



Configure el acceso de SMB a una SVM

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

- Configure el acceso de SMB a una SVM 1
 - Configure el acceso de SMB a una SVM 1
 - Cree una SVM 1
 - Compruebe que el protocolo SMB esté habilitado en la SVM 3
 - Abra la política de exportación del volumen raíz de la SVM 3
 - Cree una LIF 4
 - Habilite DNS para la resolución de nombres de host 8
 - Configurar un servidor SMB en un dominio de Active Directory 10
 - Configurar un servidor SMB en un grupo de trabajo 15
 - Compruebe las versiones habilitadas de SMB 20
 - Asigne el servidor SMB en el servidor DNS 22

Configure el acceso de SMB a una SVM

Configure el acceso de SMB a una SVM

Si todavía no tiene una SVM configurada para el acceso de cliente de SMB, debe crear y configurar una SVM nueva o configurar una SVM existente. La configuración de SMB implica abrir el acceso a volumen raíz de SVM, crear un servidor SMB, crear una LIF, habilitar la resolución de nombres de host, configurar servicios de nombres y, si lo desea, Habilitar la seguridad Kerberos.

Cree una SVM

Si no tiene al menos una SVM en un clúster para proporcionar acceso a los datos a los clientes de SMB, debe crear una.

Antes de empezar

- A partir de ONTAP 9.13.1, puede establecer una capacidad máxima para una máquina virtual de almacenamiento. También puede configurar alertas cuando la SVM se acerca a un nivel de umbral de capacidad. Para obtener más información, consulte [Gestionar la capacidad de SVM](#).

Pasos

1. Cree una SVM: `vserver create -vserver svm_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspace_name`
 - Utilice el valor NTFS para `-rootvolume-security-style` opción.
 - Utilice el C.UTF-8 predeterminado `-language` opción.
 - La `ipspace` el ajuste es opcional.

2. Compruebe la configuración y el estado de la SVM recién creada: `vserver show -vserver vserver_name`

La `Allowed Protocols` El campo debe incluir CIFS. Puede editar esta lista más tarde.

La `Vserver Operational State` el campo debe mostrar la `running` estado. Si muestra la `initializing` estado, significa que hubo un error en algunas operaciones intermedias, como la creación del volumen raíz, y que debe eliminarse la SVM y volver a crearla.

Ejemplos

El siguiente comando crea una SVM para el acceso de los datos en el espacio IP `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
```

El siguiente comando muestra que se creó una SVM con un volumen raíz de 1 GB, y se inició automáticamente y está en `running` estado. El volumen raíz tiene una política de exportación predeterminada que no incluye reglas, por lo que el volumen raíz no se exporta tras la creación.

```
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
```



A partir de ONTAP 9.13.1, puede establecer una plantilla de grupo de políticas de calidad de servicio adaptativa, aplicando un límite máximo y mínimo de rendimiento a los volúmenes en la SVM. Solo puede aplicar esta política después de crear la SVM. Para obtener más información sobre este proceso, consulte [Defina una plantilla de grupo de políticas adaptativas](#).

Compruebe que el protocolo SMB esté habilitado en la SVM

Antes de poder configurar y utilizar SMB en las SVM, debe comprobar que el protocolo esté habilitado.

Acerca de esta tarea

Esto suele hacerse durante la configuración de la SVM, pero si no ha habilitar el protocolo durante la configuración, puede habilitarla más adelante mediante el `vserver add-protocols` comando.



Una vez creado, no puede agregar ni quitar un protocolo de una LIF.

También puede deshabilitar protocolos en las SVM mediante el `vserver remove-protocols` comando.

Pasos

1. Compruebe qué protocolos están habilitados y deshabilitados actualmente para la SVM: `vserver show -vserver vserver_name -protocols`

También puede utilizar el `vserver show-protocols` Comando para ver los protocolos habilitados actualmente en todas las SVM del clúster.

2. Si es necesario, habilite o deshabilite un protocolo:

- Para habilitar el protocolo SMB: `vserver add-protocols -vserver vserver_name -protocols cifs`
- Para desactivar un protocolo: `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`

3. Confirme que los protocolos activados y deshabilitados se han actualizado correctamente: `vserver show -vserver vserver_name -protocols`

Ejemplo

El siguiente comando muestra qué protocolos están habilitados y deshabilitados actualmente (permitidos y deshabilitados) en la SVM llamada vs1:

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

El siguiente comando permite acceder a través de SMB añadiendo `cifs` A la lista de protocolos habilitados en la SVM llamada vs1:

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

Abra la política de exportación del volumen raíz de la SVM

La política de exportación predeterminada del volumen raíz de la SVM debe incluir una

regla para permitir que todos los clientes tengan acceso abierto a través de SMB. Sin esta regla, se deniega el acceso a la SVM y a sus volúmenes a todos los clientes SMB.

Acerca de esta tarea

Cuando se crea una SVM nueva, se crea automáticamente una política de exportación predeterminada (denominada predeterminada) para el volumen raíz de la SVM. Debe crear una o varias reglas para la política de exportación predeterminada para que los clientes puedan acceder a los datos de la SVM.

Debe verificar que todo el acceso a SMB esté abierto en la política de exportación predeterminada y, más adelante, restringir el acceso a volúmenes individuales mediante la creación de políticas de exportación personalizadas para volúmenes o qtrees individuales.

Pasos

1. Si va a utilizar una SVM existente, compruebe la política de exportación de volumen raíz predeterminada:

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

El resultado del comando debe ser similar a lo siguiente:

