



Konfigurieren Sie den NFS-Zugriff auf eine SVM

ONTAP 9

NetApp
March 30, 2023

Inhaltsverzeichnis

- Konfigurieren Sie den NFS-Zugriff auf eine SVM..... 1
 - Erstellen einer 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 eines LIF 6
 - Aktivieren Sie DNS für die Auflösung des Host-Namens 10
 - Konfigurieren Sie Name Services 12
 - Hohe Sicherheit durch Kerberos mit NFS 30

Konfigurieren Sie den NFS-Zugriff auf eine SVM

Erstellen einer SVM

Wenn nicht bereits mindestens eine SVM in einem Cluster vorhanden ist, um den Datenzugriff für NFS-Clients zu ermöglichen, müssen Sie eine SVM erstellen.

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 den `-rootvolume-security-style` Option.
- Verwenden Sie die Standard-`C.UTF-8` `-language` Option.
- Der `ipspace` Die Einstellung ist optional.

2. Konfiguration und Status der neu erstellten SVM überprüfen:

```
vserver show -vserver vserver_name
```

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

Der `Vserver Operational State` Das Feld muss angezeigt werden `running` Bundesland. Wenn der angezeigt wird `initializing` Zustand: Einiger Zwischenvorgang wie z. B. die Erstellung des Root-Volumes ist fehlgeschlagen. Außerdem müssen Sie die SVM löschen und erneut 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
```

Der folgende Befehl zeigt, dass eine SVM mit einem Root-Volume von 1 GB erstellt wurde und dass sie automatisch gestartet wurde und sich in befindet `running` Bundesland. 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

```

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

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

Über diese Aufgabe

Dies erfolgt normalerweise während der Einrichtung der SVM. Wenn Sie das Protokoll jedoch während des Setups nicht aktiviert haben, können Sie es zu einem späteren Zeitpunkt mit der aktivieren `vserver add-protocols` Befehl.



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

Außerdem können Sie mithilfe von die Protokolle auf SVMs deaktivieren `vserver remove-protocols` Befehl.

Schritte

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

```
vserver show -vserver vserver_name -protocols
```

Sie können auch die verwenden `vserver show-protocols` Befehl zum Anzeigen der derzeit aktivierten Protokolle auf allen SVMs im Cluster

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
```

Der folgende Befehl ermöglicht den Zugriff über NFS durch Hinzufügen `nfs` Unter der Liste der aktivierten Protokolle der SVM namens `vs1`:

```
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 über NFS einen offenen Zugriff zu ermöglichen. Ohne diese Regel erhält jeder NFS-Clients 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 Volumes enthält, die von Kerberos gesichert wurden, können Sie die Optionen für die Exportregel festlegen `-rorule`, `-rwrule`, und `-superuser` Für das Root-Volume zu `krb5` Oder `krb5i`.
Beispiel:

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

3. Überprüfen Sie die Regelerstellung mithilfe des `vserver export-policy rule show` Befehl.

Ergebnis

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

Erstellen Sie einen NFS-Server

Nachdem sichergestellt wurde, dass NFS für den Cluster lizenziert ist, können Sie den `vserver nfs create` Befehl zum Erstellen eines NFS-Servers auf der SVM und zur Angabe der unterstützten NFS-Versionen.

Was Sie benötigen

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

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.

Schritte

1. Vergewissern Sie sich, dass NFS auf Ihrem 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. Falls Sie pNFS unterstützen möchten, müssen Sie beide aktivieren `-v4.1` und `-v4.1-pnfs` Optionen:

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 später mithilfe von zusätzliche NFS-Funktionen aktivieren `vserver nfs modify` Befehl.

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 eines 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 kommuniziert wird.

