



# Konfigurieren des SMB-Zugriffs auf eine SVM

ONTAP 9

NetApp  
April 24, 2024

# Inhalt

Konfigurieren des SMB-Zugriffs auf eine SVM .....	1
Konfigurieren des SMB-Zugriffs auf eine SVM .....	1
Erstellen einer SVM .....	1
Vergewissern Sie sich, dass das SMB-Protokoll auf der SVM aktiviert ist .....	3
Öffnen Sie die Exportrichtlinie für das SVM-Root-Volume .....	4
Erstellen eines LIF .....	5
Aktivieren Sie DNS für die Auflösung des Host-Namens .....	8
Richten Sie einen SMB-Server in einer Active Directory-Domäne ein .....	10
Richten Sie einen SMB-Server in einer Arbeitsgruppe ein .....	15
Überprüfen Sie die aktivierten SMB-Versionen .....	21
SMB-Server auf dem DNS-Server zuordnen .....	23

# Konfigurieren des SMB-Zugriffs auf eine SVM

## Konfigurieren des SMB-Zugriffs auf eine SVM

Wenn Sie noch keine SVM für den SMB-Client-Zugriff konfiguriert haben, müssen Sie entweder eine neue SVM erstellen und konfigurieren oder eine vorhandene SVM konfigurieren. Zum Konfigurieren von SMB werden der Root-Volume-Zugriff auf SVM, die Erstellung eines SMB-Servers, die Erstellung einer logischen Schnittstelle, die Aktivierung der Hostnamenauflösung, die Konfiguration von Name Services und, falls gewünscht, ermöglicht. Aktivieren der Kerberos-Sicherheit.

## Erstellen einer SVM

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

### Bevor Sie beginnen

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

### Schritte

1. SVM erstellen: `vserver create -vserver svm_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspace_name`

- Verwenden Sie die NTFS-Einstellung für das `-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 CIFS 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 erstellt `ipspaceA`:

```
cluster1::> vservers create -vservers 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 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::> vservers show -vservers 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 können Sie eine Vorlage für anpassungsfähige QoS-Richtliniengruppen festlegen und dabei einen Durchsatz- und Höchstwert für Volumes in dieser SVM anwenden. Sie können diese Richtlinie nur anwenden, nachdem Sie die SVM erstellt haben. Weitere Informationen zu diesem Prozess finden Sie unter [Legen Sie eine Vorlage für adaptive Richtliniengruppen fest](#).

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

Bevor Sie SMB auf SVMs konfigurieren und verwenden können, müssen Sie sicherstellen, dass 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 SMB-Protokoll: `vserver add-protocols -vserver vserver_name -protocols cifs`
- 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    cifs                        nfs, fcp, iscsi, ndmp
```

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

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

# Öffnen Sie die Exportrichtlinie für das SVM-Root-Volume

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

## Über diese Aufgabe

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

Sie sollten überprüfen, ob der gesamte SMB-Zugriff in der Standard-Exportrichtlinie geöffnet ist, und den Zugriff später auf einzelne Volumes einschränken, 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: cifs
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 cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. Überprüfen Sie die Regelerstellung mithilfe des `vserver export-policy rule show` Befehl.

## Ergebnisse

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

# 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.

## Bevor Sie beginnen

- 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 erstellt `network subnet create` Befehl.

- 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 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.

## Schritte

### 1. LIF erstellen:

```
network interface create -vserver vservice_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 früher

```
`network interface create -vserver vservice_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 vservice_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 beim Erstellen einer LIF mithilfe einer Service-Richtlinie nicht erforderlich (beginnend mit ONTAP 9.6).
- Der `-data-protocol` Parameter ist beim Erstellen einer LIF mithilfe einer Service-Richtlinie nicht erforderlich (beginnend mit ONTAP 9.6). Bei der Verwendung von ONTAP 9.5 und früheren Versionen wird der `-data-protocol` Parameter angegeben, wenn die LIF erstellt wird, und kann später nicht geändert werden, ohne die Daten-LIF zu zerstören und neu zu erstellen.
- `-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.

