



Configure SMB con la interfaz de línea de comandos

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

Configure SMB con la interfaz de línea de comandos	1
Obtenga información sobre la configuración del bloque de mensajes del servidor con la CLI de ONTAP ...	1
Otras maneras de hacerlo en ONTAP	1
Flujo de trabajo de configuración de SMB de ONTAP	2
Preparación	3
Evalúe los requisitos de almacenamiento físico para pymes de ONTAP	3
Evalúe los requisitos de red del bloque de mensajes del servidor de ONTAP	3
Obtenga más información sobre ONTAP el aprovisionamiento de capacidad de almacenamiento en el bloque de mensajes del servidor	4
Hoja de datos de configuración de SMB de ONTAP	5
Configure el acceso de SMB a una SVM	13
Configure el acceso de SMB a las SVM de ONTAP	13
Cree SVM de ONTAP para proporcionar acceso a datos de SMB	13
Compruebe que el protocolo SMB esté habilitado en la SVM de ONTAP	15
Abra la política de exportación SMB del volumen raíz de la SVM de ONTAP	16
Cree LIF SMB de ONTAP	17
Habilite DNS para la resolución de nombre de host en SMB de ONTAP	21
Configurar un servidor SMB en un dominio de Active Directory	22
Configurar un servidor SMB en un grupo de trabajo	27
Verifique las versiones de bloque de mensajes del servidor de ONTAP habilitadas	33
Asigne los servidores SMB de ONTAP en el servidor DNS	34
Configure el acceso de clientes SMB al almacenamiento compartido	35
Configure el acceso de cliente SMB al almacenamiento compartido de ONTAP	35
Cree un volumen o un contenedor de almacenamiento Qtree	35
Requisitos y consideraciones al crear recursos compartidos SMB de ONTAP	38
Crear recursos compartidos de SMB de ONTAP	39
Compruebe el acceso del cliente SMB de ONTAP	40
Cree listas de control de acceso compartido de SMB de ONTAP	41
Configure los permisos de archivos NTFS en recursos compartidos SMB de ONTAP	42
Compruebe el acceso al recurso compartido del usuario SMB de ONTAP	44

Configure SMB con la interfaz de línea de comandos

Obtenga información sobre la configuración del bloque de mensajes del servidor con la CLI de ONTAP

Es posible usar comandos de la CLI de ONTAP 9 para configurar el acceso del cliente SMB a los archivos ubicados en un volumen o un qtree nuevos de una SVM nueva o existente.



SMB (bloque de mensajes del servidor) hace referencia a los dialectos modernos del protocolo del sistema común de archivos de Internet (CIFS). Seguirá viendo *CIFS* en la interfaz de línea de comandos (CLI) de ONTAP y en las herramientas de gestión de OnCommand.

Use estos procedimientos si desea configurar el acceso de SMB a un volumen o qtree de la siguiente forma:

- Desea utilizar SMB versión 2 o posterior.
- Desea ofrecer servicio únicamente a clientes SMB, no a clientes NFS (no a configuración multiprotocolo).
- Se utilizarán permisos de archivo NTFS para proteger el nuevo volumen.
- Tiene privilegios de administrador de clúster, no de administrador de SVM.

Se necesitan privilegios de administrador de clúster para crear SVM y LIF. Los privilegios de administrador de SVM son suficientes para otras tareas de configuración de SMB.

- Desea utilizar la CLI, no System Manager ni una herramienta de secuencias de comandos automatizadas.

Para utilizar System Manager para configurar el acceso multiprotocolo NAS, consulte ["Aprovisione almacenamiento NAS para Windows y Linux usando NFS y SMB"](#).

- Quiere utilizar las prácticas recomendadas, no explorar todas las opciones disponibles.

Obtenga más información sobre los comandos descritos en este procedimiento en el ["Referencia de comandos del ONTAP"](#).

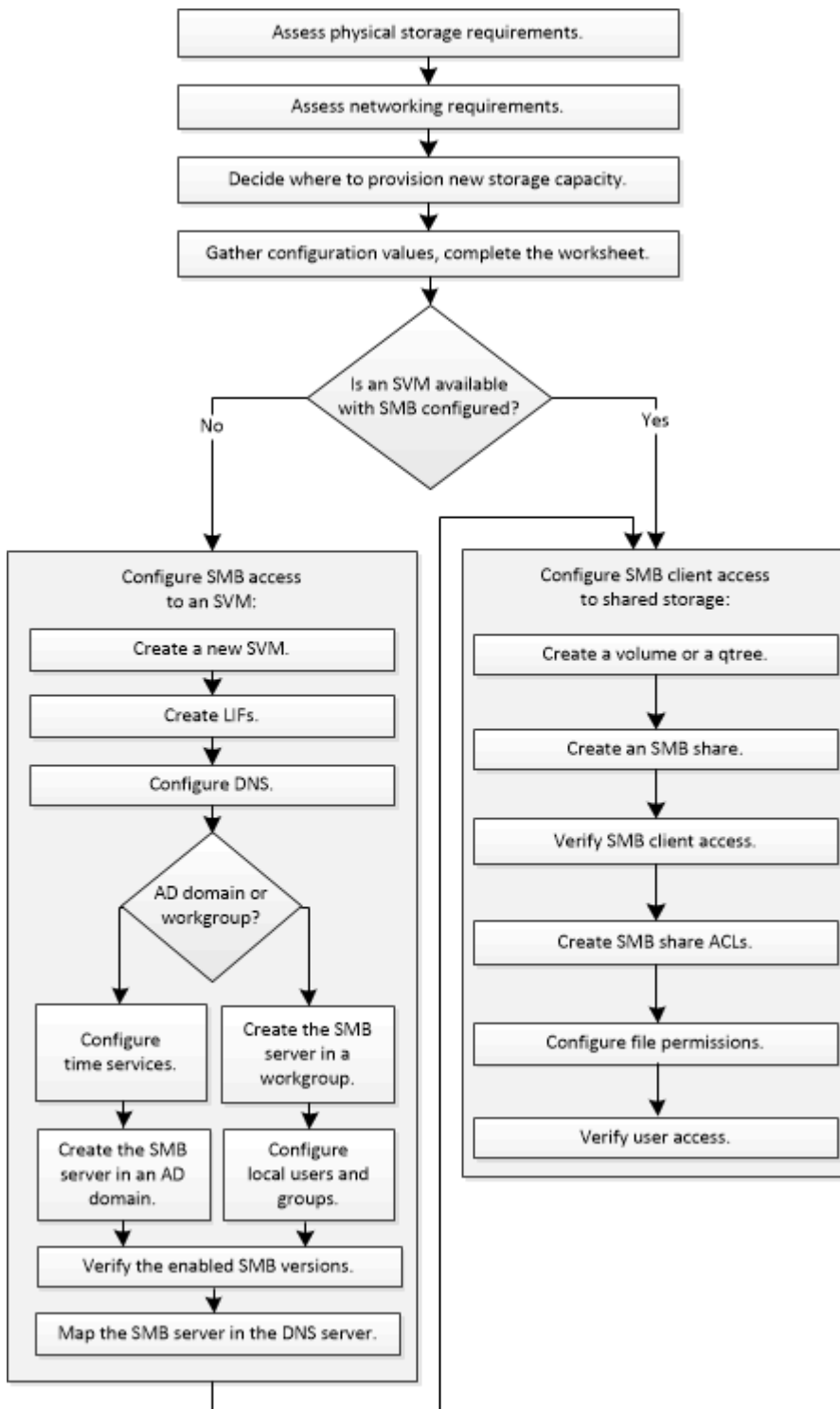
Si desea obtener más información sobre la gama de capacidades del protocolo SMB de ONTAP, consulte la ["Información general de referencia de SMB"](#).