Was Sie benötigen

- Der zugrunde liegende physische oder logische Netzwerk-Port muss für den Administrator konfiguriert worden sein `up` Status:
- 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 eine große Anzahl von LIFs im Cluster besitzen, können Sie die im Cluster unterstützte LIF-Kapazität mithilfe der überprüfen `network interface capacity show` Befehl und die LIF-Kapazität, die auf jedem Node mithilfe von unterstützt wird `network interface capacity details show` Befehl (auf der erweiterten Berechtigungsebene).
- 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 | <code>`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</code> |
| <code>-subnet-name subnet_name} -firewall-policy data -auto-revert {true</code> | <code>false}`</code> |
| ONTAP 9.6 und höher | <code>`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</code> |
| <code>-subnet-name subnet_name} -firewall-policy data -auto-revert {true</code> | <code>false}`</code> |

- Der `-role` Parameter ist beim Erstellen einer LIF mithilfe einer Service-Richtlinie nicht erforderlich (beginnend mit ONTAP 9.6).
- Der `-data-protocol` Parameter muss angegeben werden, wenn die LIF erstellt wird, und kann später nicht geändert werden, ohne die Daten-LIF zu zerstören und neu zu erstellen.

Der `-data-protocol` Parameter ist beim Erstellen einer LIF mithilfe einer Service-Richtlinie nicht erforderlich (beginnend mit ONTAP 9.6).

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

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

- `-home-port` Ist der physische oder logische Port, an den das LIF zurückgibt, wenn das `network interface revert` Befehl wird auf dem LIF ausgeführt.
- Sie können eine IP-Adresse mit dem angeben `-address` Und `-netmask` Optionen, oder Sie aktivieren die Zuweisung von einem Subnetz mit dem `-subnet_name` Option.
- 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. Der `network route create` Die man-Page enthält Informationen zum Erstellen einer statischen Route in einer SVM.
- Für das `-firewall-policy` Wählen Sie die gleiche Standardeinstellung aus `data` 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-Service-Richtlinien ersetzt. Weitere Informationen finden Sie unter ["Konfigurieren Sie Firewallrichtlinien für LIFs"](#).

- `-auto-revert` Ermöglicht Ihnen, anzugeben, ob eine Daten-LIF automatisch auf den Home-Node zurückgesetzt wird. Dies kann unter Umständen wie „Startvorgang“, ändert den Status der Management-Datenbank oder wenn die Netzwerkverbindung hergestellt wird. Die Standardeinstellung ist `false`, Aber Sie können es auf `true` einstellen. Abhängig von Netzwerkmanagement-Richtlinien in Ihrer Umgebung.

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

| Überprüfen einer... | Verwenden... |
|---------------------|----------------------------|
| IPv4-Adresse | <code>network ping</code> |
| IPv6-Adresse | <code>network ping6</code> |

- 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

Der folgende Befehl erstellt eine LIF und gibt die IP-Adresse und Netzwerkmaskenwerte mit dem `-address` und `-netmask` Parameter:

```
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 `Daten1` und `Daten2` werden mit IPv4-Adressen konfiguriert und `Daten3` wird mit einer IPv6-Adresse konfiguriert:

```
network interface show
```

| Vserver | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Port | Is |
|-----------------|-------------------|-------------------|----------------------|--------------|--------------|-------|
| 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.

Mit dem folgenden Befehl wird gezeigt, wie ein LIF mit NAS-Daten erstellt wird, das dem zugewiesen ist default-data-files Service-Richtlinie:

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

Aktivieren Sie DNS für die Auflösung des Host-Namens

Sie können das verwenden `vserver services name-service dns` Befehl zum Aktivieren von DNS für eine SVM und Konfigurieren des Befehls für die Auflösung des

Host-Namens für DNS. 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. Der `vserver services name-service dns create` Befehl gibt eine Warnung aus, wenn Sie nur einen DNS-Servernamen eingeben.

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 beginnt der `vserver services name-service dns create` Befehl führt eine automatische Konfigurationsvalidierung durch und meldet eine Fehlermeldung, wenn ONTAP den Namensserver nicht kontaktieren kann.

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

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