## 2. Überprüfen Sie, ob das LIF erfolgreich erstellt wurde:

```
network interface show
```

## 3. Vergewissern Sie sich, dass die konfigurierte IP-Adresse erreichbar ist:



Überprüfen einer...	Verwenden...
IPv4-Adresse	network ping
IPv6-Adresse	network ping6

## Beispiele

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

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port elc -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 cifs -home-node node-3 -home-port elc -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

Mit dem folgenden Befehl werden alle LIFs in Cluster-1 angezeigt. Datenschnittstellen Datenschnittstellen Datenverbund Daten3 werden mit IPv4-Adressen konfiguriert und Daten3 wird mit einer IPv6-Adresse konfiguriert:

```
network interface show
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
Home					
cluster-1					
true	cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a
node-1					
true	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
node-2					
true	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
vs1.example.com					
true	datalif1	up/down	192.0.2.145/30	node-1	e1c
vs3.example.com					
true	datalif3	up/up	192.0.2.146/30	node-2	e0c
true	datalif4	up/up	2001::2/64	node-2	e0c

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 ipspace1
```

## 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.

### Bevor Sie beginnen

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
```

- 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

## Richten Sie einen SMB-Server in einer Active Directory-Domäne ein

### Zeitdienste konfigurieren

Bevor Sie einen SMB-Server in einem Active Domain-Controller erstellen, müssen Sie sicherstellen, dass die Clusterzeit und die Zeit auf den Domänencontrollern der Domäne, zu der der SMB-Server gehört, innerhalb von fünf Minuten übereinstimmen.

#### Über diese Aufgabe

Sie sollten Cluster-NTP-Dienste so konfigurieren, dass sie dieselben NTP-Server für die Zeitsynchronisierung verwenden, die die Active Directory-Domäne verwendet.

Ab ONTAP 9.5 können Sie Ihren NTP-Server mit symmetrischer Authentifizierung einrichten.

#### Schritte

- Konfigurieren Sie Zeitdienste mithilfe von `cluster time-service ntp server create` Befehl.
  - Geben Sie den folgenden Befehl ein, um Zeitdienste ohne symmetrische Authentifizierung zu konfigurieren: `cluster time-service ntp server create -server server_ip_address`
  - Geben Sie den folgenden Befehl ein, um Zeitdienste mit symmetrischer Authentifizierung zu konfigurieren: `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`


- Überprüfen Sie, ob Zeitdienste ordnungsgemäß eingerichtet sind, indem Sie den verwenden `cluster time-service ntp server show` Befehl.


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

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

## Befehle für das Managen der symmetrischen Authentifizierung auf NTP-Servern

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

Hier...	Befehl
Konfigurieren Sie einen NTP-Server ohne symmetrische Authentifizierung	<code>cluster time-service ntp server create -server server_name</code>
Konfigurieren Sie einen NTP-Server mit symmetrischer Authentifizierung	<code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code>
Symmetrische Authentifizierung für einen vorhandenen NTP-Server aktivieren ein vorhandener NTP-Server kann angepasst werden, um die Authentifizierung durch Hinzufügen der erforderlichen Schlüssel-ID zu ermöglichen	<code>cluster time-service ntp server modify -server server_name -key-id key_id</code>
Konfigurieren Sie einen freigegebenen NTP-Schlüssel	<div> <code>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</code> </div> <div>  Freigegebene Schlüssel werden durch eine ID bezeichnet. Die ID, der Typ und der Wert müssen auf dem Node und dem NTP-Server identisch sein </div>
Konfigurieren Sie einen NTP-Server mit einer unbekannten Schlüssel-ID	<code>cluster time-service ntp server create -server server_name -key-id key_id</code>