Otras maneras de hacerlo en ONTAP

Para ejecutar estas tareas con...	Consulte...
System Manager rediseñado (disponible con ONTAP 9.7 y versiones posteriores)	"Aprovisionar almacenamiento NAS para servidores de Windows mediante SMB"
System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores)	"Información general de la configuración DE SMB"

Flujo de trabajo de configuración de SMB de ONTAP

La configuración de SMB implica evaluar los requisitos de almacenamiento físico y de red y, a continuación, elegir un flujo de trabajo específico del objetivo; configurar el acceso de SMB a una SVM nueva o existente; o añadir un volumen o qtree a una SVM existente que ya esté completamente configurada para el acceso del bloque de mensajes del servidor.



Preparación

Evalúe los requisitos de almacenamiento físico para pymes de ONTAP

Antes de aprovisionar almacenamiento de SMB para clientes, debe asegurarse de que haya espacio suficiente en un agregado existente para el nuevo volumen. Si no lo hay, puede añadir discos a un agregado existente o crear uno nuevo con el tipo deseado.

Pasos

1. Mostrar espacio disponible en los agregados existentes: `storage aggregate show`

Si hay un agregado con suficiente espacio, registre su nombre en la hoja de cálculo.

```
cluster::> storage aggregate show
```

Aggregate	Size	Available	Used%	State	#Vols	Nodes	RAID Status
aggr_0	239.0GB	11.13GB	95%	online	1	node1	raid_dp, normal
aggr_1	239.0GB	11.13GB	95%	online	1	node1	raid_dp, normal
aggr_2	239.0GB	11.13GB	95%	online	1	node2	raid_dp, normal
aggr_3	239.0GB	11.13GB	95%	online	1	node2	raid_dp, normal
aggr_4	239.0GB	238.9GB	95%	online	5	node3	raid_dp, normal
aggr_5	239.0GB	239.0GB	95%	online	4	node4	raid_dp, normal

6 entries were displayed.

2. Si no hay agregados con espacio suficiente, añada discos a un agregado existente mediante `storage aggregate add-disks` el comando o cree un agregado nuevo mediante el `storage aggregate create` comando.

Información relacionada

- ["agregado de almacenamiento, agregar discos"](#)
- ["creación de agregados de almacenamiento"](#)

Evalúe los requisitos de red del bloque de mensajes del servidor de ONTAP

Antes de proporcionar almacenamiento SMB a los clientes, debe comprobar que las redes se han configurado correctamente para cumplir los requisitos de aprovisionamiento de SMB.

Antes de empezar

Deben configurarse los siguientes objetos de red de clúster:

- Puertos físicos y lógicos
- Dominios de retransmisión
- Subredes (si es necesario)
- Espacios IP (según se requiera, además del espacio IP predeterminado)
- Grupos de conmutación por error (según sea necesario, además del grupo de conmutación por error predeterminado para cada dominio de retransmisión).
- Firewalls externos

Pasos

1. Muestra los puertos físicos y virtuales disponibles: `network port show`

- Cuando sea posible, debe utilizar el puerto con la velocidad más alta para la red de datos.
- Todos los componentes de la red de datos deben tener la misma configuración de MTU para obtener el mejor rendimiento.

Obtenga más información sobre `network port show` en el ["Referencia de comandos del ONTAP"](#).

2. Si tiene pensado utilizar un nombre de subred para asignar la dirección IP y el valor de máscara de red para una LIF, compruebe que la subred exista y que tenga suficientes direcciones disponibles: `network subnet show`

Obtenga más información sobre `network subnet show` en el ["Referencia de comandos del ONTAP"](#).

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

Obtenga más información sobre `network subnet create` en el ["Referencia de comandos del ONTAP"](#).

3. Mostrar espacios IP disponibles: `network ipspace show`

Puede usar el espacio IP predeterminado o un espacio IP personalizado.

Obtenga más información sobre `network ipspace show` en el ["Referencia de comandos del ONTAP"](#).

4. Si desea usar direcciones IPv6, compruebe que IPv6 esté habilitado en el clúster: `network options ipv6 show`

Si es necesario, puede habilitar IPv6 con `network options ipv6 modify` el comando.

Obtenga más información sobre `network options ipv6 show` y `network options ipv6 modify` en el ["Referencia de comandos del ONTAP"](#).

Obtenga más información sobre ONTAP el aprovisionamiento de capacidad de almacenamiento en el bloque de mensajes del servidor

Antes de crear un volumen o qtree de SMB nuevo, debe decidir si colocarlo en una SVM nueva o existente y cuánta configuración requiere la SVM. Esta decisión determina su flujo de trabajo.

Opciones

- Si desea aprovisionar un volumen o qtree en una SVM nueva o en una SVM existente con SMB habilitado pero sin configurar, complete los pasos de «"Configuración del acceso de SMB a una SVM" y «"adición de capacidad de almacenamiento a una SVM habilitada para SMB"».

[Configurar el acceso de SMB a una SVM](#)

[Configurar el acceso de clientes SMB a almacenamiento compartido](#)

Puede optar por crear una nueva SVM si se cumple alguna de las siguientes condiciones:

- Debe habilitar SMB en un clúster por primera vez.
- Tiene SVM existentes en un clúster en el cual no desea habilitar la compatibilidad con SMB.
- Tiene una o varias SVM habilitadas para SMB en un clúster y desea una de las siguientes conexiones:
 - A un bosque o grupo de trabajo de Active Directory diferente.
 - A un servidor SMB en un espacio de nombres aislado (escenario de multi-tenancy). También debe elegir esta opción para aprovisionar almacenamiento en una SVM existente con SMB habilitado pero sin configurar. Este puede ser el caso si se creó la SVM para el acceso SAN o si no se habilitó ningún protocolo cuando se creó la SVM.

