Konfiguration des SMB-Zugriffs auf eine SVM

ONTAP 9

NetApp
October 08, 2026

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

Inhalt

Konfiguration des SMB-Zugriffs auf eine SVM . . . 1
- Konfiguration des SMB-Zugriffs auf ONTAP SVMs . . . 1
- ONTAP SVMs erstellen, um SMB-Datenzugriff bereitzustellen . . . 1
- Es sollte überprüft werden, ob das SMB-Protokoll auf dem ONTAP SVM aktiviert ist. . . . 2
- ONTAP SMB LIFs erstellen . . . 3
- DNS für die ONTAP SMB-Hostnamensauflösung aktivieren . . . 7
- Einen SMB Server in einer Active Directory Domäne einrichten . . . 9
  - ONTAP Zeitdienste für SMB Server konfigurieren . . . 9
  - ONTAP Befehle zur Verwaltung der symmetrischen Authentifizierung auf NTP-Servern . . . 9
  - SMB-Server in einer ONTAP Active Directory-Domäne erstellen . . . 10
  - Erstellen von Keytab-Dateien für ONTAP SMB-Authentifizierung . . . 13
- Einen SMB Server in einer Arbeitsgruppe einrichten . . . 14
  - Informationen zur SMB-Serverkonfiguration in ONTAP Arbeitsgruppen . . . 14
  - SMB-Server auf der ONTAP SVM mit angegebenen Arbeitsgruppen erstellen . . . 14
  - Lokale ONTAP SMB-Benutzerkonten erstellen . . . 16
  - Lokale ONTAP SMB-Gruppen erstellen . . . 17
  - Verwaltung der lokalen ONTAP SMB-Gruppenmitgliedschaft . . . 18
- Aktivierte ONTAP SMB-Versionen überprüfen . . . 19
- ONTAP SMB-Server auf dem DNS-Server zuordnen . . . 21

Konfiguration des SMB-Zugriffs auf eine SVM

Konfiguration des SMB-Zugriffs auf ONTAP SVMs

Falls Sie noch keine SVM für den SMB-Clientzugriff konfiguriert haben, müssen Sie entweder eine neue SVM erstellen und konfigurieren oder eine vorhandene SVM konfigurieren. Die Konfiguration von SMB umfasst das Öffnen des SVM-Root-Volume-Zugriffs, das Erstellen eines SMB-Servers, das Erstellen einer LIF, das Aktivieren der Host-Name-Auflösung, das Konfigurieren der Namensdienste und, falls gewünscht, das Aktivieren der Kerberos-Sicherheit.

ONTAP SVMs erstellen, um SMB-Datenzugriff bereitzustellen

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

Bevor Sie beginnen

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

Schritte

1. Eine SVM erstellen: `vserver create -vserver` *`svm_name`* `-rootvolume` *`root_volume_name`* `-aggregate` *`aggregate_name`* `-rootvolume-security-style ntfs -language C.UTF-8 -ipspace` *`ipspace_name`*
   - Die NTFS-Einstellung für die `-rootvolume-security-style` Option verwenden.
   - Die Standardoption C.UTF-8 `-language` kann verwendet werden.
   - Die `ipspace` Einstellung ist optional.
2. Die Konfiguration und der Status der neu erstellten SVM können überprüft werden: `vserver show -vserver` *`vserver_name`*

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

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

Beispiele

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

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

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

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

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

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

Es sollte überprüft werden, ob das SMB-Protokoll auf dem ONTAP SVM aktiviert ist.

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

Über diese Aufgabe

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

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

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

Schritte

1. Es kann überprüft werden, welche Protokolle für die SVM aktuell aktiviert und deaktiviert sind: `vserver show -vserver vserver_name -protocols`

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

2. Gegebenenfalls kann ein Protokoll aktiviert oder deaktiviert werden:
   - Um das SMB-Protokoll zu aktivieren: `vserver add-protocols -vserver vserver_name -protocols cifs`
   - Ein Protokoll kann wie folgt deaktiviert werden: `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`
3. Bestätigen Sie, dass die aktivierten und deaktivierten Protokolle korrekt aktualisiert wurden: `vserver show -vserver vserver_name -protocols`

Beispiel

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

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

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

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

ONTAP SMB LIFs erstellen

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

Bevor Sie beginnen

- Der zugrunde liegende physische oder logische Netzwerkport muss auf den administrativen `up` Status

konfiguriert sein.