Hier...	Befehl
Konfigurieren Sie einen Server mit einer Schlüssel-ID, die nicht auf dem NTP-Server konfiguriert ist.	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre> <div>  <p>Die Schlüssel-ID, der Typ und der Wert müssen identisch mit der auf dem NTP-Server konfigurierten Schlüssel-ID, dem Typ und dem Wert sein.</p> </div>
Deaktivieren Sie die symmetrische Authentifizierung	<pre>cluster time-service ntp server modify -server server_name -authentication disabled</pre>

## Erstellen Sie einen SMB-Server in einer Active Directory-Domäne

Sie können das verwenden `vserver cifs create` Befehl zum Erstellen eines SMB-Servers auf der SVM und zur Angabe der Active Directory-Domäne (AD), der sie angehört.

### Bevor Sie beginnen

Die SVM und die LIFs, die Sie zur Bedienung von Daten verwenden, müssen konfiguriert worden sein, um das SMB-Protokoll zu unterstützen. Die LIFs müssen in der Lage sein, eine Verbindung zu den DNS-Servern herzustellen, die auf der SVM konfiguriert sind, und zu einem AD-Domänencontroller der Domäne, mit dem Sie dem SMB-Server beitreten möchten.

Jeder Benutzer, der zum Erstellen von Computerkonten in der AD-Domäne autorisiert ist, zu der Sie dem SMB-Server beitreten, kann den SMB-Server auf der SVM erstellen. Dies kann auch Benutzer aus anderen Domänen umfassen.

Ab ONTAP 9.7 kann Ihr AD-Administrator Ihnen einen URI zu einer Keytab-Datei als Alternative zur Bereitstellung eines Namens und Kennworts für ein privilegiertes Windows-Konto zur Verfügung stellen. Wenn Sie den URI erhalten, geben Sie ihn in das ein `-keytab-uri` Parameter mit `vserver cifs` Befehle.

### Über diese Aufgabe

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

- Sie müssen den vollständig qualifizierten Domänennamen (FQDN) verwenden, wenn Sie die Domäne angeben.
- Die Standardeinstellung besteht darin, das SMB-Serverrechnerkonto dem Objekt Active Directory CN=Computer hinzuzufügen.
- Sie können den SMB-Server mit der zu einer anderen Organisationseinheit (OU) hinzufügen `-ou` Option.
- Sie können optional eine kommasetrennte Liste mit einem oder mehreren NetBIOS-Aliasen (bis zu 200) für den SMB-Server hinzufügen.

Das Konfigurieren von NetBIOS-Aliase für einen SMB-Server kann nützlich sein, wenn Sie Daten von anderen Dateiservern auf den SMB-Server konsolidieren und den SMB-Server auf die Namen der ursprünglichen Server reagieren möchten.

Der `vserver cifs` Man-Pages enthalten zusätzliche optionale Parameter und Benennungsanforderungen.



Ab ONTAP 9.1 können Sie SMB Version 2.0 aktivieren, um eine Verbindung zu einem Domain Controller (DC) herzustellen. Wenn Sie SMB 1.0 auf Domänencontrollern deaktiviert haben, ist dies erforderlich. Ab ONTAP 9.2 ist SMB 2.0 standardmäßig aktiviert.

Ab ONTAP 9.8 können Sie festlegen, dass Verbindungen zu Domänencontrollern verschlüsselt werden. ONTAP erfordert Verschlüsselung für Domain Controller-Kommunikation, wenn der `-encryption-required -for-dc-connection` Die Option ist auf festgelegt `true`; Die Standardeinstellung ist `false`. Wenn die Option eingestellt ist, wird nur das SMB3-Protokoll für ONTAP-DC-Verbindungen verwendet, da Verschlüsselung nur von SMB3 unterstützt wird. .

["SMB-Management"](#) Enthält weitere Informationen zu SMB-Serverkonfigurationsoptionen.

### Schritte

1. Vergewissern Sie sich, dass SMB für Ihr Cluster lizenziert ist: `system license show -package cifs`

Die SMB-Lizenz ist in enthalten ["ONTAP One"](#). Wenn Sie ONTAP One nicht besitzen und die Lizenz nicht installiert ist, wenden Sie sich an Ihren Vertriebsmitarbeiter.

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

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

Beim Beitritt zu einer Domäne kann dieser Befehl einige Minuten dauern.

Mit dem folgenden Befehl wird der SMB-Server „smb\_server01“ in der Domäne „`example.com`“ erstellt

```
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. Überprüfen Sie die SMB-Serverkonfiguration mit `vserver cifs show` Befehl.