Después de habilitar SMB en la SVM, continúe aprovisionando un volumen o un qtree.

- Si desea aprovisionar un volumen o qtree en una SVM existente que esté completamente configurada para el acceso SMB, complete los pasos del apartado «"adición de capacidad de almacenamiento a una SVM habilitada para SMB"».

[Configurar el acceso de clientes SMB a almacenamiento compartido](#)

Hoja de datos de configuración de SMB de ONTAP

La hoja de datos de configuración de SMB permite recopilar la información necesaria para configurar el acceso SMB para clientes.

Debe rellenar una o ambas secciones de la hoja de datos, en función de la decisión que haya tomado sobre dónde aprovisionar almacenamiento:

- Si va a configurar el acceso SMB a una SVM, debe completar ambas secciones.

[Configurar el acceso de SMB a una SVM](#)

[Configurar el acceso de clientes SMB a almacenamiento compartido](#)

- Si va a añadir capacidad de almacenamiento a una SVM habilitada para SMB, solo debe completar la segunda sección.

[Configurar el acceso de clientes SMB a almacenamiento compartido](#)

Obtenga más información sobre los parámetros en el ["Referencia de comandos del ONTAP"](#).

Configurar el acceso de SMB a una SVM

Parámetros para crear una SVM

Debe proporcionar estos valores con `vserver create` el comando si va a crear una SVM nueva. Obtenga más información sobre `vserver create` en el ["Referencia de comandos del ONTAP"](#).

Campo	Descripción	Su valor
<code>-vserver</code>	Un nombre que se proporciona para la SVM nueva que es un nombre de dominio completo (FQDN) o sigue otra convención que aplica nombres de SVM únicos en un clúster.	
<code>-aggregate</code>	El nombre de un agregado en el clúster con espacio suficiente para la nueva capacidad de almacenamiento de SMB.	
<code>-rootvolume</code>	Un nombre único que se proporciona para el volumen raíz de SVM.	
<code>-rootvolume-security-style</code>	Utilice el estilo de seguridad NTFS para la SVM.	<code>ntfs</code>
<code>-language</code>	Utilice la configuración de idioma predeterminada en este flujo de trabajo.	<code>C.UTF-8</code>
<code>ipspace</code>	Opcional: Los espacios IP son espacios de direcciones IP distintos en los que residen las SVM.	

Parámetros para crear una LIF

Proporcione estos valores con `network interface create` el comando cuando cree las LIF. Obtenga más información sobre `network interface create` en el ["Referencia de comandos del ONTAP"](#).

Campo	Descripción	Su valor
<code>-lif</code>	Nombre que se proporciona para la nueva LIF.	
<code>-role</code>	Utilice el rol de LIF de datos en este flujo de trabajo.	<code>data</code>
<code>-data-protocol</code>	Utilice solo el protocolo SMB en este flujo de trabajo.	<code>cifs</code>

Campo	Descripción	Su valor
-home-node	El nodo al que devuelve la LIF cuando <code>network interface revert</code> se ejecuta el comando en la LIF. Obtenga más información sobre <code>network interface revert</code> en el "Referencia de comandos del ONTAP" .	
-home-port	El puerto o grupo de interfaces al que devuelve la LIF cuando <code>network interface revert</code> se ejecuta el comando en la LIF.	
-address	La dirección IPv4 o IPv6 del clúster que se usará para el acceso a los datos mediante la nueva LIF.	
-netmask	La máscara de red y la puerta de enlace para la LIF.	
-subnet	Un conjunto de direcciones IP. Se utiliza en lugar de <code>-address</code> y <code>-netmask</code> para asignar direcciones y máscaras de red automáticamente.	
-firewall-policy	Utilice la política de firewall de datos predeterminada en este flujo de trabajo.	data
-auto-revert	Opcional: Especifica si un LIF de datos se revierte automáticamente a su nodo principal en el inicio o bajo otras circunstancias. El valor predeterminado es <code>false</code> .	

Parámetros para la resolución del nombre de host DNS

Proporcione estos valores con `vserver services name-service dns create` el comando cuando configura DNS. Obtenga más información sobre `vserver services name-service dns create` en el ["Referencia de comandos del ONTAP"](#).

Campo	Descripción	Su valor
-domains	Hasta cinco nombres de dominio DNS.	

Campo	Descripción	Su valor
-name-servers	Hasta tres direcciones IP para cada servidor de nombres DNS.	

Configuración de un servidor SMB en un dominio de Active Directory

Parámetros para la configuración del servicio de tiempo

Estos valores se proporcionan con el `cluster time-service ntp server create` comando cuando se configuran los servicios de hora. Obtenga más información sobre `cluster time-service ntp server create` en el ["Referencia de comandos del ONTAP"](#).

Campo	Descripción	Su valor
-server	El nombre de host o la dirección IP del servidor NTP para el dominio de Active Directory.	

Parámetros para crear un servidor SMB en un dominio de Active Directory

Debe proporcionar estos valores con el `vserver cifs create` comando al crear un nuevo servidor SMB y especificar la información del dominio. Obtenga más información sobre `vserver cifs create` en el ["Referencia de comandos del ONTAP"](#).

Campo	Descripción	Su valor
-vserver	Nombre de la SVM en la que se creará el servidor SMB.	
-cifs-server	El nombre del servidor SMB (hasta 15 caracteres).	
-domain	El nombre de dominio completo (FQDN) del dominio de Active Directory para asociarlo con el servidor SMB.	
-ou	Opcional: La unidad organizativa del dominio de Active Directory que se asocia con el servidor SMB. De forma predeterminada, este parámetro se establece en CN=Computers.	
-netbios-aliases	Opcional: Lista de alias NetBIOS, que son nombres alternativos al nombre del servidor SMB.	

Campo	Descripción	Su valor
-comment	Opcional: Comentario de texto para el servidor. Los clientes de Windows pueden ver esta descripción del servidor SMB al explorar servidores en la red.	

Configuración de un servidor SMB en un grupo de trabajo

Parámetros para crear un servidor SMB en un grupo de trabajo

Debe proporcionar estos valores con el `vserver cifs create` comando al crear un nuevo servidor SMB y especificar versiones SMB compatibles. Obtenga más información sobre `vserver cifs create` en el ["Referencia de comandos del ONTAP"](#).

Campo	Descripción	Su valor
-vserver	Nombre de la SVM en la que se creará el servidor SMB.	
-cifs-server	El nombre del servidor SMB (hasta 15 caracteres).	
-workgroup	El nombre del grupo de trabajo (hasta 15 caracteres).	
-comment	Opcional: Comentario de texto para el servidor. Los clientes de Windows pueden ver esta descripción del servidor SMB al explorar servidores en la red.	