- Wenn geplant ist, einen Subnetznamen zu verwenden, um die IP-Adresse und den Netzwerkmaskenwert für ein LIF zuzuweisen, muss das Subnetz bereits existieren.

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

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

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

Über diese Aufgabe

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

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

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

Schritte

1. Eine LIF erstellen:

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

- Der `-role` Parameter ist nicht erforderlich, wenn eine LIF mithilfe einer Dienstrichtlinie erstellt wird (ab ONTAP 9.6).
- Der `-data-protocol` Parameter ist nicht erforderlich, wenn eine LIF mithilfe einer Dienstrichtlinie erstellt wird (ab ONTAP 9.6). Bei ONTAP 9.5 und älteren Versionen muss der `-data-protocol` Parameter bei der Erstellung der LIF angegeben werden und kann später nicht mehr geändert werden, ohne die Daten LIF zu löschen und neu zu erstellen.
- `-home-node` ist der Knoten, zu dem die LIF zurückkehrt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.

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

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

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

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

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

2. Überprüfen, ob die LIF erfolgreich erstellt wurde:

   ```
   network interface show
   ```

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

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

Beispiele

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

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

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

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

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

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
```

```
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

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

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

Verwandte Informationen

- "Netzwerk-Ping"
- "Netzwerkschnittstelle zurücksetzen"

DNS für die ONTAP SMB-Hostnamensauflösung aktivieren

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

Bevor Sie beginnen

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

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

Über diese Aufgabe

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

Schritte

1. DNS auf der SVM aktivieren: `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

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

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

```
enabled
```

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

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

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

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

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

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
          Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

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

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

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

Einen SMB Server in einer Active Directory Domäne einrichten

ONTAP Zeitdienste für SMB Server konfigurieren

Bevor ein SMB-Server in einem Active Domain Controller erstellt wird, muss sichergestellt werden, dass die Clusterzeit und die Zeit auf den Domänencontrollern der Domäne, zu der der SMB-Server gehören wird, innerhalb von fünf Minuten übereinstimmen.

Über diese Aufgabe

Die Cluster-NTP-Dienste sind so zu konfigurieren, dass für die Synchronisierung dieselben NTP-Server wie von der Active Directory-Domäne verwendet werden.

Ab ONTAP 9.5 ist die Einrichtung Ihres NTP-Servers mit symmetrischer Authentifizierung möglich.

Schritte

1. Zeitdienste werden mithilfe des `cluster time-service ntp server create`Befehls konfiguriert.
   - Um Zeitdienste ohne symmetrische Authentifizierung zu konfigurieren, ist folgender Befehl einzugeben: `cluster time-service ntp server create -server server_ip_address`
   - Um Zeitdienste mit symmetrischer Authentifizierung zu konfigurieren, den folgenden Befehl eingeben: `cluster time-service ntp server create -server server_ip_address -key-id key_id cluster time-service ntp server create -server 10.10.10.1 cluster time-service ntp server create -server 10.10.10.2`
2. Es kann überprüft werden, ob die Zeitdienste korrekt eingerichtet sind, indem der `cluster time-service ntp server show` Befehl verwendet wird.

   ```
   cluster time-service ntp server show
   ```

   ```
   Server                         Version
   ------------------------------ -------
   10.10.10.1                     auto
   10.10.10.2                     auto
   ```

Verwandte Informationen

- "Cluster Zeitdienst NTP"

ONTAP Befehle zur Verwaltung der symmetrischen Authentifizierung auf NTP-Servern

Ab ONTAP 9.5 wird das Network Time Protocol (NTP) Version 3 unterstützt. NTPv3 beinhaltet eine symmetrische Authentifizierung mit SHA-1-Schlüsseln, was die Netzwerksicherheit erhöht.