In diesem Beispiel zeigt die Befehlsausgabe an, dass ein SMB-Server mit dem Namen „SMB\_SERVER01“ auf 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: -
```

4. Aktivieren Sie bei Bedarf die verschlüsselte Kommunikation mit dem Domain Controller (ONTAP 9.8 und höher): `vserver cifs security modify -vserver svm_name -encryption-required-for -dc-connection true`

### Beispiele

Mit dem folgenden Befehl wird ein SMB-Server mit dem Namen „smb\_server02“ auf SVM vs2.example.com in der Domäne „example.com“ erstellt. Das Maschinenkonto 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
```

Mit dem folgenden Befehl kann ein Benutzer aus einer anderen Domäne, in diesem Fall ein Administrator einer vertrauenswürdigen Domäne, einen SMB-Server mit dem Namen „smb\_server03“ auf SVM vs3.example.com erstellen. Der `-domain` Option gibt den Namen der Home-Domain an (angegeben in der DNS-Konfiguration), in der der SMB-Server erstellt werden soll. Der `username` Option gibt den Administrator der vertrauenswürdigen Domäne an.

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



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

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

```
Password: . . .
```

## Erstellen von Keytab-Dateien für die SMB-Authentifizierung

Ab ONTAP 9.7 unterstützt ONTAP die SVM-Authentifizierung mit Active Directory (AD) Servern unter Verwendung von Keytab-Dateien. AD-Administratoren erzeugen eine Keytab-Datei und stellen sie ONTAP-Administratoren als einheitliche Ressourcen-ID (URI) zur Verfügung, die bei der Bereitstellung bereitgestellt wird `vsync cifs` Befehle erfordern eine Kerberos-Authentifizierung mit der AD-Domäne.

AD-Administratoren können die Keytab-Dateien mit dem Standard-Windows-Server erstellen `ktpass` Befehl. Der Befehl sollte in der primären Domäne ausgeführt werden, in der eine Authentifizierung erforderlich ist. Der `ktpass` Der Befehl kann verwendet werden, um Keytab-Dateien nur für primäre Domain-Benutzer zu generieren; Schlüssel, die mit vertrauenswürdigen Domain-Benutzern generiert werden, werden nicht unterstützt.

Keytab-Dateien werden für bestimmte ONTAP Admin-Benutzer generiert. Solange sich das Passwort des Admin-Benutzers nicht ändert, ändern sich die für den jeweiligen Verschlüsselungstyp und die Domäne generierten Schlüssel nicht. Daher ist immer dann eine neue Keytab-Datei erforderlich, wenn 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 der höchste Verschlüsselungstyp und sollte verwendet werden, wenn diese auf dem ONTAP-System aktiviert ist.

Keytab-Dateien können entweder durch Angabe des Admin-Passworts oder durch die Verwendung eines zufällig generierten Passworts generiert werden. Allerdings kann zu einem bestimmten Zeitpunkt nur eine Kennwortoption verwendet werden, da ein privater Schlüssel, der für den Admin-Benutzer spezifisch ist, auf dem AD-Server zum Entschlüsseln der Schlüssel in der Keytab-Datei benötigt wird. Jede Änderung des privaten Schlüssels für einen bestimmten Administrator wird die Keytab-Datei ungültig.

## Richten Sie einen SMB-Server in einer Arbeitsgruppe ein

### Richten Sie einen SMB-Server in einer Übersicht über die Arbeitsgruppe ein

Die Einrichtung eines SMB-Servers als Mitglied in einer Arbeitsgruppe besteht darin, den

SMB-Server zu erstellen und dann lokale Benutzer und Gruppen zu erstellen.

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

Ein SMB-Server im Workgroup-Modus unterstützt nur NTLM-Authentifizierung und unterstützt keine Kerberos-Authentifizierung.

## Erstellen Sie einen SMB-Server in einer Arbeitsgruppe

Sie können das verwenden `vserver cifs create` Befehl zum Erstellen eines SMB-Servers auf der SVM und zur Angabe der Arbeitsgruppe, zu der er gehört.