Parámetros para crear usuarios locales

Estos valores se proporcionan cuando se crean usuarios locales con el `vserver cifs users-and-groups local-user create` comando. Son necesarios para los servidores SMB en grupos de trabajo y opcionales en dominios AD. Obtenga más información sobre `vserver cifs users-and-groups local-user create` en el ["Referencia de comandos del ONTAP"](#).

Campo	Descripción	Su valor
-vserver	El nombre de la SVM en la que se creará el usuario local.	
-user-name	El nombre del usuario local (hasta 20 caracteres).	

Campo	Descripción	Su valor
-full-name	Optional: Nombre completo del usuario. Si el nombre completo contiene un espacio, escriba el nombre completo entre comillas dobles.	
-description	Optional: Una descripción para el usuario local. Si la descripción contiene un espacio, el parámetro debe escribirse entre comillas.	
-is-account-disabled	Opcional: 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.	

Parámetros para crear grupos locales

Estos valores se proporcionan al crear grupos locales mediante el `vserver cifs users-and-groups local-group create` comando. Son opcionales para servidores SMB en dominios AD y grupos de trabajo. Obtenga más información sobre `vserver cifs users-and-groups local-group create` en el ["Referencia de comandos del ONTAP"](#).

Campo	Descripción	Su valor
-vserver	Nombre de la SVM en la que se creará el grupo local.	
-group-name	El nombre del grupo local (hasta 256 caracteres).	
-description	Opcional: Descripción del grupo local. Si la descripción contiene un espacio, el parámetro debe escribirse entre comillas.	

Se añade capacidad de almacenamiento a una SVM habilitada para SMB

Parámetros para crear un volumen

Debe introducir estos valores con `volume create` el comando si va a crear un volumen en lugar de un qtrees. Obtenga más información sobre `volume create` en el ["Referencia de comandos del ONTAP"](#).

Campo	Descripción	Su valor
-vserver	El nombre de una SVM nueva o existente que alojará el nuevo volumen.	
-volume	Se suministra un nombre descriptivo único para el volumen nuevo.	
-aggregate	El nombre de un agregado en el clúster de con espacio suficiente para el nuevo volumen de SMB.	
-size	Se proporciona un entero para el tamaño del nuevo volumen.	
-security-style	Utilice el estilo de seguridad NTFS para este flujo de trabajo.	ntfs
-junction-path	Ubicación bajo la raíz (/) donde se va a montar el nuevo volumen.	

Parámetros para crear un qtree

Debe proporcionar estos valores con `volume qtree create` el comando si va a crear un qtree en lugar de un volumen. Obtenga más información sobre `volume qtree create` en el ["Referencia de comandos del ONTAP"](#).

Campo	Descripción	Su valor
-vserver	El nombre de la SVM en la que reside el volumen que contiene el qtree.	
-volume	El nombre del volumen que contendrá el nuevo qtree.	
-qtree	Nombre descriptivo único que se proporciona para el nuevo qtree, con 64 caracteres o menos.	
-qtree-path	El argumento de la ruta de qtree en el formato <code>/vol/volume_name/qtree_name\></code> se puede especificar en lugar de especificar el volumen y el qtree como argumentos independientes.	

Parámetros para crear recursos compartidos SMB

Proporcione estos valores con el `vserver cifs share create` comando. Obtenga más información sobre `vserver cifs share create` en el ["Referencia de comandos del ONTAP"](#).

Campo	Descripción	Su valor
<code>-vserver</code>	Nombre de la SVM en la que se creará el recurso compartido de SMB.	
<code>-share-name</code>	El nombre del recurso compartido de SMB que se desea crear (hasta 256 caracteres).	
<code>-path</code>	El nombre de la ruta al recurso compartido de SMB (hasta 256 caracteres). Esta ruta debe existir en un volumen antes de crear el recurso compartido.	
<code>-share-properties</code>	Opcional: Una lista de propiedades de recursos compartidos. Los valores predeterminados son <code>oplocks</code> , <code>browsable</code> , <code>changenotify</code> y <code>show-previous-versions</code> .	
<code>-comment</code>	Optional: Comentario de texto para el servidor (hasta 256 caracteres). Los clientes de Windows pueden ver esta descripción del recurso compartido de SMB al navegar por la red.	

Parámetros para crear listas de control de acceso de recursos compartidos SMB (ACL)

Proporcione estos valores con el `vserver cifs share access-control create` comando. Obtenga más información sobre `vserver cifs share access-control create` en el ["Referencia de comandos del ONTAP"](#).

Campo	Descripción	Su valor
<code>-vserver</code>	Nombre de la SVM en la que se creará la ACL de SMB.	
<code>-share</code>	Nombre del recurso compartido de SMB en el que se va a crear.	

Campo	Descripción	Su valor
-user-group-type	El tipo del usuario o grupo que se añadirá a la ACL del recurso compartido. El tipo predeterminado es windows	windows
-user-or-group	El usuario o grupo que se añadirá a la ACL del recurso compartido. Si especifica el nombre de usuario, debe incluir el dominio del usuario con el formato "dain\username".	
-permission	Especifica los permisos para el usuario o grupo.	`[No_access
Read	Change	Full_Control]`

Configure el acceso de SMB a una SVM

Configure el acceso de SMB a las SVM de ONTAP

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 SVM de ONTAP para proporcionar acceso a datos de SMB

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 -ipstack ipstack_name`
 - Utilice la configuración NTFS para la `-rootvolume-security-style` opción.
 - Utilice `-language` la opción predeterminada C.UTF-8.
 - `-ipstack`El ajuste es opcional.`
2. Compruebe la configuración y el estado de la SVM recién creada: `vserver show -vserver vserver_name`

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

`Vserver Operational State`El campo debe mostrar `running` el estado. Si muestra `initializing` el estado, significa que se produjo un error en alguna operación intermedia como la creación del volumen raíz, y debe eliminar 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::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspaceA

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

El siguiente comando muestra que una SVM se creó con un volumen raíz de 1 GB, y se inició automáticamente y está `running` en 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::> vserver show -vserver vs1.example.com
Vserver: vs1.example.com
Vserver Type: data
Vserver Subtype: default
Vserver UUID: b8375669-19b0-11e5-b9d1-00a0983d9736
Root Volume: root_vs1
Aggregate: aggr1
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: C.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
Disallowed Protocols: -
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspaceA
```



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 de ONTAP

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

Acerca de esta tarea

Esto suele realizarse durante la configuración de la SVM, pero si no habilitó el protocolo durante la configuración, puede habilitarlo más adelante mediante `vserver add-protocols` el comando.



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

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

Pasos

1. Compruebe qué protocolos están habilitados y deshabilitados en 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 desactivados 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 el acceso a través de SMB agregando `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 SMB del volumen raíz de la SVM de ONTAP

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 utiliza 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. Verifique la creación de reglas con el `vserver export-policy rule show` comando.

Resultados

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

Cree LIF SMB de ONTAP

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 haberse configurado en el `up` estado administrativo. Obtenga más información sobre `up` en el ["Referencia de comandos del ONTAP"](#).
- 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 el `network subnet create` comando.

Obtenga más información sobre `network subnet create` en el ["Referencia de comandos del ONTAP"](#).

- 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 comprobar la capacidad de LIF compatible en el clúster mediante `network interface capacity show` el comando y la capacidad de LIF admitida en cada nodo mediante el comando `network interface capacity details show` (en el nivel de privilegio avanzado).

Obtenga más información sobre `network interface` en el ["Referencia de comandos del ONTAP"](#).

- 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

```
`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 y posterior

```
`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}`
```

- `-role`` No es necesario utilizar el parámetro cuando se crea una LIF mediante una política de servicio (empezando por ONTAP 9.6).
- `-data-protocol`` No es necesario utilizar el parámetro cuando se crea una LIF mediante una política de servicio (empezando por ONTAP 9.6). Cuando se utiliza ONTAP 9 E.5 y versiones anteriores, el `-data-protocol` parámetro se debe especificar al crear la 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 la LIF cuando `network interface revert` se ejecuta el comando en la LIF.

También puede especificar si el LIF debe volver automáticamente al nodo de inicio y al puerto de inicio con `-auto-revert` la opción.

- `-home-port`` Es el puerto físico o lógico al que devuelve la LIF cuando `network interface`

`revert` el comando se ejecuta en la LIF.

- Puede especificar una dirección IP con las `-address` `-netmask` opciones y, o bien habilitar la asignación desde una subred con `-subnet_name` la 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. Obtenga más información sobre `network route create` y cómo crear una ruta estática dentro de una SVM en el ["Referencia de comandos del ONTAP"](#).
- Para `-firewall-policy` la opción, utilice el mismo valor predeterminado `data` que el rol 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 una LIF de datos se revierte automáticamente a su nodo de inicio en circunstancias como el inicio, los cambios en el estado de la base de datos de gestión o el momento en que se establece la conexión de red. El valor por defecto es `false`, pero puede definirlo en `false` función de las políticas de gestión 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 la máscara de red mediante `-address` `-netmask` los parámetros y:

```
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
cluster-1	cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a
node-1	clus1	up/up	192.0.2.12/24	node-1	e0a
	clus2	up/up	192.0.2.13/24	node-1	e0b
	mgmt1	up/up	192.0.2.68/24	node-1	e1a
node-2	clus1	up/up	192.0.2.14/24	node-2	e0a
	clus2	up/up	192.0.2.15/24	node-2	e0b
	mgmt1	up/up	192.0.2.69/24	node-2	e1a
vs1.example.com	datalif1	up/down	192.0.2.145/30	node-1	e1c
vs3.example.com	datalif3	up/up	192.0.2.146/30	node-2	e0c
	datalif4	up/up	2001::2/64	node-2	e0c

5 entries were displayed.

El siguiente comando muestra cómo crear una LIF de datos NAS que está asignada a la 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
```

Información relacionada

- ["ping de red"](#)
- ["reversión de la interfaz de red"](#)

Habilite DNS para la resolución de nombre de host en SMB de ONTAP

Puede usar `vserver services name-service dns` el comando para habilitar DNS en una SVM y configurarlo para que utilice DNS para la resolución de nombre de host. Los nombres de host se resuelven mediante servidores DNS externos. Obtenga más información sobre `vserver services name-service dns` en el ["Referencia de comandos del ONTAP"](#).

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. El `vserver services name-service dns create` comando emite una advertencia si se introduce solo un nombre de servidor DNS. Obtenga más información sobre `vserver services name-service dns create` en el ["Referencia de comandos del ONTAP"](#).

Acerca de esta tarea

Más información sobre ["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
```



El `vserver services name-service dns create` comando realiza una validación automática de la configuración y informa un mensaje de error si ONTAP no puede contactar con el servidor de nombres.

2. Muestra la configuración del dominio DNS mediante `vserver services name-service dns show` el 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 mediante `vserver services name-service dns check` el comando.

```
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

Configure los servicios de tiempo de ONTAP para servidores SMB

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 utilizar los mismos servidores NTP para la sincronización 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 `cluster time-service ntp server create` el 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. Verifique que los servicios de hora están configurados correctamente mediante `cluster time-service ntp server show` el comando.

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

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

Información relacionada

- ["ntp de servicio horario del clúster"](#)

Comandos de ONTAP 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	<code>cluster time-service ntp server create -server server_name</code>
Configure un servidor NTP con autenticación simétrica	<code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code>
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	<code>cluster time-service ntp server modify -server server_name -key-id key_id</code>

Para hacer esto...	Se usa este comando...
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>
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>

Información relacionada

- ["ntp de servicio horario del clúster"](#)

Cree servidores SMB en un dominio de ONTAP Active Directory

Puede usar `vserver cifs create` el comando 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` parámetro con `vserver cifs` los 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 la `-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.

Obtenga más información acerca de `vserver cifs` los parámetros opcionales y los requisitos de nomenclatura en el ["Referencia de comandos del ONTAP"](#).

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 la `-encryption-required -for-dc-connection` opción está establecida en `true`; El valor por defecto 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 sobre 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. Verifique la configuración del servidor SMB mediante `vserver cifs show` el 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`. `domain` La opción especifica el nombre del dominio raíz (especificado en la configuración DNS) en el que desea crear el servidor SMB. `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: . . .
```

Cree archivos keytab para la autenticación SMB de ONTAP

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 de recursos uniforme (URI), que se proporciona cuando `vserver cifs` los comandos requieren la autenticación Kerberos con el dominio AD.

Los administradores DE AD pueden crear los archivos keytab utilizando `ktpass` el comando estándar de Windows Server. El comando debe ejecutarse en el dominio principal donde la autenticación es necesaria. El `ktpass` comando se puede utilizar para generar archivos keytab solo para usuarios de dominio primario; 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

Obtenga información sobre la configuración del servidor SMB en grupos de trabajo de ONTAP

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 servidores SMB en la SVM de ONTAP con grupos de trabajo especificados

Puede usar `vserver cifs create` el 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)

Obtenga más información acerca de `vserver cifs` los parámetros de configuración opcionales y los requisitos de nomenclatura en el ["Referencia de comandos del ONTAP"](#).

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. Verifique la configuración del servidor SMB mediante `vserver cifs show` el 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"](#)

Cree cuentas de usuario SMB de ONTAP 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.

Obtenga más información acerca de `vserver cifs users-and-groups local-user` los parámetros opcionales y los requisitos de nomenclatura en el ["Referencia de comandos del ONTAP"](#).

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
```

Cree grupos SMB de ONTAP 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.