Dazu …	Verwenden Sie diesen Befehl…
Konfiguration eines NTP-Servers ohne symmetrische Authentifizierung	`cluster time-service ntp server create -server server_name`
Einen NTP-Server mit symmetrischer Authentifizierung konfigurieren	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
Symmetrische Authentifizierung für einen bestehenden NTP serverAn Server aktivieren. Ein bestehender NTP Server kann modifiziert werden, um die Authentifizierung durch Hinzufügen der erforderlichen Schlüssel-ID zu ermöglichen.	`cluster time-service ntp server modify -server server_name -key-id key_id`
Einen gemeinsamen NTP-Schlüssel konfigurieren	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` Gemeinsame Schlüssel werden über eine ID referenziert. Die ID, ihr Typ und ihr Wert müssen sowohl auf dem Knoten als auch auf dem NTP Server identisch sein.
Einen NTP-Server mit einer unbekannten Schlüssel-ID konfigurieren	`cluster time-service ntp server create -server server_name -key-id key_id`
Ein Server mit einer Schlüssel-ID, die auf dem NTP-Server nicht konfiguriert ist, wird konfiguriert.	`cluster time-service ntp server create -server server_name -key-id key_id` Die Schlüssel-ID, der Schlüsseltyp und der Schlüsselwert müssen mit der auf dem NTP-Server konfigurierten Schlüssel-ID, dem Schlüsseltyp und dem Schlüsselwert identisch sein.
Symmetrische Authentifizierung deaktivieren	`cluster time-service ntp server modify -server server_name -authentication disabled`

Verwandte Informationen

- "Cluster Zeitdienst NTP"

SMB-Server in einer ONTAP Active Directory-Domäne erstellen

Mit dem `vserver cifs create` Befehl lässt sich ein SMB-Server auf der SVM erstellen und die Active Directory (AD)-Domäne angeben, zu der er gehört.

Bevor Sie beginnen

Die von Ihnen zur Datenbereitstellung verwendeten SVM und LIFs müssen so konfiguriert sein, dass das SMB-Protokoll zugelassen ist. Die LIFs müssen eine Verbindung zu den auf der SVM konfigurierten DNS-Servern und zu einem AD-Domänencontroller der Domäne herstellen können, der der SMB-Server beitreten soll.

Jeder Benutzer, der berechtigt ist, Computerkonten in der AD-Domäne zu erstellen, zu der Sie den SMB-Server hinzufügen, kann den SMB-Server auf der SVM erstellen. Dies kann auch Benutzer aus anderen Domänen umfassen.

Sie benötigen die folgenden Mindestberechtigungen für die Organisationseinheit (OU), um den SMB-Server zu erstellen:

- Computerobjekte erstellen
- Computerobjekte löschen
- Passwort zurücksetzen
- Lese- und Schreibbeschränkungen für Konten
- Validierter Schreibvorgang zum DNS-Hostnamen
- Validierte Schreibvorgänge für Service Principal Names
- Lesen Sie msDS-SupportedEncryptedTypes
- Schreiben Sie msDS-SupportedEncryptedTypes

Ab ONTAP 9.7 kann Ihnen Ihr AD-Administrator als Alternative zu einem Namen und Passwort für ein privilegiertes Windows-Konto eine URI zu einer Keytab-Datei bereitstellen. Nach Erhalt der URI ist diese im `-keytab-uri` Parameter mit den `vserver cifs` Befehlen anzugeben.

Über diese Aufgabe

Beim Erstellen eines SMB-Servers in einer Activity Directory-Domäne:

- Es ist erforderlich, den vollqualifizierten Domainnamen (FQDN) zu verwenden, wenn die Domäne angegeben wird.
- Standardmäßig wird das SMB-Server-Computerkonto dem Active Directory CN=Computer-Objekt hinzugefügt.
- Sie können wählen, den SMB-Server mithilfe der `-ou` Option einer anderen Organisationseinheit hinzuzufügen.
- Ab ONTAP 9.13.1 können Sie einen Standardstandort für den SMB-Server konfigurieren. ONTAP kann diesen Standort verwenden, wenn ein LIF keiner Standortmitgliedschaft angehört, und als Ausweichmöglichkeit, falls die Standortermittlung für eine vertrauenswürdige Domäne beim Auffinden von Domänencontrollern der vertrauenswürdigen Domäne fehlschlägt.
- Optional kann eine durch Kommas getrennte Liste von einem oder mehreren NetBIOS-Aliasen (bis zu 200) für den SMB-Server hinzugefügt werden.

  Die Konfiguration von NetBIOS-Aliasen für einen SMB-Server kann nützlich sein, wenn Daten von anderen Dateiservern auf den SMB-Server konsolidiert werden und der SMB-Server auf die Namen der ursprünglichen Server reagieren soll.

Weitere Informationen zu `vserver cifs` und optionalen Parametern sowie Namensanforderungen finden Sie in der "ONTAP-Befehlsreferenz".