```
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
```

Si existe una regla de este tipo que permite el acceso abierto, esta tarea se completa. De lo contrario, continúe con el siguiente paso.

2. Cree una regla de exportación para el volumen raíz de la SVM: `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. Compruebe la creación de reglas mediante `vserver export-policy rule show` comando.

Resultados

Ahora, cualquier cliente de SMB puede acceder a cualquier volumen o qtree creado en la SVM.

Cree una LIF

Una LIF es una dirección IP asociada con un puerto físico o lógico. Si hay un fallo de un componente, un LIF puede conmutar al respaldo o migrarse a un puerto físico diferente,

lo que continúa comunicándose con la red.

Antes de empezar

- El puerto de red físico o lógico subyacente debe haber sido configurado para el administrador up estado.
- Si tiene pensado utilizar un nombre de subred para asignar la dirección IP y el valor de máscara de red para una LIF, la subred ya debe existir.

Las subredes contienen un grupo de direcciones IP que pertenecen a la misma subred de capa 3. Se crean mediante la `network subnet create` comando.

- El mecanismo para especificar el tipo de tráfico que maneja una LIF ha cambiado. Para ONTAP 9.5 y versiones anteriores, LIF usaba funciones para especificar el tipo de tráfico que gestionaría. A partir de ONTAP 9.6, los LIF utilizan políticas de servicio para especificar el tipo de tráfico que manejaría.

Acerca de esta tarea

- Puede crear tanto LIF IPv4 como IPv6 en el mismo puerto de red.
- Si tiene un gran número de LIF en su clúster, puede verificar la capacidad de LIF admitida en el clúster mediante el `network interface capacity show` Comando y la capacidad de LIF admitida en cada nodo mediante el `network interface capacity details show` (en el nivel de privilegio avanzado).
- A partir de ONTAP 9.7, si ya existen otras LIF para la SVM en la misma subred, no es necesario especificar el puerto de inicio de la LIF. ONTAP elige automáticamente un puerto aleatorio en el nodo raíz especificado en el mismo dominio de retransmisión que las otras LIF ya configuradas en la misma subred.

Pasos

1. Cree una LIF:

```
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 y anteriores
<code>`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</code>
<code>-subnet-name subnet_name} -firewall-policy data -auto-revert {true</code>
<code>false}`</code>

ONTAP 9.6 y posterior
<code>`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</code>
<code>-subnet-name subnet_name} -firewall-policy data -auto-revert {true</code>
<code>false}`</code>

- La `-role` No se requiere el parámetro al crear una LIF con una política de servicio (a partir de ONTAP 9.6).

- `-data-protocol` No se requiere el parámetro al crear una LIF con una política de servicio (a partir de ONTAP 9.6). Cuando se utiliza ONTAP 9,5 y versiones anteriores, el `-data-protocol` Debe especificarse el parámetro cuando se crea el LIF y no se puede modificar más adelante sin destruir ni volver a crear la LIF de datos.
- `-home-node` Es el nodo al que devuelve el LIF cuando el `network interface revert` El comando se ejecuta en la LIF.

