      - Verwenden Sie die `-ad-domain` Option, um die LDAP-Servererkennung in der Active Directory-Domäne zu aktivieren.
        - Sie können die `-restrict-discovery-to-site` Option verwenden, um die LDAP-Servererkennung auf den CIFS-Standardstandort für die angegebene Domäne zu beschränken. Wenn Sie diese Option verwenden, müssen Sie auch die CIFS-Standardsite mit angeben `-default-site`.
      - Sie können die `-preferred-ad-servers` Option verwenden, um einen oder mehrere bevorzugte Active Directory-Server nach IP-Adresse in einer kommagetrennten Liste anzugeben. Nachdem der Client erstellt wurde, können Sie diese Liste mit dem `vserver services name-service ldap client modify` Befehl ändern.
      - Verwenden Sie die `-servers` Option, um einen oder mehrere LDAP-Server (Active Directory oder UNIX) nach IP-Adresse in einer kommagetrennten Liste anzugeben.

> Die `-servers` Option ist in ONTAP 9.2 veraltet. Ab ONTAP 9.2 wird `-ldap -servers` das `-servers` Feld durch das Feld ersetzt. Dieses Feld kann entweder einen Hostnamen oder eine IP-Adresse für den LDAP-Server annehmen.

b. Geben Sie ein Standard- oder ein benutzerdefiniertes LDAP-Schema an.

   Die meisten LDAP-Server können die von ONTAP bereitgestellten Standardschemata für schreibgeschützte Lesevorgänge verwenden. Es empfiehlt sich, diese Standardschemata zu verwenden, es sei denn, es ist eine andere Voraussetzung zu tun. In diesem Fall können Sie Ihr eigenes Schema erstellen, indem Sie ein Standardschema kopieren (es handelt sich um schreibgeschützt) und dann die Kopie ändern.

   Standardschemas:

   - MS-AD-BIS

     Basierend auf RFC-2307bis ist dies das bevorzugte LDAP-Schema für die meisten Standard-LDAP-Bereitstellungen unter Windows 2012 und höher.

   - `AD-IDMU`

     Basierend auf Active Directory Identity Management für UNIX ist dieses Schema für die meisten Windows 2008-, Windows 2012- und späteren AD-Server geeignet.

   - `AD-SFU`

     Dieses Schema basiert auf Active Directory Services für UNIX und ist für die meisten Windows 2003- und früheren AD-Server geeignet.

   - `RFC-2307`

     Dieses Schema basiert auf RFC-2307 (*an Approach for Using LDAP as a Network Information Service*) und ist für die meisten UNIX AD-Server geeignet.

c. Wählen Sie Bindungswerte.

   - `-min-bind-level {anonymous|simple|sasl}` Gibt die minimale binde-Authentifizierungsstufe an.

     Der Standardwert ist **`anonymous`**.

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

     Für Active Directory-Server müssen Sie den Benutzer im Konto- (DOMAIN\user) oder Principal (user@domain.com)-Formular angeben. Andernfalls müssen Sie den Benutzer in einem Formular mit distinguished Name (CN=user,DC=Domain,DC=com) angeben.

   - `-bind-password` *`password`* Gibt das Bindungskennwort an.

d. Wählen Sie bei Bedarf die Sicherheitsoptionen für die Sitzung aus.

   Sie können LDAP-Signing und -Sealing oder LDAP über TLS aktivieren, falls vom LDAP-Server erforderlich.

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

Sie können Signing (`sign`, Datenintegrität), Signing und Sealing (`seal`, Datenintegrität und Verschlüsselung), oder keine `none`, keine Signatur oder Versiegelung). Der Standardwert ist `none`.

Sie sollten auch `-min-bind-level` {`sasl`} einstellen, es sei denn, Sie möchten, dass die binde-Authentifizierung zurückfällt **`anonymous`** oder **`simple`** wenn die Signing and Sealing Bind fehlschlägt.

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

  Wenn auf festgelegt **`true`** und der LDAP-Server ihn unterstützt, verwendet der LDAP-Client eine verschlüsselte TLS-Verbindung zum Server. Der Standardwert ist **`false`**. Sie müssen ein selbstsigniertes Root-CA-Zertifikat des LDAP-Servers installieren, um diese Option verwenden zu können.