Ab ONTAP 9.8 kann angegeben werden, dass Verbindungen zu Domänencontrollern verschlüsselt werden. ONTAP erfordert die Verschlüsselung der Kommunikation mit Domänencontrollern, wenn die `-encryption -required-for-dc-connection` Option auf `true` gesetzt ist; der Standardwert ist `false`. Wenn die Option gesetzt ist, wird für ONTAP DC-Verbindungen ausschließlich das SMB3-Protokoll verwendet, da Verschlüsselung nur von SMB3 unterstützt wird. .

"SMB Management" enthält weitere Informationen zu den Konfigurationsoptionen des SMB-Servers.

Schritte

1. Es sollte überprüft werden, ob SMB auf Ihrem Cluster lizenziert ist: `system license show -package cifs`

   Die SMB-Lizenz ist mit "ONTAP One" enthalten. Wenn ONTAP One nicht vorhanden ist und die Lizenz nicht installiert ist, sollte der Vertriebsmitarbeiter kontaktiert werden.

   Eine CIFS-Lizenz ist nicht erforderlich, wenn der SMB-Server nur zur Authentifizierung verwendet wird.

2. Erstellen des SMB-Servers in einer AD-Domäne: `vserver cifs create -vserver vserver_name -cifs-server smb_server_name -domain FQDN [-ou organizational_unit][-default-site site_name][-netbios-aliases NetBIOS_name, ...][-keytab-uri {(ftp|http)://hostname|IP_address}][-comment text]`

   Beim Beitritt zu einer Domäne kann dieser Befehl mehrere Minuten in Anspruch nehmen.

   Der folgende Befehl erstellt den SMB-Server “smb_server01” in der Domäne “example.com”:

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   smb_server01 -domain example.com
   ```

   Der folgende Befehl erstellt den SMB-Server “smb_server02” in der Domäne “mydomain.com” und authentifiziert den ONTAP-Administrator mit einer Keytab-Datei:

   ```
   cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
   smb_server02 -domain mydomain.com -keytab-uri
   http://admin.mydomain.com/ontap1.keytab
   ```

3. Die SMB-Serverkonfiguration kann mit dem `vserver cifs show` Befehl überprüft werden.

   In diesem Beispiel zeigt die Befehlsausgabe, dass ein SMB-Server mit dem Namen “SMB_SERVER01” auf der SVM vs1.example.com erstellt und der Domäne “example.com” hinzugefügt wurde.

   ```
   cluster1::> vserver cifs show -vserver vs1

                                         Vserver: vs1.example.com
                       CIFS Server NetBIOS Name: SMB_SERVER01
                   NetBIOS Domain/Workgroup Name: EXAMPLE
                     Fully Qualified Domain Name: EXAMPLE.COM
   Default Site Used by LIFs Without Site Membership:
                              Authentication Style: domain
                 CIFS Server Administrative Status: up
                           CIFS Server Description: -
                           List of NetBIOS Aliases: -
   ```

Ab ONTAP 9.13.1 wird der Standardstandort des SMB-Servers auch als Fallback verwendet, wenn ONTAP keine Standortinformationen für eine vertrauenswürdige Domäne ermitteln kann.

1. Bei Bedarf kann die verschlüsselte Kommunikation mit dem Domänencontroller aktiviert werden (ONTAP 9.8 und höher): `vserver cifs security modify -vserver svm_name -encryption-required -for-dc-connection true`

Beispiele

Der folgende Befehl erstellt einen SMB-Server mit dem Namen „smb_server02“ auf der SVM vs2.example.com in der Domäne „example.com“. Das Computerkonto wird im Container „OU=eng,OU=corp,DC=example,DC=com“ erstellt. Dem SMB-Server wird ein NetBIOS-Alias zugewiesen.

```
cluster1::> vserver cifs create -vserver vs2.example.com –cifs-server
smb_server02 -domain example.com –ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1
                                        Vserver: vs2.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER02
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

Der folgende Befehl ermöglicht es einem Benutzer aus einer anderen Domäne, in diesem Fall einem Administrator einer vertrauenswürdigen Domäne, einen SMB-Server mit dem Namen „smb_server03“ auf der SVM vs3.example.com zu erstellen. Die `-domain` Option gibt den Namen der Heimatdomäne (in der DNS-Konfiguration festgelegt) an, in der der SMB-Server erstellt werden soll. Die `username` Option gibt den Administrator der vertrauenswürdigen Domäne an.