También puede especificar si el LIF debería volver automáticamente al nodo raíz y al puerto raíz con el `-auto-revert` opción.

- `-home-port` Es el puerto físico o lógico al que devuelve la LIF cuando el `network interface revert` El comando se ejecuta en la LIF.
- Puede especificar una dirección IP con el `-address` y.. `-netmask` o puede habilitar la asignación desde una subred con `-subnet_name` opción.
- Al usar una subred para suministrar la dirección IP y la máscara de red, si la subred se definió con una puerta de enlace, se añadirá automáticamente a la SVM una ruta predeterminada a esa puerta de enlace cuando se cree una LIF con dicha subred.
- Si asigna direcciones IP manualmente (sin una subred), es posible que deba configurar una ruta predeterminada para una puerta de enlace si hay clientes o controladores de dominio en una subred IP diferente. La `network route create` La página man contiene información sobre la creación de una ruta estática dentro de una SVM.
- Para la `-firewall-policy` opción, utilice el mismo valor predeterminado `data` Como el rol de LIF.

Si lo desea, puede crear y agregar una política de firewall personalizada más adelante.



A partir de ONTAP 9.10.1, las políticas de firewall están obsoletas y sustituidas por completo por políticas de servicios LIF. Para obtener más información, consulte "[Configurar políticas de firewall para LIF](#)".

- `-auto-revert` Permite especificar si un LIF de datos se revierte automáticamente a su nodo principal en circunstancias como el inicio, los cambios en el estado de la base de datos de gestión o el momento en que se realiza la conexión de red. El valor predeterminado es `false`, pero puede establecerlo en `false` según las políticas de administración de red del entorno.

2. Compruebe que la LIF se ha creado correctamente:

```
network interface show
```

3. Compruebe que se pueda acceder a la dirección IP configurada:

Para verificar una...	Usar...
Dirección IPv4	<code>network ping</code>
Dirección IPv6	<code>network ping6</code>

Ejemplos

El siguiente comando crea una LIF y especifica la dirección IP y los valores de máscara de red mediante el `-address` y.. `-netmask` parámetros:


```
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
```

El siguiente comando crea una LIF y asigna valores de dirección IP y máscara de red a partir de la subred especificada (denominada cliente1_sub):

```
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
```

El siguiente comando muestra todas las LIF del clúster-1. Data LIF datalif1 y datalif3 están configurados con direcciones IPv4, y datalif4 está configurado con una dirección IPv6:

```
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.					

El siguiente comando muestra cómo crear una LIF de datos NAS asignada con default-data-files política de servicio:

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

Habilite DNS para la resolución de nombres de host

Puede utilizar el `vserver services name-service dns` Comando para habilitar DNS en una SVM y configurarlo para usar DNS en la resolución de nombres de host. Los

nombres de host se resuelven mediante servidores DNS externos.

Antes de empezar

Un servidor DNS para todo el sitio debe estar disponible para las búsquedas de nombre de host.

Debe configurar más de un servidor DNS para evitar un único punto de error. La `vserver services name-service dns create` El comando emite una advertencia si introduce solo un nombre de servidor DNS.

Acerca de esta tarea

La *Network Management Guide* contiene información acerca de la configuración de DNS dinámico en la SVM.

Pasos

1. Habilite DNS en la SVM: `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

El siguiente comando habilita los servidores DNS externos en la 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
```



A partir de ONTAP 9.2, el `vserver services name-service dns create` El comando realiza una validación automática de la configuración e informa de un mensaje de error si ONTAP no puede ponerse en contacto con el servidor de nombres.

2. Muestre las configuraciones del dominio DNS mediante `vserver services name-service dns show` comando. "

El siguiente comando muestra las configuraciones de DNS de todas las SVM del clúster:

```
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

El siguiente comando muestra información detallada de la configuración de DNS para SVM vs1:

```
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. Valide el estado de los servidores de nombres utilizando `vserver services name-service dns check` comando.