### Bevor Sie beginnen

Die SVM und die LIFs, die Sie zur Bedienung von Daten verwenden, müssen konfiguriert worden sein, um das SMB-Protokoll zu unterstützen. Die LIFs müssen in der Lage sein, eine Verbindung zu den auf der SVM konfigurierten DNS-Servern herzustellen.

### Über diese Aufgabe

SMB-Server im Workgroup-Modus unterstützen die folgenden SMB-Funktionen nicht:

- SMB B3 Witness Protokoll
- SMB3 CA-Freigaben
- SQL und SMB
- Ordnerumleitung
- Roaming-Profile
- Gruppenrichtlinienobjekt (GPO)
- Volume Snapshot Service (VSS)

Der `vserver cifs` Man-Pages enthalten zusätzliche optionale Konfigurationsparameter und Benennungsanforderungen.

### Schritte

1. Vergewissern Sie sich, dass SMB für Ihr Cluster lizenziert ist: `system license show -package cifs`

Die SMB-Lizenz ist in enthalten "ONTAP One". Wenn Sie ONTAP One nicht besitzen und die Lizenz nicht installiert ist, wenden Sie sich an Ihren Vertriebsmitarbeiter.

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

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

Mit dem folgenden Befehl wird der SMB-Server „smb\_server01“ in der Arbeitsgruppe „workgroup01“ erstellt:

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

### 3. Überprüfen Sie die SMB-Serverkonfiguration mit `vserver cifs show` Befehl.

Im folgenden Beispiel zeigt die Befehlsausgabe an, dass auf SVM `vs1.example.com` in der Arbeitsgruppe „workgroup01“ ein SMB-Server mit dem Namen „smb\_server01“ 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 müssen lokale Benutzer und optional lokale Gruppen auf der SVM erstellt werden.

#### Verwandte Informationen

["SMB-Management"](#)

## Erstellen von lokalen Benutzerkonten

Sie können ein lokales Benutzerkonto erstellen, das über eine SMB-Verbindung für den Zugriff auf die in der SVM enthaltenen Daten verwendet werden kann. Sie können auch lokale Benutzerkonten zur Authentifizierung verwenden, wenn Sie eine SMB-Sitzung erstellen.

#### Über diese Aufgabe

Beim Erstellen der SVM ist die lokale Benutzerfunktion standardmäßig aktiviert.

Beim Erstellen eines lokalen Benutzerkontos müssen Sie einen Benutzernamen angeben. Zudem müssen Sie die SVM angeben, der das Konto zugeordnet werden soll.

Der `vserver cifs users-and-groups local-user` Handbuch-Seiten enthalten Details zu optionalen Parametern und Benennungsanforderungen.

#### Schritte

1. Erstellen Sie den lokalen Benutzer: `vserver cifs users-and-groups local-user create -vserver vserver_name -user-name user_name optional_parameters`

Die folgenden optionalen Parameter könnten hilfreich 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 die Standardeinstellung, das Benutzerkonto zu aktivieren.

Der Befehl fordert das Kennwort des lokalen Benutzers auf.

2. Geben Sie ein Kennwort für den lokalen Benutzer ein, und bestätigen Sie anschließend das Passwort.
3. Überprüfen Sie, ob der Benutzer erfolgreich erstellt wurde: `vserver cifs users-and-groups local-user show -vserver vserver_name`

### Beispiel

Im folgenden Beispiel wird ein lokaler Benutzer „SMB\_SERVER01\sue“ mit dem vollständigen Namen „Sue Chang“ erstellt, der SVM vs1.example.com zugeordnet 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
```

## Erstellen von lokalen Gruppen

Lokale Gruppen können zur Autorisierung des Zugriffs auf Daten, die der SVM zugeordnet sind, über eine SMB-Verbindung erstellt werden. Sie können auch Berechtigungen zuweisen, die definieren, welche Benutzerrechte oder Funktionen ein Mitglied der Gruppe hat.

### Über diese Aufgabe

Bei der Erstellung der SVM ist die Funktion der lokalen Gruppe standardmäßig aktiviert.

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

Der `vserver cifs users-and-groups local-group` Handbuch-Seiten enthalten Details zu optionalen Parametern und Benennungsanforderungen.

### Schritte

1. Erstellen Sie die lokale Gruppe: `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

Der folgende optionale Parameter könnte hilfreich sein:

- ° `-description`

Eine Beschreibung für die lokale Gruppe.

2. Vergewissern Sie sich, dass die Gruppe erfolgreich erstellt wurde: `vserver cifs users-and-groups local-group show -vserver vserver_name`

### Beispiel

Im folgenden Beispiel wird eine lokale Gruppe „SMB\_SERVER01\Engineering“ erstellt, die zu SVM vs1 gehört:

```
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 Gruppenmitgliedschaft

Sie können die lokale Gruppenmitgliedschaft verwalten, indem Sie lokale Benutzer oder

Domänenbenutzer hinzufügen und entfernen oder Domänengruppen hinzufügen und entfernen. Dies ist nützlich, wenn Sie den Zugriff auf Daten anhand von Zugriffskontrollen, die in der Gruppe platziert sind, steuern möchten oder wenn Benutzer über Berechtigungen verfügen möchten, die dieser Gruppe zugeordnet sind.

### Über diese Aufgabe

Wenn Sie nicht mehr möchten, dass ein lokaler Benutzer, ein Domänenbenutzer oder eine Domänengruppe aufgrund einer Mitgliedschaft in einer Gruppe Zugriffsrechte oder Berechtigungen besitzen soll, können Sie das Mitglied aus der Gruppe entfernen.

Beim Hinzufügen von Mitgliedern zu einer lokalen Gruppe müssen Sie Folgendes beachten:

- Sie können keine Benutzer zur speziellen *everyone*-Gruppe hinzufügen.
- Sie können einer anderen lokalen Gruppe keine lokale Gruppe hinzufügen.
- Um einen Domänenbenutzer oder eine Gruppe zu einer lokalen Gruppe hinzuzufügen, muss ONTAP in der Lage sein, den Namen zu einem SID aufzulösen.

Beim Entfernen von Mitgliedern aus einer lokalen Gruppe müssen Sie Folgendes beachten:

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

### Schritte

1. Fügen Sie ein Mitglied zu einer Gruppe hinzu oder entfernen Sie ein Mitglied aus einer Gruppe.

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

Sie können eine kommagetrennte Liste von lokalen Benutzern, Domänenbenutzern oder Domänengruppen angeben, die der angegebenen lokalen Gruppe hinzugefügt werden sollen.

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

Sie können eine durch Komma getrennte Liste der lokalen Benutzer, Domänenbenutzer oder Domänengruppen angeben, die aus der angegebenen lokalen Gruppe entfernt werden sollen.

### Beispiele

Im folgenden Beispiel wird der lokalen Gruppe „SMB\_SERVER01\sue“ auf SVM vs1.example.com ein lokaler Benutzer „SMB\_SERVER01\Engineering“ hinzugefügt:

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

Im folgenden Beispiel werden die lokalen Benutzer „SMB\_SERVER01\sue“ und „SMB\_SERVER01\james“ aus der lokalen Gruppe „SMB\_SERVER01\Engineering“ auf SVM vs1.example.com entfernt:

```
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
```

## Überprüfen Sie die aktivierten SMB-Versionen

Ihre ONTAP Version 9 legt fest, welche SMB-Versionen standardmäßig für Verbindungen mit Clients und Domänen-Controllern aktiviert sind. Überprüfen Sie, ob der SMB-Server die in Ihrer Umgebung erforderlichen Clients und Funktionen unterstützt.

### Über diese Aufgabe

Für Verbindungen mit Clients und Domänen-Controllern sollten Sie SMB 2.0 und höher aktivieren, sofern möglich. Aus Sicherheitsgründen sollten Sie die Verwendung von SMB 1.0 vermeiden. Sie sollten diese deaktivieren, wenn Sie bestätigt haben, dass dies in Ihrer Umgebung nicht erforderlich ist.

In ONTAP 9 sind SMB-Versionen 2.0 und höher standardmäßig für Client-Verbindungen aktiviert. Die standardmäßig aktivierte Version von SMB 1.0 hängt jedoch von Ihrer ONTAP Version ab.