- Heimdomain: example.com
- Vertrauenswürdige Domain: trust.lab.com
- Benutzername für die vertrauenswürdige Domäne: Administrator1

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com

Username: Administrator1@trust.lab.com
Password: . . .
```

Erstellen von Keytab-Dateien für ONTAP SMB-Authentifizierung

Ab ONTAP 9.7 unterstützt ONTAP die SVM-Authentifizierung mit Active Directory (AD)-

Servern mithilfe von Keytab-Dateien. AD-Administratoren erstellen eine Keytab-Datei und stellen sie ONTAP Administratoren als Uniform Resource Identifier (URI) zur Verfügung, der bereitgestellt wird, wenn `vserver cifs` Befehle eine Kerberos-Authentifizierung mit der AD-Domäne erfordern.

AD-Administratoren können die Keytab-Dateien mithilfe des Standardbefehls von Windows Server `ktpass` erstellen. Der Befehl sollte in der primären Domäne ausgeführt werden, in der Authentifizierung erforderlich ist. Der `ktpass` Befehl kann verwendet werden, um Keytab-Dateien nur für Benutzer der primären Domäne zu generieren; Schlüssel, die mit Benutzern vertrauenswürdiger Domänen generiert wurden, werden nicht unterstützt.

Keytab-Dateien werden für bestimmte ONTAP-Admin-Benutzer generiert. Solange sich das Passwort des Admin-Benutzers nicht ändert, bleiben die für den jeweiligen Verschlüsselungstyp und die jeweilige Domain generierten Schlüssel unverändert. Daher ist eine neue Keytab-Datei erforderlich, sobald das Passwort des Admin-Benutzers geändert wird.

Folgende Verschlüsselungstypen werden unterstützt:

- AES256-SHA1
- DES-CBC-MD5

  ONTAP unterstützt den Verschlüsselungstyp DES-CBC-CRC nicht.

- RC4-HMAC

AES256 ist die höchste Verschlüsselungsstufe und sollte verwendet werden, wenn sie auf dem ONTAP System aktiviert ist.

Keytab-Dateien können entweder durch Angabe des Administratorpassworts oder durch Verwendung eines zufällig generierten Passworts erstellt werden. Es kann jedoch immer nur eine Passwortoption verwendet werden, da auf dem AD-Server ein dem Administrator zugeordneter privater Schlüssel benötigt wird, um die Schlüssel in der Keytab-Datei zu entschlüsseln. Jede Änderung des privaten Schlüssels eines bestimmten Administrators macht die Keytab-Datei ungültig.

Einen SMB Server in einer Arbeitsgruppe einrichten

Informationen zur SMB-Serverkonfiguration in ONTAP Arbeitsgruppen

Die Einrichtung eines SMB-Servers als Mitglied einer Arbeitsgruppe besteht aus der Erstellung des SMB-Servers und anschließend der Erstellung lokaler Benutzer und Gruppen.

Sie können einen SMB-Server in einer Arbeitsgruppe konfigurieren, wenn die Microsoft Active Directory-Domäneninfrastruktur nicht verfügbar ist.

Ein SMB-Server im Arbeitsgruppenmodus unterstützt nur die NTLM-Authentifizierung und unterstützt keine Kerberos-Authentifizierung.

SMB-Server auf der ONTAP SVM mit angegebenen Arbeitsgruppen erstellen

Mit dem `vserver cifs create`Befehl lässt sich ein SMB-Server auf der SVM erstellen und

die Arbeitsgruppe angeben, zu der er gehört.

Bevor Sie beginnen

Die von Ihnen zur Datenbereitstellung verwendeten SVM und LIFs müssen so konfiguriert sein, dass das SMB-Protokoll zugelassen ist. Die LIFs müssen in der Lage sein, eine Verbindung zu den auf der SVM konfigurierten DNS-Servern herzustellen.

Über diese Aufgabe

SMB-Server im Arbeitsgruppenmodus unterstützen die folgenden SMB-Funktionen nicht:

- SMB3 Witness-Protokoll
- SMB3 CA Shares
- SQL über SMB
- Ordnerumleitung
- Roaming Profile
- Gruppenrichtlinienobjekt (GPO)
- Volume Snapshot Service (VSS)

Weitere Informationen zu `vserver cifs` und optionalen Konfigurationsparametern sowie Namensanforderungen finden Sie in der "ONTAP-Befehlsreferenz".

Schritte

1. Es sollte überprüft werden, ob SMB auf Ihrem Cluster lizenziert ist: `system license show -package cifs`

   Die SMB-Lizenz ist mit "ONTAP One" enthalten. Wenn ONTAP One nicht vorhanden ist und die Lizenz nicht installiert ist, sollte der Vertriebsmitarbeiter kontaktiert werden.

   Eine CIFS-Lizenz ist nicht erforderlich, wenn der SMB-Server nur zur Authentifizierung verwendet wird.

2. Den SMB-Server in einer Arbeitsgruppe erstellen: `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

   Der folgende Befehl erstellt den SMB-Server “smb_server01” in der Arbeitsgruppe “workgroup01”:

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   SMB_SERVER01 -workgroup workgroup01
   ```