La `vserver services name-service dns check` El comando está disponible a partir de ONTAP 9.2.

```
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

Configurar un servidor SMB en un dominio de Active Directory

Configurar los servicios de tiempo

Antes de crear un servidor SMB en una controladora de Active Domain, debe asegurarse de que la hora y la hora del clúster de los controladores de dominio al que pertenecerá el servidor SMB coincidan con en un plazo de cinco minutos.

Acerca de esta tarea

Debe configurar los servicios NTP del clúster para que usen los mismos servidores NTP para la sincronización horaria que utiliza el dominio de Active Directory.

A partir de ONTAP 9.5, puede configurar el servidor NTP con autenticación simétrica.

Pasos

1. Configure los servicios de hora mediante el `cluster time-service ntp server create` comando.
 - Para configurar los servicios de hora sin autenticación simétrica, introduzca el siguiente comando:
`cluster time-service ntp server create -server server_ip_address`
 - Para configurar los servicios de hora con autenticación simétrica, introduzca el siguiente comando:
`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. Compruebe que los servicios de hora se han configurado correctamente mediante el `cluster time-service ntp server show` comando.


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

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

Comandos para gestionar la autenticación simétrica en servidores NTP

A partir de ONTAP 9.5, se admite la versión 3 del protocolo de tiempo de redes (NTP). NTPv3 incluye autenticación simétrica mediante claves SHA-1 que aumenta la seguridad de la red.

Para hacer esto...	Se usa este comando...
Configure un servidor NTP sin autenticación simétrica	<pre>cluster time-service ntp server create -server server_name</pre>
Configure un servidor NTP con autenticación simétrica	<pre>cluster time-service ntp server create -server server_ip_address -key-id key_id</pre>
Habilitar autenticación simétrica para un servidor NTP existente se puede modificar el servidor NTP existente para habilitar la autenticación agregando el Id. De clave requerido	<pre>cluster time-service ntp server modify -server server_name -key-id key_id</pre>
Configure una clave NTP compartida	<pre>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</pre> <div><p>Las claves compartidas se refieren a un ID. El ID, su tipo y el valor deben ser idénticos tanto en el nodo como en el servidor NTP</p></div>
Configure un servidor NTP con un ID de clave desconocido	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre>

Para hacer esto...	Se usa este comando...
Configure un servidor con un ID de clave no configurado en el servidor NTP.	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre> <div>  <p>El ID de clave, el tipo y el valor deben ser idénticos al ID de clave, el tipo y el valor configurados en el servidor NTP.</p> </div>
Deshabilitar la autenticación simétrica	<pre>cluster time-service ntp server modify -server server_name -authentication disabled</pre>

Cree un servidor SMB en un dominio de Active Directory

Puede utilizar el `vserver cifs create` Para crear un servidor SMB en la SVM y especificar el dominio de Active Directory (AD) al que pertenece.

Antes de empezar

Las SVM y los LIF que utiliza para servir datos deben haberse configurado para permitir el protocolo SMB. Las LIF deben poder conectarse a los servidores DNS configurados en la SVM y a un controlador de dominio AD del dominio al que desea unirse al servidor SMB.

Cualquier usuario con autorización para crear cuentas de máquina en el dominio de AD al que se va a unir el servidor SMB puede crear el servidor SMB en la SVM. Esto puede incluir usuarios de otros dominios.

A partir de ONTAP 9.7, el administrador de AD puede proporcionarle un URI a un archivo keytab como alternativa a proporcionarle un nombre y una contraseña a una cuenta de Windows con privilegios. Cuando reciba el URI, inclúyalo en el `-keytab-uri` con el `vserver cifs` comandos.

Acerca de esta tarea

Al crear un servidor SMB en un dominio de directorio de actividades:

- Debe usar el nombre de dominio completo (FQDN) al especificar el dominio.
- La configuración predeterminada es agregar la cuenta de máquina del servidor SMB al objeto CN=Computer de Active Directory.
- Puede optar por agregar el servidor SMB a una unidad organizativa (OU) diferente mediante el `-ou` opción.
- Opcionalmente, puede elegir agregar una lista delimitada por comas de uno o más alias NetBIOS (hasta 200) para el servidor SMB.

La configuración de alias NetBIOS para un servidor SMB puede ser útil cuando está consolidando datos de otros servidores de archivos en el servidor SMB y desea que el servidor SMB responda a los nombres de los servidores originales.

La `vserver cifs` las páginas de manual contienen parámetros opcionales y requisitos de nomenclatura adicionales.



A partir de ONTAP 9.1, puede habilitar SMB versión 2.0 para conectarse a un controlador de dominio (DC). Hacerlo es necesario si ha deshabilitado SMB 1.0 en controladores de dominio. A partir de ONTAP 9.2, SMB 2.0 está habilitado de forma predeterminada.

A partir de ONTAP 9.8, puede especificar que se cifren las conexiones a los controladores de dominio. ONTAP requiere cifrado para las comunicaciones del controlador de dominio cuando el `-encryption-required -for-dc-connection` opción establecida en `true`; el valor predeterminado es `false`. Cuando se establece la opción, solo se utilizará el protocolo SMB3 para las conexiones ONTAP-DC, ya que el cifrado solo es compatible con SMB3. .

"[Gestión de SMB](#)" Contiene más información acerca de las opciones de configuración del servidor SMB.

Pasos

1. Compruebe que SMB tiene licencia en el clúster: `system license show -package cifs`

La licencia SMB se incluye con "ONTAP One". Si no tiene ONTAP One y la licencia no está instalada, póngase en contacto con su representante de ventas.

No se requiere una licencia de CIFS si el servidor SMB se usará solo para autenticación.

2. Cree el servidor SMB en un dominio de AD: `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]`

Al unirse a un dominio, este comando puede tardar varios minutos en completarse.

El siguiente comando crea el servidor SMB «s' mb_server01» en el dominio "example.com":

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

El siguiente comando crea el servidor SMB «smemoria_servidor 2» en el dominio «mydomain.com» y autentica al administrador ONTAP con un archivo keytab:

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

3. Compruebe la configuración del servidor SMB mediante el `vserver cifs show` comando.

En este ejemplo, el resultado del comando muestra que se creó en SVM vs1.example.com un servidor SMB denominado "MB_SERVER01", que se unió al dominio "example.com".