> Wenn der Speicher-VM einen SMB-Server zu einer Domäne hinzugefügt hat und der LDAP-Server einer der Domänen-Controller der Home-Domain des SMB-Servers ist, können Sie die `-session-security-for-ad-ldap` Option mit dem `vserver cifs security modify` Befehl ändern.

e. Wählen Sie Port-, Abfrage- und Basiswerte aus.

Die Standardwerte werden empfohlen, aber Sie müssen mit Ihrem LDAP-Administrator überprüfen, dass sie für Ihre Umgebung geeignet sind.

- `-port` *`port`* Gibt den LDAP-Serverport an.

  Der Standardwert ist `389`.

Wenn Sie die LDAP-Verbindung mit Start TLS sichern möchten, müssen Sie den Standardport 389 verwenden. Start TLS beginnt als Klartext-Verbindung über den LDAP-Standardport 389 und wird dann auf TLS aktualisiert. Wenn Sie den Port ändern, schlägt Start TLS fehl.

- `-query-timeout` *`integer`* Gibt das Abfragezeitlimit in Sekunden an.

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

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

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

- `-base-scope` {`base`|`onelevel`|`subtree`} Gibt den Suchbereich der Basis an.

  Der Standardwert ist `subtree`.

- `-referral-enabled` {`true`|`false`} Gibt an, ob LDAP-Empfehlungsverfolgung aktiviert ist.

  Ab ONTAP 9.5 kann der LDAP-Client von ONTAP Anfragen auf andere LDAP-Server verweisen, wenn vom primären LDAP-Server eine LDAP-Empfehlungsantwort zurückgegeben wird, die angibt, dass die gewünschten Datensätze auf den empfohlenen LDAP-Servern vorhanden sind. Der Standardwert ist **`false`**.

Um nach Datensätzen zu suchen, die in den genannten LDAP-Servern vorhanden sind, muss der Basis-dn

der genannten Datensätze im Rahmen der LDAP-Client-Konfiguration dem Basis-dn hinzugefügt werden.

2. Erstellen Sie eine LDAP-Client-Konfiguration auf der Storage-VM:

```
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 müssen Sie den Namen der Storage-VM angeben.

3. Überprüfen Sie, ob die LDAP-Client-Konfiguration erfolgreich erstellt wurde:

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

Beispiele

Mit dem folgenden Befehl wird eine neue LDAP-Client-Konfiguration namens ldap1 für die Speicher-VM vs1 erstellt, die mit einem Active Directory-Server für LDAP arbeitet:

```
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
```

Mit dem folgenden Befehl wird eine neue LDAP-Client-Konfiguration namens ldap1 für die Speicher-VM vs1 erstellt, die mit einem Active Directory-Server für LDAP funktioniert, auf dem Signieren und Versiegeln erforderlich ist, und die LDAP-Servererkennung ist auf einen bestimmten Standort für die angegebene Domäne beschränkt:

```
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
```

Mit dem folgenden Befehl wird eine neue LDAP-Client-Konfiguration namens ldap1 für die Speicher-VM vs1 erstellt, um mit einem Active Directory-Server für LDAP zu arbeiten, für den LDAP-Empfehlungsverfahren erforderlich sind:

```
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
```

Mit dem folgenden Befehl wird die LDAP-Client-Konfiguration namens ldap1 für die Speicher-VM vs1 durch Angabe des Basis-DN geändert:

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

Mit dem folgenden Befehl wird die LDAP-Client-Konfiguration namens ldap1 für die Speicher-VM vs1 geändert, indem die Referenzsuche 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
```

Zuordnen der LDAP-Client-Konfiguration zu SVMs

Um LDAP auf einer SVM `vserver services name-service ldap create` zu aktivieren, müssen Sie mit dem Befehl eine LDAP-Client-Konfiguration mit der SVM verknüpfen.

Was Sie benötigen

- Eine LDAP-Domäne muss bereits im Netzwerk vorhanden sein und für den Cluster, auf dem sich die SVM befindet, zugänglich sein.
- 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`*

   > Ab ONTAP 9.2 `vserver services name-service ldap create` führt der Befehl eine automatische Konfigurationsprüfung durch und meldet eine Fehlermeldung, wenn ONTAP den Name Server nicht kontaktieren kann.