3. Die SMB-Serverkonfiguration kann mit dem `vserver cifs show` Befehl überprüft werden.

   Im folgenden Beispiel zeigt die Befehlsausgabe, dass ein SMB-Server mit dem Namen “smb_server01” auf der SVM vs1.example.com in der Arbeitsgruppe “workgroup01” erstellt wurde:

   ```
   cluster1::> vserver cifs show -vserver vs0

                                          Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
   ```

```
                    NetBIOS Domain/Workgroup Name: workgroup01
                      Fully Qualified Domain Name: -
                              Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
                                   Workgroup Name: workgroup01
                              Authentication Style: workgroup
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

Nachdem Sie fertig sind

Für einen CIFS-Server in einer Arbeitsgruppe sind lokale Benutzer und optional lokale Gruppen auf der SVM zu erstellen.

Verwandte Informationen

"SMB Management"

Lokale ONTAP SMB-Benutzerkonten erstellen

Sie können ein lokales Benutzerkonto erstellen, das zur Autorisierung des Zugriffs auf die im SVM enthaltenen Daten über eine SMB-Verbindung verwendet werden kann. Sie können lokale Benutzerkonten auch für die Authentifizierung beim Erstellen einer SMB-Sitzung verwenden.

Über diese Aufgabe

Die Funktionalität für lokale Benutzer ist bei der Erstellung der SVM standardmäßig aktiviert.

Wenn ein lokales Benutzerkonto erstellt wird, müssen ein Benutzername und die SVM angegeben werden, mit der das Konto verknüpft wird.

Weitere Informationen zu `vserver cifs users-and-groups local-user` und optionalen Parametern sowie Namensanforderungen finden Sie in der "ONTAP-Befehlsreferenz".

Schritte

1. Lokalen Benutzer anlegen: `vserver cifs users-and-groups local-user create -vserver` *`vserver_name`* `-user-name` *`user_name optional_parameters`*

   Folgende optionale Parameter könnten nützlich sein:

   - `-full-name`

     Der vollständige Name des Benutzers.

   - `-description`

     Eine Beschreibung für den lokalen Benutzer.

   - `-is-account-disabled {true|false}`

     Gibt an, ob das Benutzerkonto aktiviert oder deaktiviert ist. Wenn dieser Parameter nicht angegeben

wird, ist das Benutzerkonto standardmäßig aktiviert.

Der Befehl fordert zur Eingabe des Passworts des lokalen Benutzers auf.

2. Ein Passwort für den lokalen Benutzer eingeben und anschließend das Passwort bestätigen.
3. Es wird überprüft, ob der Benutzer erfolgreich erstellt wurde: `vserver cifs users-and-groups local-user show -vserver vserver_name`

Beispiel

Das folgende Beispiel erstellt einen lokalen Benutzer “SMB_SERVER01\sue” mit dem vollständigen Namen “Sue Chang”, der mit SVM vs1.example.com verknüpft ist:

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                   Full Name  Description
-------- --------------------------- ---------- -------------
vs1      SMB_SERVER01\Administrator             Built-in administrator
account
vs1      SMB_SERVER01\sue             Sue Chang
```

Lokale ONTAP SMB-Gruppen erstellen

Sie können lokale Gruppen erstellen, die zur Autorisierung des Zugriffs auf Daten im Zusammenhang mit der SVM über eine SMB-Verbindung verwendet werden können. Es ist außerdem möglich, Berechtigungen zuzuweisen, die festlegen, über welche Benutzerrechte oder -funktionen ein Mitglied der Gruppe verfügt.

Über diese Aufgabe

Die Funktionalität lokaler Gruppen ist standardmäßig aktiviert, wenn die SVM erstellt wird.