```
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. Si lo desea, habilite la comunicación cifrada con el controlador de dominio (ONTAP 9.8 y posterior):
- ```
vserver cifs security modify -vserver svm_name -encryption-required-for-dc
-connection true
```

### Ejemplos

El siguiente comando crea un servidor SMB denominado «mb\_server02» en la SVM vs2.example.com en el dominio «'example.com'». La cuenta de equipo se crea en el contenedor "OU=eng,OU=corp,DC=example,DC=com". Al servidor SMB se le asigna un alias NetBIOS.

```
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
```

El siguiente comando permite a un usuario de un dominio diferente, en este caso un administrador de un dominio de confianza, crear un servidor SMB denominado «smemoria\_servidor03» en la SVM vs3.example.com. La `-domain` La opción especifica el nombre del dominio principal (especificado en la configuración DNS) en el que desea crear el servidor SMB. La `username` la opción especifica el administrador del dominio de confianza.

- Dominio principal: example.com
- Dominio de confianza: trust.lab.com
- Nombre de usuario del dominio de confianza: Administrador1



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

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

```
Password: . . .
```

## Crear archivos keytab para autenticación SMB

A partir de ONTAP 9.7, ONTAP admite la autenticación de SVM con servidores Active Directory (AD) mediante archivos keytab. Los administradores DE AD generan un archivo keytab y lo ponen a disposición de los administradores de ONTAP como un identificador uniforme de recursos (URI), que se proporciona cuando `vserver cifs`. Los comandos requieren autenticación Kerberos con el dominio AD.

Los administradores DE AD pueden crear los archivos keytab utilizando el servidor estándar de Windows `ktpass` comando. El comando debe ejecutarse en el dominio principal donde la autenticación es necesaria. La `ktpass` el comando se puede utilizar para generar archivos keytab sólo para usuarios de dominio principal; las claves generadas con usuarios de dominio de confianza no son compatibles.

Los archivos keytab se generan para usuarios específicos de administrador de ONTAP. Siempre que la contraseña del usuario administrador no cambie, las claves generadas para el tipo de cifrado específico y el dominio no cambiarán. Por lo tanto, se requiere un nuevo archivo keytab cada vez que se cambia la contraseña del usuario admin.