   Mit dem folgenden Befehl wird LDAP auf der SVM „vs1“ aktiviert und so konfiguriert, dass sie die LDAP-Client-Konfiguration „ldap1“ verwendet:

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

2. Überprüfen Sie den Status der Namensserver mithilfe des LDAP-Prüfbefehls vserver Services Name-Service.

   Mit dem folgenden Befehl werden die LDAP-Server auf der SVM vs1 validiert.

```
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".                                              |
```

   Der Befehl Name Service Check ist ab ONTAP 9.2 verfügbar.

Überprüfen Sie die LDAP-Quellen in der Tabelle Namensdienst-Switch

In der Namensservice-Switch-Tabelle für die SVM müssen Sie überprüfen, ob LDAP-Quellen für Namensdienste korrekt aufgeführt sind.

Schritte

1. Zeigt den aktuellen Inhalt der Tabelle des Namensdienstschalters an:

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

   Mit dem folgenden Befehl werden die Ergebnisse für die SVM My_SVM angezeigt:

```
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, die nach Informationen zur Namenszuordnung und in welcher Reihenfolge gesucht werden sollen. In einer UNIX-Umgebung ist dieser Eintrag nicht erforderlich. Name Mapping ist nur in einer gemischten Umgebung mit UNIX und Windows erforderlich.

2. Aktualisieren Sie den `ns-switch` Eintrag entsprechend:

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`
Informationen zur Netzwerkgruppe	`vserver services name-service ns-switch modify -vserver` *`vserver_name`* `-database netgroup -sources ldap,files`

Hohe Sicherheit durch Kerberos mit NFS

Übersicht über die Verwendung von Kerberos mit NFS für hohe Sicherheit

Wenn Kerberos in Ihrer Umgebung für eine starke Authentifizierung verwendet wird, müssen Sie mit Ihrem Kerberos-Administrator zusammenarbeiten, um die Anforderungen und die entsprechenden Speichersystemkonfigurationen zu ermitteln und die SVM als Kerberos-Client zu aktivieren.

Ihre Umgebung sollte die folgenden Richtlinien erfüllen:

- Die Bereitstellung Ihres Standorts sollte die Best Practices für Kerberos-Server und die Client-Konfiguration befolgen, bevor Sie Kerberos für ONTAP konfigurieren.
- Falls möglich, verwenden Sie NFSv4 oder höher, wenn Kerberos-Authentifizierung erforderlich ist.

  NFSv3 kann mit Kerberos verwendet werden. Die vollständigen Sicherheitsvorteile von Kerberos werden jedoch nur in ONTAP-Bereitstellungen von NFSv4 oder höher realisiert.

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

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

- Verzeichnisdienst

Sie sollten einen sicheren Verzeichnisdienst in Ihrer Umgebung verwenden, z. B. Active Directory oder OpenLDAP, der für die Verwendung von LDAP über SSL/TLS konfiguriert ist. Verwenden Sie NIS nicht, deren Anfragen in Klartext gesendet werden und daher nicht sicher sind.

- NTP

  Sie müssen über einen Arbeitszeitserver verfügen, auf dem NTP ausgeführt wird. Dies ist notwendig, um ein Versagen der Kerberos-Authentifizierung aufgrund von Zeitverzerrung zu verhindern.

- DNS (Domain Name Resolution)

  Jeder UNIX-Client und jede SVM-LIF müssen über einen entsprechenden Service-Datensatz (SRV) verfügen, der beim KDC unter „Forward and Reverse Lookup Zones“ registriert ist. Alle Teilnehmer müssen über DNS richtig lösbar sein.

Überprüfen Sie die Berechtigungen für die Kerberos-Konfiguration

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

Schritte

1. Zeigen Sie die entsprechenden Berechtigungen für das SVM-Root-Volume an:

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

   Das Root-Volume der SVM muss über folgende Konfiguration verfügen:

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

   Werden diese Werte nicht angezeigt, `volume modify` aktualisieren Sie sie mit dem Befehl.

2. Zeigen Sie die lokalen UNIX-Benutzer an:

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

   Die SVM muss über die folgenden UNIX-Benutzer konfiguriert sein:

Benutzername	User-ID	ID der primären Gruppe	Kommentar
nfs	500	0	Erforderlich für die GSS-INIT-Phase. Die erste Komponente des SPN-Client-Benutzers des NFS wird als Benutzer verwendet. Der nfs-Benutzer ist nicht erforderlich, wenn eine Kerberos-UNIX Namenszuweisung für das SPN des NFS-Client-Benutzers besteht.
Stamm	0	0	Zur Montage erforderlich.

Werden diese Werte nicht angezeigt, können Sie `vserver services name-service unix-user modify` sie mit dem Befehl aktualisieren.

3. Zeigen Sie die lokalen UNIX-Gruppen an:

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

   Die SVM muss über die folgenden UNIX-Gruppen konfiguriert sein:

Gruppenname	Gruppen-ID
Dämon	1
Stamm	0

Werden diese Werte nicht angezeigt, können Sie `vserver services name-service unix-group modify` sie mit dem Befehl aktualisieren.

Erstellen Sie eine NFS-Kerberos-Bereichskonfiguration

Wenn ONTAP auf externe Kerberos-Server in Ihrer Umgebung zugreifen soll, müssen Sie zunächst die SVM so konfigurieren, dass sie einen vorhandenen Kerberos-Bereich verwendet. Dazu müssen Sie Konfigurationswerte für den Kerberos-KDC-Server erfassen und dann mit dem `vserver nfs kerberos realm create` Befehl die Kerberos-Bereichskonfiguration auf einer SVM erstellen.

Was Sie benötigen

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

Schritte

1. Wenden Sie sich an Ihren Kerberos-Administrator, um die geeigneten Konfigurationswerte `vserver nfs kerberos realm create` für den Befehl zu ermitteln.
2. Erstellen einer Kerberos-Bereichskonfiguration 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. Vergewissern Sie sich, dass die Kerberos-Bereichskonfiguration erfolgreich erstellt wurde:

   `vserver nfs kerberos realm show`

Beispiele

Mit dem folgenden Befehl wird eine NFS-Kerberos-Bereichskonfiguration für die SVM vs1 erstellt, die einen Microsoft Active Directory-Server als KDC-Server verwendet. Der Kerberos-Bereich ist AUTH.EXAMPLE.COM. Der Active Directory-Server hat den Namen ad-1 und seine IP-Adresse lautet 10.10.8.14. Die zulässige Taktschiefe beträgt 300 Sekunden (Standardeinstellung). Die IP-Adresse des KDC-Servers ist 10.10.8.14 und seine Portnummer ist 88 (Standard). „Microsoft Kerberos config“ ist der Kommentar.