Obtenga más información acerca de `vserver cifs users-and-groups local-group` los parámetros opcionales y los requisitos de nomenclatura en el ["Referencia de comandos del ONTAP"](#).

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
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	

Después de terminar

Debe agregar miembros al nuevo grupo.

Gestionar la pertenencia a un grupo SMB de ONTAP local

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.

- Agregar un 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.

- Eliminar 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
```

Verifique las versiones de bloque de mensajes del servidor de ONTAP habilitadas

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.

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



Si `-smb1-enabled-for-dc-connections` se establece en `false` while `-smb1-enabled` está establecido en `true`, ONTAP deniega las conexiones SMB 1,0 como cliente, pero continúa aceptando las conexiones SMB 1,0 entrantes como servidor.

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

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
```

Valores posibles para `smb_version`:

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

El siguiente comando habilita SMB 3,1 en SVM vs1.example.com: `cluster1::*> vserver`

```
cifs options modify -vserver vs1.example.com -smb31-enabled true
```

- Para deshabilitar una versión de SMB:

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

4. 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
```

5. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Asigne los servidores SMB de ONTAP 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.

Configure el acceso de clientes SMB al almacenamiento compartido

Configure el acceso de cliente SMB al almacenamiento compartido de ONTAP

Para proporcionar acceso al cliente SMB al almacenamiento compartido en una SVM, debe crear un volumen o qtree para proporcionar un contenedor de almacenamiento y, a continuación, crear o modificar un recurso compartido para ese contenedor. Luego, puede configurar los permisos de recursos compartidos y archivos, y probar el acceso desde sistemas cliente.

Antes de empezar

- El bloque de mensajes del servidor debe estar configurado por completo en la SVM.
- Se debe completar cualquier actualización de la configuración de los servicios de nombres.
- Cualquier adición o modificación a una configuración de dominio o grupo de trabajo de Active Directory debe estar completa.

Cree un volumen o un contenedor de almacenamiento Qtree

Cree volúmenes de bloque de mensajes del servidor de ONTAP

Puede crear un volumen y especificar su punto de unión y otras propiedades mediante `volume create` el comando.

Acerca de esta tarea

Un volumen debe incluir una *ruta de unión* para que sus datos estén disponibles para los clientes. Puede especificar la ruta de unión cuando cree un nuevo volumen. Si crea un volumen sin especificar una ruta de unión, debe *mount* el volumen en el espacio de nombres de la SVM con `volume mount` el comando.

Antes de empezar

- SMB debe estar configurado y en ejecución.
- El estilo de seguridad de la SVM debe ser NTFS.
- A partir de ONTAP 9.13.1, se pueden crear volúmenes con análisis de capacidad y seguimiento de actividades habilitados. Para activar la capacidad o el seguimiento de actividad, ejecute el `volume create` comando con `-analytics-state on` o `-activity-tracking-state on`.

Para obtener más información sobre el análisis de capacidad y el seguimiento de actividades, consulte ["Active File System Analytics"](#). Obtenga más información sobre `volume create` en el ["Referencia de comandos del ONTAP"](#).

Pasos

1. Cree el volumen con un punto de unión: `volume create -vserver svm_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]}`

```
-security-style ntfs -junction-path junction_path]
```

Las opciones para `-junction-path` son las siguientes:

- Directamente bajo raíz, por ejemplo, `/new_vol`

Puede crear un nuevo volumen y especificar que se monte directamente en el volumen raíz de SVM.

- En un directorio existente, por ejemplo, `/existing_dir/new_vol`

Puede crear un nuevo volumen y especificar que se monte en un volumen existente (en una jerarquía existente), expresado como un directorio.

Si desea crear un volumen en un nuevo directorio (en una jerarquía nueva en un volumen nuevo), por ejemplo, `/new_dir/new_vol`, primero debe crear un volumen primario nuevo que esté unido al volumen raíz de la SVM. A continuación, creará el nuevo volumen secundario en la ruta de unión del nuevo volumen principal (nuevo directorio).

2. Compruebe que el volumen se creó con el punto de unión deseado: `volume show -vserver svm_name -volume volume_name -junction`

Ejemplos

El siguiente comando crea un nuevo volumen denominado `user1` en la SVM `vs1.example.com` y el agregado `aggr1`. El nuevo volumen está disponible en `/users`. El tamaño del volumen es de 750 GB y su garantía de volumen es del tipo `volume` (de forma predeterminada).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
```

		Junction		Junction
Vserver	Volume	Active	Junction Path	Path Source
vs1.example.com	users1	true	/users	RW_volume

El siguiente comando crea un nuevo volumen denominado «'home4'» en la SVM «'vs1.example.com'» y el agregado «'aggr1'». El directorio `/eng/` ya existe en el espacio de nombres para la SVM de VS1, y el nuevo volumen está disponible en `/eng/home`, que se convierte en el directorio inicial del `/eng/` espacio de nombres. El volumen tiene un tamaño de 750 GB y su garantía de volumen es de tipo `volume` (de forma predeterminada).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	home4	true	/eng/home	RW_volume

Cree qtrees SMB de ONTAP

Puede crear un qtree para que contenga los datos y especificar sus propiedades mediante `volume qtree create` el comando.

Antes de empezar

- La SVM y el volumen que contendrán el nuevo qtree ya deben existir.
- El estilo de seguridad de la SVM debe ser NTFS y el SMB debe configurarse y ejecutarse.

Pasos

1. Cree el qtree: `volume qtree create -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs`

Puede especificar el volumen y el qtree como argumentos independientes, o bien especificar el argumento de la ruta de qtree en el formato `/vol/volume_name/_qtree_name`.