```
vserver services name-service dns show
```

| Vserver | State | Domains | Name 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 mithilfe von `vserver services name-service dns check` Befehl.

Der `vserver services name-service dns check` Der 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 beispielsweise NIS in Ihrer Umgebung nicht verwendet wird, geben Sie nicht die an `-sources nis` Option.

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 verwenden `vserver services name-service ns-switch modify` Oder `vserver services name-service ns-switch delete` Befehle.

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

Sie können das verwenden `vserver services name-service unix-user create` Befehl zum Erstellen lokaler UNIX-Benutzer. 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

Alternativ zur manuellen Erstellung einzelner lokaler UNIX-Benutzer in SVMs können Sie die Aufgabe vereinfachen, indem Sie eine Liste lokaler UNIX-Benutzer von einer einheitlichen Ressourcen-ID (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 in UNIX enthalten `/etc/passwd` Format:

```
user_name: password: user_ID: group_ID: full_name
```


Der Befehl entwirft den Wert des *password* Feld 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. Die Standardeinstellung lautet `false`.

Beispiel

Mit dem folgenden Befehl werden eine Liste der lokalen UNIX-Benutzer aus dem URI geladen `ftp://ftp.example.com/passwd` Unter dem Namen `vs1` beschrieben. 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

Sie können das verwenden `vserver services name-service unix-group create` Befehl zum Erstellen von lokalen UNIX Gruppen für die SVM. 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

Sie können das verwenden `vserver services name-service unix-group adduser` Befehl zum Hinzufügen eines Benutzers zu einer zusätzlichen UNIX-Gruppe, die sich lokal 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

Als Alternative zum manuellen Erstellen einzelner lokaler UNIX-Gruppen können Sie mithilfe von die eine Liste lokaler UNIX-Gruppen in SVMs von einer einheitlichen Resource Identifier (URI) laden `vserver services name-service unix-group load-from-uri` Befehl.

Schritte

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

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

```
group_name: password: group_ID: comma_separated_list_of_users
```

Der Befehl entwirft den Wert des `password` Feld.

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. Falls in der SVM bereits Einträge vorhanden sind, müssen Sie entweder den `-overwrite` Parameter an `true` Um alle vorhandenen Einträge mit der neuen Datei zu überschreiben oder sicherzustellen, 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. Die Standardeinstellung lautet `false`. Wenn Sie diesen Parameter als `true` angeben, ONTAP ersetzt die gesamte bestehende lokale UNIX-Gruppendatenbank der angegebenen SVM durch die Einträge aus der Datei, die Sie laden.

Beispiel

Mit dem folgenden Befehl wird eine Liste der lokalen UNIX-Gruppen aus dem URI geladen

`ftp://ftp.example.com/group` Unter dem Namen `vs1` beschrieben. 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 über externe Nameserver (LDAP oder NIS) den Zugriff auf Netzgruppen ermöglichen oder Netgroups über eine einheitliche Resource Identifier (URI) in SVMs laden `vserver services name-service netgroup load` Befehl.

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 Netzwerkgruppen verwendeten Hostnamen zu unerwarteten Verhaltensweisen führen können, z. B. fehlgeschlagene Exportprüfungen.
- Alle IPv6-Adressen, die in Netzwerkgruppen 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 Netzwerkgruppen arbeiten, können Sie die folgenden Vorgänge ausführen:

- Sie können das verwenden `vserver export-policy netgroup check-membership` Befehl, um zu ermitteln, ob eine Client-IP Mitglied einer bestimmten Netzwerkgruppe ist.
- Sie können das verwenden `vserver services name-service getxxbyyy netgrp` Befehl, um zu überprüfen, ob ein Client Teil einer Netzwerkgruppe ist.

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

Laden Sie Netzwerkgruppen 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 `Netgroups` von einer einheitlichen Resource Identifier (URI) in SVMs laden als Alternative zur Verwendung von in externen Name Servern gespeicherten `Netgroups` (`vserver services name-service netgroup load`).

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 Netzwerkgruppendatei müssen klein geschrieben werden.
- Die maximal unterstützte Dateigröße beträgt 5 MB.
- Die maximal unterstützte Stufe für das Nesting von Netzwerkgruppen 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 Netzwerkgruppendatei 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|https|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 die Gruppensdefinitionen von der HTTP-URL in die SVM 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 Netzwerkgruppen in die SVM geladen haben, können Sie den verwenden `vserver services name-service netgroup status` Befehl zum Überprüfen des Status der netgroup-Definitionen. 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 Name-Services verwendet wird, müssen Sie eine NIS-Domänenkonfiguration für die SVM mithilfe von `vserver services name-service nis-domain create` Befehl erstellen.

Was Sie benötigen

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

Sie können mehrere NIS-Domänen erstellen. Sie können jedoch nur ein Gerät verwenden, das auf festgelegt ist `active`.

Wenn Ihre NIS-Datenbank eine enthält `netgroup.byhost` ONTAP kann das Programm für schnellere Suchvorgänge verwenden. Der `netgroup.byhost` Und `netgroup` Karten im Verzeichnis müssen stets synchron gehalten werden, um Clientzugriffsprobleme zu vermeiden. Ab ONTAP 9.7 ist NIS verfügbar `netgroup.byhost` Einträge können mit dem zwischengespeichert werden `vserver services name-service nis-domain netgroup-database` Befehle.

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 -active true -servers IP_addresses
```