```
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"
```

Mit dem folgenden Befehl wird eine NFS Kerberos-Bereichskonfiguration für die SVM vs1 erstellt, die einen mit KDC verwendet. Der Kerberos-Bereich ist SECURITY.EXAMPLE.COM. Die zulässige Taktschiefe beträgt 300 Sekunden. Die IP-Adresse des KDC-Servers ist 10.10.9.1 und seine Portnummer ist 88. Der KDC-Anbieter weist auf einen UNIX-Anbieter hin. Die IP-Adresse des Verwaltungsservers ist 10.10.9.1, und seine Portnummer ist 749 (die Standardeinstellung). Die IP-Adresse des Kennwortservers lautet 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"
```

Konfigurieren von NFS-Kerberos-zulässigen Verschlüsselungstypen

Standardmäßig unterstützt ONTAP die folgenden Verschlüsselungstypen für NFS Kerberos: DES, 3DES, AES-128 und AES-256. Sie können die zulässigen Verschlüsselungstypen für jede SVM mithilfe des `vserver nfs modify` Befehls mit dem `-permitted-enc-types` Parameter so konfigurieren, dass sie den Sicherheitsanforderungen Ihrer jeweiligen Umgebung entsprechen.

Über diese Aufgabe

Für eine maximale Client-Kompatibilität unterstützt ONTAP standardmäßig sowohl schwache DES als auch eine starke AES-Verschlüsselung. Wenn Sie beispielsweise die Sicherheit erhöhen und die Umgebung unterstützt, können Sie mit diesem Verfahren DAS und 3DES deaktivieren und benötigen von Clients nur die AES-Verschlüsselung.