2. Compruebe que el qtree se ha creado con la ruta de unión deseada: `volume qtree show -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path }`

Ejemplo

En el ejemplo siguiente se crea un qtree llamado qt01 ubicado en la SVM vs1.example.com que tiene una ruta de unión `/vol/data1`:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path  
/vol/data1/qt01 -security-style ntfs  
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume qtree show -vserver vs1.example.com -qtree-path  
/vol/data1/qt01
```

```
          Vserver Name: vs1.example.com  
          Volume Name: data1  
          Qtree Name: qt01  
Actual (Non-Junction) Qtree Path: /vol/data1/qt01  
          Security Style: ntfs  
          Oplock Mode: enable  
          Unix Permissions: ---rwxr-xr-x  
          Qtree Id: 2  
          Qtree Status: normal  
          Export Policy: default  
Is Export Policy Inherited: true
```

Requisitos y consideraciones al crear recursos compartidos SMB de ONTAP

Antes de crear un recurso compartido SMB, debe comprender los requisitos para las rutas de acceso compartidas y las propiedades compartidas, especialmente para los directorios iniciales.

La creación de un recurso compartido de SMB implica especificar una estructura de ruta de directorio (mediante `-path` la opción del `vserver cifs share create` comando) a la que accederán los clientes. La ruta de directorio corresponde a la ruta de unión para un volumen o qtree que ha creado en el espacio de nombres de la SVM. Debe haber la ruta de directorio y la ruta de unión correspondiente antes de crear el recurso compartido.

Las rutas de recursos compartidos tienen los siguientes requisitos:

- Un nombre de ruta de acceso de directorio puede tener hasta 255 caracteres.
- Si hay un espacio en el nombre de la ruta de acceso, toda la cadena se debe poner entre comillas (por ejemplo, `"/new volume/mount here"`).
- Si la ruta UNC (`\\servername\sharename\filepath`) del recurso compartido contiene más de 256 caracteres (excluyendo el `"\"` inicial en la ruta UNC), entonces la pestaña **Seguridad** en el cuadro Propiedades de Windows no estará disponible.

Se trata de un problema del cliente Windows y no de un problema de ONTAP. Para evitar este problema, no cree recursos compartidos con rutas UNC con más de 256 caracteres.

Se pueden cambiar los valores predeterminados de las propiedades compartidas:

- Las propiedades iniciales por defecto para todos los recursos compartidos son `oplocks`, `browsable`, `changenotify` y `show-previous-versions`.

- Es opcional especificar propiedades de recurso compartido al crear un recurso compartido.

Sin embargo, si especifica propiedades de recurso compartido al crear el recurso compartido, no se utilizan los valores predeterminados. Si utiliza `-share-properties` el parámetro al crear un recurso compartido, debe especificar todas las propiedades de recurso compartido que desea aplicar al recurso compartido mediante una lista delimitada por comas.

- Para designar un recurso compartido de directorio principal, utilice la `homedirectory` propiedad.

Esta función permite configurar un recurso compartido que se asigna a directorios diferentes en función del usuario que se conecta a él y un conjunto de variables. En lugar de tener que crear recursos compartidos independientes para cada usuario, puede configurar un solo recurso compartido con varios parámetros del directorio inicial para definir la relación de un usuario entre un punto de entrada (el recurso compartido) y su directorio inicial (un directorio en la SVM).



No puede agregar ni quitar esta propiedad después de crear el recurso compartido.

Los recursos compartidos del directorio inicial tienen los siguientes requisitos:

- Antes de crear directorios iniciales SMB, debe añadir al menos una ruta de búsqueda del directorio inicial mediante `vserver cifs home-directory search-path add` el comando.
- Los recursos compartidos del directorio inicial especificados por el valor de `homedirectory` en el `-share-properties` parámetro deben incluir `%w` la variable dinámica (nombre de usuario de Windows) en el nombre del recurso compartido.

El nombre del recurso compartido puede contener además la `%d` variable dinámica (nombre de dominio) (por ejemplo, `%d/%w`) o una parte estática en el nombre del recurso compartido (por ejemplo, `home1_%w`).

- Si los administradores o usuarios utilizan el recurso compartido para conectarse a los directorios principales de otros usuarios (mediante las opciones del `vserver cifs home-directory modify` comando), el patrón de nombre de recurso compartido dinámico debe ir precedido por una tilde (`~`).

Obtenga más información sobre `vserver cifs share` en el ["Referencia de comandos del ONTAP"](#).

Información relacionada

- ["Gestión de SMB"](#)

Crear recursos compartidos de SMB de ONTAP

Debe crear un recurso compartido de SMB para poder compartir datos desde un servidor SMB con clientes SMB. Cuando se crea un recurso compartido, se pueden establecer propiedades de recurso compartido, como designar el recurso compartido como un directorio inicial. También puede personalizar el recurso compartido configurando ajustes opcionales.

Antes de empezar

La ruta de directorio del volumen o `qtree` debe existir en el espacio de nombres de la SVM antes de crear el recurso compartido.

Acerca de esta tarea

Al crear un recurso compartido, la ACL de uso compartido por defecto (permisos de uso compartido por

defecto) es Everyone / Full Control. Después de probar el acceso al recurso compartido, debe quitar la ACL de recurso compartido predeterminada y reemplazarla por una alternativa más segura.

Pasos

- 1. Si es necesario, cree la estructura de ruta de acceso de directorio para el recurso compartido.

El `vserver cifs share create` comando comprueba la ruta especificada en la `-path` opción durante la creación de recursos compartidos. Si la ruta especificada no existe, el comando falla.

- 2. Cree un recurso compartido de SMB asociado con la SVM especificada: `vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`
- 3. Compruebe que se ha creado el recurso compartido: `vserver cifs share show -share-name share_name`

Ejemplos

El siguiente comando crea un recurso compartido de SMB llamado «share1» en SVM `vs1.example.com`. Su ruta de acceso al directorio es `/users`, y se crea con propiedades predeterminadas.

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name SHARE1 -path /users

cluster1::> vserver cifs share show -share-name SHARE1
```

Vserver	Share	Path	Properties	Comment	ACL
vs1.example.com	SHARE1	/users	oplocks	-	Everyone / Full Control
			browsable		
			changenotify		
			show-previous-versions		

Compruebe el acceso del cliente SMB de ONTAP

Debe verificar si ha configurado SMB correctamente accediendo y escribiendo los datos en el recurso compartido. Debe probar el acceso utilizando el nombre del servidor SMB y todos los alias NetBIOS.

Pasos

- 1. Inicie sesión en un cliente Windows.
 - 2. Probar el acceso mediante el nombre del servidor SMB:
 - a. En el Explorador de Windows, asigne una unidad al recurso compartido en el siguiente formato: `\\SMB_Server_Name\Share_Name`
- Si la asignación no se realiza correctamente, es posible que la asignación DNS aún no se haya propagado por toda la red. Debe probar el acceso más adelante con el nombre del servidor SMB.

Si el servidor SMB se llama vs1.example.com y el recurso compartido se llama share1, debe introducir lo siguiente: `\\vs0.example.com\SHARE1`

b. En la unidad recién creada, cree un archivo de prueba y, a continuación, elimine el archivo.

Verificó el acceso de escritura al recurso compartido mediante el nombre del servidor SMB.

3. Repita el paso 2 para cualquier alias NetBIOS.

Cree listas de control de acceso compartido de SMB de ONTAP

La configuración de permisos de uso compartido mediante la creación de listas de control de acceso (ACL) para recursos compartidos de SMB permite controlar el nivel de acceso a un recurso compartido para usuarios y grupos.