Sie können bis zu 10 NIS-Server angeben.



Ab ONTAP 9.2 Field Portal `-nis-servers` Ersetzt 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 aktive NIS-Domain-Konfiguration für eine NIS-Domäne namens `nisdomain` auf der SVM mit dem Namen `vs1` erstellt und mit einem NIS-Server unter der IP-Adresse `192.0.2.180` erstellt:

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -active true -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 die LDAP-Kanalbindung mit Namenservern zu deaktivieren oder erneut zu aktivieren, verwenden Sie das `-try-channel-binding` Parameter mit `ldap client modify` Befehl.

Weitere Informationen finden Sie unter "[2020 LDAP-Channel-Bindung 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 (das `-session-security` Option)
 - Verschlüsselte TLS-Verbindungen (das `-use-start-tls` Option)
 - Kommunikation über LDAPS-Port 636 (der `-use-ldaps-for-ad-ldap` Option)

- 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 Hostnamens wird nicht unterstützt.

Weitere Informationen finden Sie unter ["Technischer Bericht von NetApp 4835: Konfigurieren von LDAP in ONTAP"](#).

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 (Windows 2008, Windows 2012 und höher AD-Server)
- 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
```

Installieren Sie das selbstsignierte Root-CA-Zertifikat auf der SVM

Wenn bei der Anbindung an LDAP-Server eine LDAP-Authentifizierung mit TLS erforderlich ist, müssen Sie zuerst das selbstsignierte Root-CA-Zertifikat auf der SVM installieren.

Über diese Aufgabe

Wenn LDAP über TLS aktiviert ist, unterstützt der ONTAP-LDAP-Client der SVM nicht wiederrief Zertifikate in ONTAP 9.0 und 9.1.

Ab ONTAP 9.2 können alle Anwendungen innerhalb von ONTAP, die TLS-Kommunikation verwenden, den digitalen Zertifikatsstatus mithilfe des Online Certificate Status Protocol (OCSP) überprüfen. Wenn OCSP für LDAP über TLS aktiviert ist, werden zurückgeworfene Zertifikate abgelehnt und die Verbindung schlägt fehl.

Schritte

1. Installieren Sie das selbstsignierte Root-CA-Zertifikat:

- a. Starten Sie die Zertifikatinstallation:

```
security certificate install -vserver vserver_name -type server-ca
```

Über die Konsolenausgabe wird die folgende Meldung angezeigt:

```
Please enter Certificate: Press <Enter> when done
```

- a. Öffnen Sie das Zertifikat `.pem` Datei mit einem Texteditor, kopieren Sie das Zertifikat, einschließlich der Zeilen beginnend mit `-----BEGIN CERTIFICATE-----` Und endet mit `-----END CERTIFICATE-----`, Und fügen Sie dann das Zertifikat nach der Eingabeaufforderung ein.
- b. Vergewissern Sie sich, dass das Zertifikat ordnungsgemäß angezeigt wird.
- c. Schließen Sie die Installation durch Drücken der Eingabetaste ab.

2. Vergewissern Sie sich, dass das Zertifikat installiert ist:

```
security certificate show -vserver vserver_name
```

Erstellen Sie eine LDAP-Client-Konfiguration

Wenn ONTAP auf die externen LDAP-Server in Ihrer Umgebung zugreifen soll, müssen Sie zuerst einen LDAP-Client auf dem Speichersystem einrichten.

Was Sie benötigen

Einer der ersten drei Server in der Liste „AD-Domäne“, die aufgelöst wurde, muss Daten verfügbar sein. Andernfalls schlägt diese Aufgabe fehl.



Es gibt mehrere Server, von denen aus mehr als zwei Server zu einem beliebigen Zeitpunkt ausfallen.

Schritte

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

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

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

- Verwenden Sie die `-ad-domain` Option zum Aktivieren der LDAP-Servererkennung in der Active Directory-Domäne.

Sie können das verwenden `-preferred-ad-servers` Option zum Festlegen eines oder mehrerer bevorzugter Active Directory-Server anhand von IP-Adressen in einer durch Komma getrennten Liste. Nachdem der Client erstellt wurde, können Sie diese Liste mithilfe der ändern `vserver services name-service ldap client modify` Befehl.

- Verwenden Sie die `-servers` Option zum Festlegen eines oder mehrerer LDAP-Server (AD oder UNIX) nach IP-Adresse in einer durch Komma getrennten Liste.



Der `-servers` Option ist veraltet in ONTAP 9.2. Ab ONTAP 9.2 beginnt der `-ldap -servers` Feld ersetzt das `-servers` Feld. Dieses neue Feld kann entweder einen Hostnamen oder eine IP-Adresse für den LDAP-Server übernehmen.

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 Mindestauthentifizierungsstufe für Bindungen an.

Der Standardwert ist **anonymous**.

- `-bind-dn LDAP_DN` Gibt den Bindebenutzer 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 Bindekennwort 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 das Signieren aktivieren (`sign`, Datenintegrität), Signing und Sealing (`seal`, Datenintegrität und Verschlüsselung) oder keines von beiden `none`, Kein Signing oder Sealing). Der Standardwert ist `none`.

Außerdem sollten Sie einstellen `-min-bind-level {sasl}` Es sei denn, Sie möchten, dass die Bindeauthentifizierung zurückfällt **anonymous** Oder **simple** Wenn das Signieren und Versiegeln fehlschlägt.

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

Wenn eingestellt auf **true** Und der LDAP-Server unterstützt ihn, der LDAP-Client verwendet 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 SVM einen SMB-Server zu einer Domäne hinzugefügt wird und der LDAP-Server einer der Domänencontroller der Home-Domain des SMB-Servers ist, können Sie den ändern `-session-security-for-ad-ldap` Mit der Option `vserver cifs security modify` Befehl.

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 die Zeitüberschreitung für die Abfrage 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 Umfang der Basissuche an.

Der Standardwert ist subtree.

- `-referral-enabled {true|false}` Gibt an, ob LDAP-Referenzsuche 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. LDAP-Client-Konfiguration auf der SVM 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 -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 SVM-Namen 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 mit dem Namen ldap1 für die SVM vs1 erstellt, die mit einem Active Directory-Server für LDAP verwendet wird:

```
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 mit dem Namen ldap1 für die SVM vs1 erstellt, die mit einem Active Directory-Server für LDAP arbeitet, auf dem das Signieren und Versiegeln 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=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 mit dem Namen ldap1 erstellt, damit die SVM vs1 mit einem Active Directory-Server für LDAP arbeitet, wobei LDAP-Weiterleitung verfolgt werden muss:

```
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 mit dem Namen ldap1 für die SVM 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 mit dem Namen ldap1 für die SVM vs1 geändert, indem Sie die Weiterleitung aktivieren:

```
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 zu aktivieren, müssen Sie den verwenden `vserver services name-service ldap create` Befehl zum Zuordnen einer LDAP-Client-Konfiguration zur SVM.