Beim Erstellen einer lokalen Gruppe müssen Sie einen Namen für die Gruppe angeben und die SVM angeben, mit der die Gruppe verknüpft werden soll. Sie können einen Gruppennamen mit oder ohne den lokalen Domänennamen angeben und optional eine Beschreibung für die lokale Gruppe angeben. Sie können keine lokale Gruppe zu einer anderen lokalen Gruppe hinzufügen.

Weitere Informationen zu `vserver cifs users-and-groups local-group` und optionalen Parametern sowie Namensanforderungen finden Sie in der "ONTAP-Befehlsreferenz".

Schritte

1. Lokale Gruppe erstellen: `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

   Der folgende optionale Parameter könnte nützlich sein:

- `-description`

  Eine Beschreibung für die lokale Gruppe.

2. Es wird überprüft, ob die Gruppe erfolgreich erstellt wurde: `vserver cifs users-and-groups local-group show -vserver vserver_name`

Beispiel

Das folgende Beispiel erstellt eine lokale Gruppe “SMB_SERVER01\engineering”, die mit SVM vs1 verknüpft ist:

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering

cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
Vserver          Group Name                     Description
---------------- ------------------------------ ----------------------------
vs1.example.com  BUILTIN\Administrators         Built-in Administrators
group
vs1.example.com  BUILTIN\Backup Operators       Backup Operators group
vs1.example.com  BUILTIN\Power Users            Restricted administrative
privileges
vs1.example.com  BUILTIN\Users                  All users
vs1.example.com  SMB_SERVER01\engineering
vs1.example.com  SMB_SERVER01\sales
```

Nachdem Sie fertig sind

Sie müssen der neuen Gruppe Mitglieder hinzufügen.

Verwaltung der lokalen ONTAP SMB-Gruppenmitgliedschaft

Sie können die Mitgliedschaft in lokalen Gruppen verwalten, indem Sie lokale oder Domänenbenutzer hinzufügen und entfernen oder Domänengruppen hinzufügen und entfernen. Dies ist nützlich, wenn der Zugriff auf Daten auf Grundlage der für die Gruppe festgelegten Zugriffskontrollen gesteuert werden soll oder wenn Benutzer die mit dieser Gruppe verbundenen Berechtigungen erhalten sollen.

Über diese Aufgabe

Wenn ein lokaler Benutzer, Domänenbenutzer oder eine Domänengruppe keine Zugriffsrechte oder Berechtigungen mehr basierend auf der Mitgliedschaft in einer Gruppe erhalten soll, kann das Mitglied aus der Gruppe entfernt werden.

Beim Hinzufügen von Mitgliedern zu einer lokalen Gruppe ist Folgendes zu beachten:

- Sie können keine Benutzer zur speziellen Gruppe *Everyone* hinzufügen.
- Sie können keine lokale Gruppe zu einer anderen lokalen Gruppe hinzufügen.

- Um einen Domänenbenutzer oder eine Domänengruppe zu einer lokalen Gruppe hinzuzufügen, muss ONTAP in der Lage sein, den Namen in eine SID aufzulösen.

Beim Entfernen von Mitgliedern aus einer lokalen Gruppe ist Folgendes zu beachten:

- Sie können keine Mitglieder aus der speziellen Gruppe *Everyone* entfernen.
- Um ein Mitglied aus einer lokalen Gruppe zu entfernen, muss ONTAP in der Lage sein, dessen Namen in eine SID aufzulösen.

Schritte

1. Ein Mitglied kann zu einer Gruppe hinzugefügt oder aus einer Gruppe entfernt werden.
   - Mitglied hinzufügen: `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     Sie können eine durch Kommas getrennte Liste von lokalen Benutzern, Domänenbenutzern oder Domänengruppen angeben, die zur angegebenen lokalen Gruppe hinzugefügt werden.

   - Mitglied entfernen: `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     Sie können eine durch Kommas getrennte Liste von lokalen Benutzern, Domänenbenutzern oder Domänengruppen angeben, die aus der angegebenen lokalen Gruppe entfernt werden.

Beispiele

Das folgende Beispiel fügt den lokalen Benutzer “SMB_SERVER01\sue” der lokalen Gruppe “SMB_SERVER01\engineering” auf SVM vs1.example.com hinzu:

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

Das folgende Beispiel entfernt die lokalen Benutzer “SMB_SERVER01\sue” und “SMB_SERVER01\james” aus der lokalen Gruppe “SMB_SERVER01\engineering” auf SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Aktivierte ONTAP SMB-Versionen überprüfen

Ihre ONTAP 9 Version bestimmt, welche SMB Versionen standardmäßig für Verbindungen mit Clients und Domänencontrollern aktiviert sind. Es sollte überprüft werden, ob der SMB Server die in Ihrer Umgebung benötigten Clients und Funktionen unterstützt.

Über diese Aufgabe

Für Verbindungen sowohl mit Clients als auch mit Domänencontrollern sollte nach Möglichkeit SMB 2.0 oder

höher aktiviert werden. Aus Sicherheitsgründen sollte die Verwendung von SMB 1.0 vermieden und SMB 1.0 deaktiviert werden, wenn verifiziert wurde, dass es in Ihrer Umgebung nicht erforderlich ist.

Ab ONTAP 9.3 ist sie auf neuen SVMs standardmäßig deaktiviert.

> Wenn `-smb1-enabled-for-dc-connections` auf `false` gesetzt ist, während `-smb1-enabled` auf `true` gesetzt ist, verweigert ONTAP als Client SMB 1.0-Verbindungen, akzeptiert jedoch weiterhin eingehende SMB 1.0-Verbindungen als Server.

"SMB Management" enthält Details zu unterstützten SMB Versionen und Funktionen.

Schritte

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