- Ab ONTAP 9.1 P8 kann SMB 1.0 auf SVMs deaktiviert werden.

Der `-smb1-enabled` Option für die `vserver cifs options modify` Befehl aktiviert oder deaktiviert SMB 1.0.

- Ab ONTAP 9.3 ist die Funktion bei neuen SVMs standardmäßig deaktiviert.

Wenn sich Ihr SMB-Server in einer Active Directory-Domäne (AD) befindet, können Sie SMB 2.0 für die Verbindung zu einem Domain Controller (DC) aktivieren, der ab ONTAP 9.1 beginnt. Dies ist nötig, wenn Sie SMB 1.0 auf DCs deaktiviert haben. Ab ONTAP 9.2 ist SMB 2.0 standardmäßig für DC-Verbindungen aktiviert.



Wenn `-smb1-enabled-for-dc-connections` Ist auf festgelegt `false` Während `-smb1-enabled` Ist auf festgelegt `true`, ONTAP verweigert SMB 1.0-Verbindungen als Client, akzeptiert jedoch weiterhin eingehende SMB 1.0-Verbindungen als Server.

"[SMB-Management](#)" Enthält Details zu unterstützten SMB-Versionen und -Funktionen.

### Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Vergewissern Sie sich, welche SMB-Versionen aktiviert sind:

```
vserver cifs options show
```

Sie können in der Liste nach unten blättern, um die für Client-Verbindungen aktivierten SMB-Versionen anzuzeigen, und wenn Sie einen SMB-Server in einer AD-Domäne konfigurieren, für AD-Domänenverbindungen.

### 3. Aktivieren oder Deaktivieren des SMB-Protokolls für Client-Verbindungen nach Bedarf:

- So aktivieren Sie eine SMB-Version:

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

- So deaktivieren Sie eine SMB-Version:

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

Mögliche Werte für `smb_version`:

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

Mit dem folgenden Befehl wird SMB 3.1 auf SVM `vs1.example.com` aktiviert:

```
cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31-enabled true
```

### 1. Wenn sich Ihr SMB-Server in einer Active Directory-Domäne befindet, aktivieren oder deaktivieren Sie das SMB-Protokoll für DC-Verbindungen nach Bedarf:

- So aktivieren Sie eine SMB-Version:

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

- So deaktivieren Sie eine SMB-Version:

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

### 2. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```



# SMB-Server auf dem DNS-Server zuordnen

Der DNS-Server Ihres Standorts muss über einen Eintrag verfügen, der den SMB-Servernamen und alle NetBIOS-Aliase auf die IP-Adresse der Daten-LIF verweist, damit Windows-Benutzer ein Laufwerk dem SMB-Servernamen zuordnen können.

## Bevor Sie beginnen

Sie müssen über Administratorzugriff auf den DNS-Server Ihres Standorts verfügen. Wenn Sie keinen Administratorzugriff haben, müssen Sie den DNS-Administrator bitten, diese Aufgabe auszuführen.

## Über diese Aufgabe

Wenn Sie NetBIOS Aliase für den SMB-Servernamen verwenden, ist es eine Best Practice, DNS-Server-Einstiegspunkte für jeden Alias zu erstellen.

## Schritte

1. Melden Sie sich beim DNS-Server an.
2. Erstellen Sie Einträge zum Forward (A - Address Record) und Reverse (PTR - Zeigerdatensatz), um den Namen des SMB-Servers der IP-Adresse der Daten-LIF zuzuordnen.
3. Wenn Sie NetBIOS-Aliase verwenden, erstellen Sie einen Alias Canonical Name (CNAME Resource Record)-Sucheintrag, um jeden Alias der IP-Adresse der Daten-LIF des SMB-Servers zuzuordnen.

## Ergebnisse

Nachdem das Mapping über das Netzwerk verbreitet wurde, können Windows-Benutzer ein Laufwerk dem SMB-Servernamen oder seinen NetBIOS-Aliasen zuordnen.

## Copyright-Informationen

Copyright © 2024 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, 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.