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 beginnt der `vserver services name-service ldap create` Der Befehl führt eine automatische Konfigurationsvalidierung durch und meldet eine Fehlermeldung, wenn ONTAP den Namensserver 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
```

| Vserver | Database | Source |
|---------|----------|---------------|
| ----- | ----- | ----- |
| 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 Namenszuweisung 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 die ns-switch Eintrag nach Bedarf:

| Wenn Sie den ns-Switch-Eintrag für aktualisieren möchten... | Geben Sie den Befehl ein... |
|---|--|
| Benutzerinformationen | <pre>vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files</pre> |
| Gruppeninformationen | <pre>vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files</pre> |
| Informationen zur Netzwerkgruppe | <pre>vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files</pre> |

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 mit Prüfsummen)
 - `krb5p` (Kerberos v5-Protokoll mit Datenschutzservice)

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 |

Wenn diese Werte nicht angezeigt werden, verwenden Sie den `volume modify` Befehl zum Aktualisieren der Daten.

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

Wenn diese Werte nicht angezeigt werden, können Sie den verwenden `vserver services name-service unix-user modify` Befehl zum Aktualisieren der Daten.

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 |

Wenn diese Werte nicht angezeigt werden, können Sie den verwenden `vserver services name-service unix-group modify` Befehl zum Aktualisieren der Daten.

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 den verwenden `vserver nfs kerberos realm create` Befehl zum Erstellen der Kerberos-Bereichskonfiguration auf einer SVM.

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 entsprechenden Konfigurationswerte für das zu ermitteln `vserver nfs kerberos realm create` Befehl.
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 so konfigurieren, dass sie den Sicherheitsanforderungen für Ihre Umgebung entsprechen, indem Sie den verwenden `vserver nfs modify` Befehl mit dem `-permitted-enc-types` Parameter.

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 | <p>a. Konfigurieren Sie die von NFS Kerberos zulässigen Verschlüsselungstypen der SVM:</p> <pre>vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types</pre> <p>Trennen Sie mehrere Verschlüsselungstypen durch ein Komma.</p> <p>b. Überprüfen Sie, ob die Änderung erfolgreich war:</p> <pre>vserver nfs show -vserver vserver_name -fields permitted-enc- types</pre> |
| AES-128 oder AES-256 | <p>a. Legen Sie fest, auf welcher SVM und LIF Kerberos aktiviert ist:</p> <pre>vserver nfs kerberos interface show</pre> <p>b. Deaktivieren Sie Kerberos auf allen LIFs auf der SVM, deren NFS-Kerberos-Verschlüsselungstyp Sie ändern möchten:</p> <pre>vserver nfs kerberos interface disable -lif lif_name</pre> <p>c. Konfigurieren Sie die von NFS Kerberos zulässigen Verschlüsselungstypen der SVM:</p> <pre>vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types</pre> <p>Trennen Sie mehrere Verschlüsselungstypen durch ein Komma.</p> <p>d. Überprüfen Sie, ob die Änderung erfolgreich war:</p> <pre>vserver nfs show -vserver vserver_name -fields permitted-enc- types</pre> <p>e. Kerberos auf allen LIFs der SVM erneut aktivieren:</p> <pre>vserver nfs kerberos interface enable -lif lif_name -spn service_principal_name</pre> <p>f. Vergewissern Sie sich, dass Kerberos auf allen LIFs aktiviert ist:</p> <pre>vserver nfs kerberos interface show</pre> |

Aktivieren Sie Kerberos auf einer Daten-LIF

Sie können das verwenden `vserver nfs kerberos interface enable` Befehl zum Aktivieren von Kerberos auf einer Daten-LIF. 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 das SPN in einer anderen OU des Kerberos-Bereichs erstellen müssen, können Sie die Option angeben `-ou` Parameter.

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 | <code>-admin-username kdc_admin_username</code> |
| Sie haben keine KDC-Administratoranmeldedaten, haben aber eine Keytab-Datei aus dem KDC, die den Schlüssel enthält | <code>-keytab-uri {ftp http}://uri</code> |

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.
```

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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, BEISPIELHAFT 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 IRGEND EINER 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.