Se admiten los siguientes tipos de cifrado:

- AES256-SHA1
- DES-CBC-MD5



ONTAP no admite el tipo de cifrado DES-CBC-CRC.

- RC4-HMAC

AES256 es el tipo de cifrado más alto y se debe utilizar si está activado en el sistema ONTAP.

Los archivos keytab se pueden generar especificando la contraseña de administrador o mediante una contraseña generada aleatoriamente. Sin embargo, en cualquier momento sólo se puede utilizar una opción de contraseña, ya que en el servidor AD se necesita una clave privada específica para el usuario administrador para descifrar las claves del archivo keytab. Cualquier cambio en la clave privada de un administrador específico anulará el archivo keytab.

## Configurar un servidor SMB en un grupo de trabajo

### Configure un servidor SMB en una descripción general de grupo de trabajo

La configuración de un servidor SMB como miembro de un grupo de trabajo consiste en crear el servidor SMB y, a continuación, crear usuarios y grupos locales.

Puede configurar un servidor SMB en un grupo de trabajo cuando la infraestructura de dominio de Microsoft Active Directory no está disponible.

Un servidor SMB en modo de grupo de trabajo sólo admite autenticación NTLM y no admite autenticación Kerberos.

## Cree un servidor SMB en un grupo de trabajo

Puede utilizar el `vserver cifs create` Comando para crear un servidor SMB en la SVM y especificar el grupo de trabajo al que pertenece.

### Antes de empezar

Las SVM y los LIF que utiliza para servir datos deben haberse configurado para permitir el protocolo SMB. Los LIF deben poder conectarse con los servidores DNS que estén configurados en la SVM.

### Acerca de esta tarea

Los servidores SMB en modo de grupo de trabajo no admiten las siguientes funciones de SMB:

- Protocolo de testimonio de SMB3
- Recursos compartidos de CA de SMB3
- SQL sobre SMB
- Redirección de carpetas
- Perfiles de roaming
- Objeto de directiva de grupo (GPO)
- Servicio Snapshot de volumen (VSS)

La `vserver cifs` las páginas de manual contienen parámetros de configuración y requisitos de nomenclatura opcionales adicionales.

### Pasos

1. Compruebe que SMB tiene licencia en el clúster: `system license show -package cifs`

La licencia SMB se incluye con "ONTAP One". Si no tiene ONTAP One y la licencia no está instalada, póngase en contacto con su representante de ventas.

No se requiere una licencia de CIFS si el servidor SMB se usará solo para autenticación.

2. Cree el servidor SMB en un grupo de trabajo: `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

El siguiente comando crea el servidor SMB «s' mb\_server01» en el grupo de trabajo «'workgroup01'»:

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

3. Compruebe la configuración del servidor SMB mediante el `vserver cifs show` comando.

En el ejemplo siguiente, el resultado del comando muestra que se creó un servidor SMB denominado

«MB\_server01» en SVM vs1.example.com en el grupo de trabajo «'workgroup01'»:

```
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: -
```

### Después de terminar

Para un servidor CIFS en un grupo de trabajo, debe crear usuarios locales y, opcionalmente, grupos locales en la SVM.

### Información relacionada

["Gestión de SMB"](#)

## Crear cuentas de usuario locales

Se puede crear una cuenta de usuario local que se pueda utilizar para autorizar el acceso a los datos contenidos en la SVM a través de una conexión de SMB. También es posible usar cuentas de usuario locales para la autenticación al crear una sesión SMB.

### Acerca de esta tarea

La funcionalidad de usuario local se habilita de forma predeterminada cuando se crea la SVM.

Al crear una cuenta de usuario local, debe especificar un nombre de usuario y debe especificar la SVM con la que desea asociar la cuenta.

La `vserver cifs users-and-groups local-user` las páginas de manual contienen detalles sobre parámetros opcionales y requisitos de nomenclatura.

### Pasos

1. Cree el usuario local: `vserver cifs users-and-groups local-user create -vserver vserver_name -user-name user_name optional_parameters`

Los siguientes parámetros opcionales pueden ser útiles:

- ° `-full-name`

Nombre completo del usuario.