Sie sollten die stärkste verfügbare Verschlüsselung verwenden. Für ONTAP, also AES-256. Sie sollten mit Ihrem KDC-Administrator bestätigen, dass diese Verschlüsselungsstufe in Ihrer Umgebung unterstützt wird.

- Die vollständige Aktivierung oder Deaktivierung von AES (AES-128 und AES-256) auf SVMs führt zu Unterbrechungen, da dies die ursprüngliche DES-Principal/Keytab-Datei zerstört. Dadurch muss die Kerberos-Konfiguration auf allen LIFs für die SVM deaktiviert werden.

  Bevor Sie diese Änderung vornehmen, sollten Sie überprüfen, ob NFS-Clients auf der AES-Verschlüsselung auf der SVM basieren.

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

Schritt

1. Aktivieren oder deaktivieren Sie den gewünschten Verschlüsselungstyp:

Wenn Sie aktivieren oder deaktivieren möchten…	Führen Sie die folgenden Schritte aus…
DES oder 3DES	a. Konfigurieren Sie die zulässigen NFS-Kerberos-Verschlüsselungstypen der SVM: `vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`* Trennen Sie mehrere Verschlüsselungstypen durch ein Komma. b. Überprüfen Sie, ob die Änderung erfolgreich war: `vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`

Wenn Sie aktivieren oder deaktivieren möchten…	Führen Sie die folgenden Schritte aus…

AES-128 oder AES-256	a. Ermitteln, auf welcher SVM und welcher LIF Kerberos aktiviert ist:
	`vserver nfs kerberos interface show`
	b. Deaktivieren Sie Kerberos auf allen LIFs auf der SVM, deren NFS Kerberos den Verschlüsselungstyp zulässt, den Sie ändern möchten:
	`vserver nfs kerberos interface disable -lif lif_name`
	c. Konfigurieren Sie die zulässigen NFS-Kerberos-Verschlüsselungstypen der SVM:
	`vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types`
	
	Trennen Sie mehrere Verschlüsselungstypen durch ein Komma.
	d. Überprüfen Sie, ob die Änderung erfolgreich war:
	`vserver nfs show -vserver vserver_name -fields permitted-enc-types`
	e. Aktivieren Sie Kerberos auf allen LIFs auf der SVM:
	`vserver nfs kerberos interface enable -lif lif_name -spn service_principal_name`
	f. Überprüfen Sie, ob Kerberos auf allen LIFs aktiviert ist:
	`vserver nfs kerberos interface show`

Aktivieren Sie Kerberos auf einer Daten-LIF

Sie können den `vserver nfs kerberos interface enable` Befehl verwenden, um Kerberos auf einer Daten-LIF zu aktivieren. Dies ermöglicht der SVM, Kerberos-Sicherheitsdienste für NFS zu nutzen.

Über diese Aufgabe

Wenn Sie ein Active Directory KDC verwenden, müssen die ersten 15 Zeichen einer verwendeten SPNs über SVMs innerhalb eines Bereichs oder einer Domäne eindeutig sein.

Schritte

1. Erstellen Sie die NFS-Kerberos-Konfiguration:

```
vserver nfs kerberos interface enable -vserver vserver_name -lif
```

logical_interface -spn *service_principal_name*

ONTAP erfordert den geheimen Schlüssel für das SPN vom KDC, um die Kerberos-Schnittstelle zu aktivieren.

Für Microsoft KDCs wird das KDC kontaktiert und ein Benutzername und eine Passwort-Eingabeaufforderung werden an der CLI ausgegeben, um den geheimen Schlüssel zu erhalten. Wenn Sie die SPN in einer anderen Organisationseinheit des Kerberos-Bereichs erstellen müssen, können Sie den optionalen `-ou` Parameter angeben.