```
set -privilege advanced
```

2. Überprüfen, welche SMB-Versionen aktiviert sind:

```
vserver cifs options show
```

In der Liste kann nach unten gescrollt werden, um die für Clientverbindungen aktivierten SMB-Versionen anzuzeigen, und falls ein SMB-Server in einer AD-Domäne konfiguriert wird, auch die für AD-Domänenverbindungen.

3. Das SMB-Protokoll kann für Clientverbindungen je nach Bedarf aktiviert oder deaktiviert werden:
   - Eine SMB-Version aktivieren:

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
true
```

Mögliche Werte für `smb_version`:

- `-smb1-enabled`
- `-smb2-enabled`
- `-smb3-enabled`
- `-smb31-enabled`

Der folgende Befehl aktiviert SMB 3.1 auf SVM vs1.example.com: `cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31-enabled true`

   - Eine SMB-Version kann wie folgt deaktiviert werden:

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
false
```

4. Wenn sich Ihr SMB-Server in einer Active Directory-Domäne befindet, kann das SMB-Protokoll für DC-Verbindungen je nach Bedarf aktiviert oder deaktiviert werden:
   - Eine SMB-Version aktivieren:

     ```
     vserver cifs security modify -vserver <vserver_name> -smb2-enabled
     -for-dc-connections true
     ```

   - Eine SMB-Version kann wie folgt deaktiviert werden:

     ```
     vserver cifs security modify -vserver <vserver_name> -smb2-enabled
     -for-dc-connections false
     ```

5. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

ONTAP SMB-Server auf dem DNS-Server zuordnen

Der DNS-Server Ihrer Site muss einen Eintrag enthalten, der den SMB-Servernamen und alle NetBIOS-Aliase auf die IP-Adresse des Daten-LIF verweist, sodass Windows-Benutzer ein Laufwerk dem SMB-Servernamen zuordnen können.

Bevor Sie beginnen

Sie benötigen Administratorzugriff auf den DNS-Server Ihrer Website. Falls Sie keinen Administratorzugriff besitzen, ist der DNS-Administrator zu bitten, diese Aufgabe zu übernehmen.

Über diese Aufgabe

Wenn Sie NetBIOS-Aliase für den SMB-Servernamen verwenden, ist es eine bewährte Methode, für jeden Alias einen DNS-Server-Eintragspunkt zu erstellen.

Schritte

1. Melden Sie sich beim DNS Server an.
2. Vorwärts- (A - Adressdatensatz) und Rückwärts-Lookup-Einträge (PTR - Zeigerdatensatz) werden erstellt, um den SMB-Servernamen der IP-Adresse des Daten-LIF zuzuordnen.
3. Wenn Sie NetBIOS-Aliase verwenden, ist ein Alias-Canonical-Name-Lookup-Eintrag (CNAME-Ressourceneintrag) zu erstellen, um jeden Alias der IP-Adresse der Daten-LIF des SMB-Servers zuzuordnen.

Ergebnisse

Nachdem die Zuordnung im Netzwerk verbreitet wurde, können Windows-Benutzer ein Laufwerk dem SMB-Servernamen oder seinen NetBIOS-Aliasnamen zuordnen.

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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