- -description

Una descripción para el usuario local.

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

Especifica si la cuenta de usuario está habilitada o deshabilitada. Si no se especifica este parámetro, el valor predeterminado es habilitar la cuenta de usuario.

El comando solicita la contraseña del usuario local.

2. Introduzca una contraseña para el usuario local y confirme la contraseña.

3. Compruebe que el usuario se ha creado correctamente: `vserver cifs users-and-groups local-user show -vserver vserver_name`

### Ejemplo

En el siguiente ejemplo se crea un usuario local «MMB\_SERVER01\sue», con el nombre completo «Sue Chang», asociado a SVM vs1.example.com:

```
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
```

## Crear grupos locales

Es posible crear grupos locales que se puedan utilizar para autorizar el acceso a los datos asociados con la SVM a través de una conexión de SMB. También puede asignar privilegios que definen los derechos de usuario o las capacidades que tiene un miembro del grupo.

### Acerca de esta tarea

La funcionalidad de grupo local se habilita de forma predeterminada cuando se crea la SVM.

Cuando se crea un grupo local, debe especificar un nombre para el grupo y debe especificar la SVM con la que desea asociar el grupo. Puede especificar un nombre de grupo con o sin el nombre de dominio local y, opcionalmente, puede especificar una descripción para el grupo local. No puede agregar un grupo local a otro grupo local.

La `vserver cifs users-and-groups local-group` las páginas de manual contienen detalles sobre parámetros opcionales y requisitos de nomenclatura.

## Pasos

1. Cree el grupo local: `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

El siguiente parámetro opcional puede ser útil:

- ° `-description`

Una descripción para el grupo local.

2. Compruebe que el grupo se ha creado correctamente: `vserver cifs users-and-groups local-group show -vserver vserver_name`

## Ejemplo

En el siguiente ejemplo se crea un grupo local "MB\_SERVER01\engineering" asociado con SVM vs1:

```
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   |
| vs1.example.com | BUILTIN\Backup Operators | Backup Operators group    |
| vs1.example.com | BUILTIN\Power Users      | Restricted administrative |
| vs1.example.com | BUILTIN\Users            | All users                 |
| vs1.example.com | SMB_SERVER01\engineering |                           |
| vs1.example.com | SMB_SERVER01\sales       |                           |

## Después de terminar

Debe agregar miembros al nuevo grupo.

## Administrar la pertenencia a grupos locales

Puede administrar la pertenencia a grupos locales agregando y eliminando usuarios locales o de dominio, o agregando y eliminando grupos de dominios. Esto resulta útil si desea controlar el acceso a los datos basándose en los controles de acceso colocados en el grupo o si desea que los usuarios tengan privilegios asociados a ese grupo.

### Acerca de esta tarea

Si ya no desea que un usuario local, un usuario de dominio o un grupo de dominio tenga derechos de acceso o privilegios basados en la pertenencia a un grupo, puede quitar el miembro del grupo.

Debe tener en cuenta lo siguiente al agregar miembros a un grupo local:

- No puede agregar usuarios al grupo especial *Everyone*.
- No puede agregar un grupo local a otro grupo local.
- Para agregar un usuario o grupo de dominio a un grupo local, ONTAP debe poder resolver el nombre a un SID.

Debe tener en cuenta lo siguiente al quitar miembros de un grupo local:

- No puede eliminar miembros del grupo especial *Everyone*.
- Para quitar un miembro de un grupo local, ONTAP debe poder resolver su nombre a un SID.

## Pasos

### 1. Agregar o quitar un miembro de un grupo.

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

Puede especificar una lista delimitada por comas de usuarios locales, usuarios de dominio o grupos de dominio que desee agregar al grupo local especificado.

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

Puede especificar una lista delimitada por comas de usuarios locales, usuarios de dominio o grupos de dominio que desee quitar del grupo local especificado.

## Ejemplos

En el siguiente ejemplo se agrega un usuario local "MB\_SERVER01\sue" al grupo local "MB\_SERVER01\engineering" en la SVM vs1.example.com:

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

En el siguiente ejemplo se eliminan los usuarios locales "MB\_SERVER01\sue" y "MB\_SERVER01\james" del grupo local "MB\_SERVER01\engineering" en la 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
```

## Compruebe las versiones habilitadas de SMB

En la versión ONTAP 9, se determinan las versiones de SMB que se habilitan de forma predeterminada para las conexiones con clientes y controladoras de dominio. Debe verificar si el servidor SMB admite los clientes y la funcionalidad que requiere su entorno.