Antes de empezar

Debe haber decidido qué usuarios o grupos tendrán acceso al recurso compartido.

Acerca de esta tarea

Puede configurar ACL de nivel compartido utilizando nombres de usuarios o grupos locales o de Windows de dominio.

Antes de crear una nueva ACL, debe suprimir la ACL de recurso compartido por defecto `Everyone / Full Control`, que representa un riesgo de seguridad.

En modo de grupo de trabajo, el nombre de dominio local es el nombre del servidor SMB.

Pasos

1. Suprima la ACL de recurso compartido predeterminada:
`vserver cifs share access-control delete -vserver vserver_name -share share_name -user-or-group everyone`
2. Configure la nueva ACL:

Si desea configurar las ACL utilizando...	Introduzca el comando...
Usuario de Windows	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\\user_name -permission access_right</pre>
Grupo Windows	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_group_name -permission access_right</pre>

3. Verifique que la ACL aplicada al recurso compartido es correcta mediante `vserver cifs share access-control show` el comando.

Ejemplo

El siguiente comando otorga Change permisos al grupo de Windows “Equipo de ventas” para el recurso compartido “ventas” en el “vs1.example.com” SVM:

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vserver cifs share access-control show
```

Vserver	Share Name	User/Group Name	User/Group Type	Access
vs1.example.com	c\$	BUILTIN\Administrators	windows	Full_Control
vs1.example.com	sales	DOMAIN\"Sales Team"	windows	Change

Los siguientes comandos dan Change permiso al grupo local de Windows llamado “Equipo Tigre” y Full_Control permiso al usuario local de Windows llamado “Sue Chang” para el recurso compartido “atavol5” en el “VS1” SVM:

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
```

Vserver	Share Name	User/Group Name	User/Group Type	Access
vs1	c\$	BUILTIN\Administrators	windows	Full_Control
vs1	datavol5	DOMAIN\"Tiger Team"	windows	Change
vs1	datavol5	DOMAIN\"Sue Chang"	windows	Full_Control

Configure los permisos de archivos NTFS en recursos compartidos SMB de ONTAP

Para habilitar el acceso a archivos para los usuarios o grupos que tienen acceso a un

recurso compartido, debe configurar permisos de archivos NTFS en archivos y directorios de ese recurso compartido desde un cliente de Windows.

Antes de empezar

El administrador que realiza esta tarea debe tener suficientes permisos NTFS para cambiar los permisos en los objetos seleccionados.

Acerca de esta tarea

"[Gestión de SMB](#)" Y la documentación de Windows contiene información sobre cómo establecer permisos NTFS estándar y avanzados.

Pasos

1. Inicie sesión en un cliente Windows como administrador.
2. En el menú **Herramientas** del Explorador de Windows, seleccione **asignar unidad de red**.
3. Complete el cuadro **Unidad de red de mapas**:

- a. Seleccione una letra **Unidad**.
- b. En el cuadro **Folder**, escriba el nombre del servidor SMB que contiene el recurso compartido que contiene los datos a los que desea aplicar los permisos y el nombre del recurso compartido.

Si el nombre de su servidor SMB es SMB_SERVER01 y su recurso compartido se denomina «share1», debe introducir \\SMB_SERVER01\SHARE1.



Puede especificar la dirección IP de la interfaz de datos para el servidor SMB en lugar del nombre del servidor SMB.

- c. Haga clic en **Finalizar**.

La unidad seleccionada está montada y lista con la ventana del Explorador de Windows que muestra archivos y carpetas contenidos en el recurso compartido.

4. Seleccione el archivo o directorio para el que desea establecer los permisos de archivo NTFS.
5. Haga clic con el botón secundario del ratón en el archivo o directorio y seleccione **Propiedades**.
6. Seleccione la ficha **Seguridad**.

La ficha Seguridad muestra la lista de usuarios y grupos para los que se ha establecido el permiso NTFS. El cuadro permisos para <Object> muestra una lista de los permisos permitir y denegar vigentes para el usuario o grupo seleccionado.

7. Haga clic en **Editar**.

Se abrirá el cuadro permisos para <Object>.

8. Realice las acciones deseadas:

Si quieres	Haga lo siguiente...
Establezca permisos NTFS estándar para un nuevo usuario o grupo	<p>a. Haga clic en Agregar.</p> <p>Se abre la ventana Seleccionar usuario, equipos, cuentas de servicio o grupos.</p> <p>b. En el cuadro Introduzca los nombres de objeto para seleccionar , escriba el nombre del usuario o grupo en el que desea agregar permiso NTFS.</p> <p>c. Haga clic en OK.</p>
Cambiar o quitar permisos NTFS estándar de un usuario o grupo	En el cuadro nombres de grupo o de usuario , seleccione el usuario o grupo que desea cambiar o quitar.

9. Realice las acciones deseadas:

Si desea...	Haga lo siguiente
Establezca permisos NTFS estándar para un usuario o grupo nuevo o existente	En el cuadro permisos para <Object> , seleccione los cuadros permitir o Denegar para el tipo de acceso que desea permitir o no permitir para el usuario o grupo seleccionado.
Quitar un usuario o un grupo	Haga clic en Quitar .



Si algunos o todos los cuadros de permiso estándar no se pueden seleccionar, es porque los permisos se heredan del objeto primario. El cuadro **permisos especiales** no se puede seleccionar. Si está seleccionada, significa que se han establecido uno o más derechos avanzados granulares para el usuario o grupo seleccionado.

10. Después de terminar de agregar, quitar o editar permisos NTFS en ese objeto, haga clic en **Aceptar**.

Compruebe el acceso al recurso compartido del usuario SMB de ONTAP

Debe probar que los usuarios configurados pueden acceder al recurso compartido de SMB y a los archivos que contiene.

Pasos

1. En un cliente Windows, inicie sesión como uno de los usuarios que ahora tiene acceso al recurso compartido.
2. En el menú **Herramientas** del Explorador de Windows, seleccione **asignar unidad de red**.
3. Complete el cuadro **Unidad de red de mapas**:
 - a. Seleccione una letra **Unidad**.
 - b. En el cuadro **carpeta**, escriba el nombre del recurso compartido que proporcionará a los usuarios.

Si el nombre de su servidor SMB es SMB_SERVER01 y su recurso compartido se denomina «share1», debe introducir \\SMB_SERVER01\share1.

c. Haga clic en **Finalizar**.

La unidad seleccionada está montada y lista con la ventana del Explorador de Windows que muestra archivos y carpetas contenidos en el recurso compartido.

4. Cree un archivo de prueba, compruebe que existe, escriba texto y quite el archivo de prueba.

Información de copyright

Copyright © 2026 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 INTERRUPTIÓN 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.