Für nicht-Microsoft-KDCs kann der geheime Schlüssel mit einer von zwei Methoden abgerufen werden:

Sie suchen…	**Sie müssen auch den folgenden Parameter mit dem Befehl angeben…**
Die KDC-Administratoranmeldeinformationen haben, um den Schlüssel direkt aus dem KDC abzurufen	`-admin-username` *kdc_admin_username*
Sie haben keine KDC-Administratoranmeldedaten, haben aber eine Keytab-Datei aus dem KDC, die den Schlüssel enthält	`-keytab-uri` {ftp}://*uri*

2. Vergewissern Sie sich, dass Kerberos auf der LIF aktiviert war:

   ```
   vserver nfs kerberos-config show
   ```

3. Wiederholen Sie die Schritte 1 und 2, um Kerberos auf mehreren LIFs zu aktivieren.

Beispiel

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

```
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.
```

Hohe Sicherheit durch Verwendung von TLS mit NFS

Übersicht über die Verwendung von TLS mit NFS für hohe Sicherheit

TLS ermöglicht verschlüsselte Netzwerkkommunikation mit gleichwertiger Sicherheit und geringerer Komplexität als Kerberos und IPsec. Als Administrator können Sie TLS für eine hohe Sicherheit bei NFSv3- und NFSv4.x-Verbindungen mit System Manager, der ONTAP-CLI oder der ONTAP-REST-API aktivieren, konfigurieren und deaktivieren.

> NFS über TLS ist in ONTAP 9.15.1 als öffentliche Vorschau verfügbar. NFS über TLS wird in ONTAP 9.15.1 als Vorschauangebot für Produktions-Workloads nicht unterstützt.

ONTAP verwendet TLS 1.3 für NFS- über TLS-Verbindungen.

Anforderungen

NFS über TLS erfordert X.509-Zertifikate. Sie können entweder ein CA-signiertes Serverzertifikat auf dem ONTAP-Cluster installieren oder ein Zertifikat installieren, das der NFS-Service direkt verwendet. Ihre Zertifikate sollten die folgenden Richtlinien erfüllen:

- Jedes Zertifikat muss mit dem Fully Qualified Domain Name (FQDN) des NFS-Servers (der Daten-LIF, auf der TLS aktiviert/konfiguriert wird) als Common Name (CN) konfiguriert werden.
- Jedes Zertifikat muss mit der IP-Adresse oder dem FQDN des NFS-Servers (oder beides) als alternativer Antragstellername (SAN) konfiguriert sein. Wenn sowohl IP-Adresse als auch FQDN konfiguriert sind, können NFS-Clients eine Verbindung entweder über die IP-Adresse oder den FQDN herstellen.
- Sie können mehrere NFS-Servicezertifikate für dieselbe LIF installieren, aber nur eines davon kann gleichzeitig als Teil der NFS-TLS-Konfiguration verwendet werden.

Aktivieren oder deaktivieren Sie TLS für NFS-Clients

Sie können TLS auf einer Daten-LIF für NFS-Clients aktivieren oder deaktivieren. Wenn Sie NFS über TLS aktivieren, verwendet die SVM TLS zur Verschlüsselung aller Daten, die zwischen dem NFS-Client und ONTAP über das Netzwerk gesendet werden. Dies erhöht die Sicherheit von NFS-Verbindungen.

> NFS über TLS ist in ONTAP 9.15.1 als öffentliche Vorschau verfügbar. NFS über TLS wird in ONTAP 9.15.1 als Vorschauangebot für Produktions-Workloads nicht unterstützt.

Aktivieren Sie TLS

Sie können die TLS-Verschlüsselung für NFS-Clients aktivieren, um die Sicherheit von Daten bei der Übertragung zu erhöhen.

Bevor Sie beginnen

- Beziehen Sie sich "Anforderungen"vor dem Starten auf die für NFS über TLS.
- "Manuelle Seite"Weitere Informationen zum `vserver nfs tls interface enable` Befehl finden Sie in der.

Schritte

1. Wählen Sie eine Storage-VM und eine logische Schnittstelle (LIF) zur Aktivierung von TLS aus.
2. Aktivieren Sie TLS für NFS-Verbindungen auf dieser Storage-VM und Schnittstelle. Ersetzen Sie Werte in Klammern <> durch Informationen aus Ihrer Umgebung:

```
vserver nfs tls interface enable -vserver <STORAGE_VM> -lif <LIF_NAME>
-certificate-name <CERTIFICATE_NAME>
```

3. Verwenden Sie den `vserver nfs tls interface show` Befehl, um die Ergebnisse anzuzeigen:

```
vserver nfs tls interface show
```