**Acerca de esta tarea**

Para las conexiones con clientes y controladoras de dominio, debe habilitar SMB 2.0 y una versión posterior siempre que sea posible. Por motivos de seguridad, debe evitar el uso de SMB 1.0 y debe deshabilitarlo si ha verificado que no es necesario en su entorno.

En ONTAP 9, las versiones 2.0 y posteriores de SMB se habilitan de forma predeterminada para conexiones cliente, pero la versión de SMB 1.0 habilitada de forma predeterminada depende de su versión de ONTAP.

- A partir de ONTAP 9.1 P8, SMB 1.0 se puede deshabilitar en las SVM.

La `-smb1-enabled` de la `vserver cifs options modify` El comando habilita o deshabilita SMB 1.0.

- A partir de ONTAP 9.3, está deshabilitado de forma predeterminada en las nuevas SVM.

Si el servidor SMB se encuentra en un dominio de Active Directory (AD), es posible habilitar SMB 2.0 para conectarse a un controlador de dominio (DC) empezando por ONTAP 9.1. Es necesario hacerlo si ha deshabilitado SMB 1.0 en los centros de datos. A partir de ONTAP 9.2, SMB 2.0 está habilitado de forma predeterminada para las conexiones de CC.



Si `-smb1-enabled-for-dc-connections` se establece en `false` aunque `-smb1-enabled` se establece en `true`, ONTAP deniega las conexiones SMB 1.0 como cliente, pero continúa aceptando conexiones SMB 1.0 entrantes como servidor.

"[Gestión de SMB](#)" Contiene detalles sobre las versiones y la funcionalidad SMB admitidas.

## Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Compruebe qué versiones de SMB están habilitadas:

```
vserver cifs options show
```

Puede desplazarse hacia abajo por la lista para ver las versiones de SMB habilitadas para conexiones de clientes y si está configurando un servidor SMB en un dominio de AD para conexiones de dominio de AD.

3. Habilite o deshabilite el protocolo SMB para las conexiones de cliente según sea necesario:

- Para habilitar una versión de SMB:

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

- Para deshabilitar una versión de SMB:

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

Los valores posibles para `smb_version`:

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

El siguiente comando habilita SMB 3.1 en la SVM `vs1.example.com`:

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

1. Si el servidor SMB se encuentra en un dominio de Active Directory, habilite o deshabilite el protocolo SMB para las conexiones DC según sea necesario:

- Para habilitar una versión de SMB:

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

- Para deshabilitar una versión de SMB:

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

2. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

## Asigne el servidor SMB en el servidor DNS

El servidor DNS del sitio debe tener una entrada que apunte el nombre del servidor SMB y cualquier alias NetBIOS a la dirección IP de la LIF de datos para que los usuarios de Windows puedan asignar una unidad al nombre del servidor SMB.

### Antes de empezar

Debe tener acceso administrativo al servidor DNS del sitio. Si no tiene acceso administrativo, debe solicitar al administrador DNS que realice esta tarea.

### Acerca de esta tarea

Si utiliza alias NetBIOS para el nombre del servidor SMB, es una práctica recomendada crear puntos de entrada del servidor DNS para cada alias.



## **Pasos**

1. Inicie sesión en el servidor DNS.
2. Cree entradas de búsqueda hacia delante (a - Registro de dirección) e inversa (PTR - Registro de puntero) para asignar el nombre del servidor SMB a la dirección IP de la LIF de datos.
3. Si utiliza alias NetBIOS, cree una entrada de búsqueda Alias nombre canónico (registro de recursos CNAME) para asignar cada alias a la dirección IP de la LIF de datos del servidor SMB.

## **Resultados**

Una vez que la asignación se propaga a través de la red, los usuarios de Windows pueden asignar una unidad al nombre del servidor SMB o sus alias NetBIOS.

## Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

## Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.