Beispiel

Mit dem folgenden Befehl wird NFS über TLS auf der `data1` LIF der `vs1` Storage-VM aktiviert:

```
vserver nfs tls interface enable -vserver vs1 -lif data1 -certificate-name
cert_vs1
```

```
vserver nfs tls interface show
```

```
                Logical
Vserver         Interface     Address         TLS Status TLS Certificate
Name
--------------- ------------- --------------- ----------
-----------------------
vs1             data1         10.0.1.1        enabled    cert_vs1
vs2             data2         10.0.1.2        disabled   -
2 entries were displayed.
```

TLS deaktivieren

Sie können TLS für NFS-Clients deaktivieren, wenn Sie die erhöhte Sicherheit für die während der Übertragung verwendeten Daten nicht mehr benötigen.

> Wenn Sie NFS über TLS deaktivieren, wird das für die NFS-Verbindung verwendete TLS-Zertifikat entfernt. Wenn Sie in Zukunft NFS über TLS aktivieren müssen, müssen Sie während der Aktivierung erneut einen Zertifikatnamen angeben.

Bevor Sie beginnen

```
https://docs.netapp.com/us-en/ontap-cli/vserver-nfs-tls-interface-
disable.html["Manuelle Seite"^]Weitere Informationen zum `vserver nfs tls
interface disable` Befehl finden Sie in der.
```

Schritte

1. Wählen Sie eine Storage-VM und eine logische Schnittstelle (LIF) zum Deaktivieren von TLS aus.
2. Deaktivieren Sie TLS für NFS-Verbindungen auf dieser Storage-VM und Schnittstelle. Ersetzen Sie Werte in Klammern <> durch Informationen aus Ihrer Umgebung:

   ```
   vserver nfs tls interface disable -vserver <STORAGE_VM> -lif <LIF_NAME>
   ```

3. Verwenden Sie den `vserver nfs tls interface show` Befehl, um die Ergebnisse anzuzeigen:

   ```
   vserver nfs tls interface show
   ```

Beispiel

Mit dem folgenden Befehl wird NFS über TLS auf der `data1` logischen Schnittstelle der `vs1` Storage-VM deaktiviert:

```
vserver nfs tls interface disable -vserver vs1 -lif data1
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address         TLS Status TLS Certificate
Name
-------------- ------------- --------------- ----------
-----------------------
vs1            data1         10.0.1.1        disabled   -
vs2            data2         10.0.1.2        disabled   -
2 entries were displayed.
```

Bearbeiten einer TLS-Konfiguration

Sie können die Einstellungen einer vorhandenen NFS-over-TLS-Konfiguration ändern. Mit diesem Verfahren können Sie beispielsweise das TLS-Zertifikat aktualisieren.

Bevor Sie beginnen

```
https://docs.netapp.com/us-en/ontap-cli/vserver-nfs-tls-interface-
modify.html["Manuelle Seite"^]Weitere Informationen zum `vserver nfs tls
interface modify` Befehl finden Sie in der.
```

Schritte

1. Wählen Sie eine Storage-VM und eine logische Schnittstelle (Logical Interface, LIF) aus, auf der die TLS-Konfiguration für NFS-Clients geändert werden soll.
2. Ändern Sie die Konfiguration. Wenn Sie einen `status` von angeben `enable`, müssen Sie auch den `certificate-name` Parameter angeben. Ersetzen Sie Werte in Klammern <> durch Informationen aus Ihrer Umgebung:

   ```
   vserver nfs tls interface modify -vserver <STORAGE_VM> -lif <LIF_NAME>
   -status <STATUS> -certificate-name <CERTIFICATE_NAME>
   ```

3. Verwenden Sie den `vserver nfs tls interface show` Befehl, um die Ergebnisse anzuzeigen:

   ```
   vserver nfs tls interface show
   ```

Beispiel

Mit dem folgenden Befehl wird die Konfiguration von NFS über TLS auf der `data2` logischen Schnittstelle der `vs2` Storage-VM geändert:

```
vserver nfs tls interface modify -vserver vs2 -lif data2 -status enable
-certificate-name new_cert
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address         TLS Status TLS Certificate
Name
-------------- ------------- --------------- ----------
------------------------
vs1            data1         10.0.1.1        disabled   -
vs2            data2         10.0.1.2        enabled    new_cert
2 entries were displayed.
```