



# **Configure el acceso de NFS a una SVM**

## ONTAP 9

NetApp  
February 12, 2026

# Tabla de contenidos

Configure el acceso de NFS a una SVM .....	1
Crear SVM de ONTAP para el acceso a datos NFS .....	1
Verificar la habilitación del protocolo NFS en ONTAP SVM .....	2
Abrir el acceso del cliente NFS en ONTAP SVM .....	3
Crear servidores NFS de ONTAP .....	4
Crear LIF de ONTAP NFS .....	6
Habilitar DNS para la resolución de nombres de host de ONTAP NFS SVM .....	11
Configure los servicios de nombres .....	12
Obtenga más información sobre los servicios de nombres NFS de ONTAP .....	12
Configurar la tabla de conmutación del servicio de nombres NFS de ONTAP .....	12
Configurar usuarios y grupos UNIX locales .....	13
Trabajar con netgroups .....	17
Crear configuraciones de dominio NIS para SVM NFS de ONTAP .....	20
Utilice LDAP .....	21
Utilice Kerberos con NFS para una mayor seguridad .....	30
Obtenga información sobre el uso de Kerberos con ONTAP NFS para la autenticación de seguridad ..	30
Verificar los permisos de UNIX para las configuraciones NFS Kerberos en las SVM de ONTAP .....	31
Crear configuraciones de dominio Kerberos de NFS en SVM de ONTAP .....	32
Configurar los tipos de cifrado permitidos por NFS Kerberos para las SVM de ONTAP .....	33
Habilitar NFS Kerberos en LIF de ONTAP .....	35

# Configure el acceso de NFS a una SVM

## Crear SVM de ONTAP para el acceso a datos NFS

Si no tiene al menos una SVM en un clúster para proporcionar acceso a los datos a los clientes de NFS, 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 vserver_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style unix -language C.UTF-8 -ipspace ipspace_name
```

- Utilice la configuración de UNIX para `-rootvolume-security-style` la opción.
- Utilice `-language` la opción predeterminada C.UTF-8.
- ``ipspace`` El ajuste es opcional.

2. Compruebe la configuración y el estado de la SVM recién creada:

```
vserver show -vserver vserver_name
```

``Allowed Protocols`` El campo debe incluir NFS. 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 acceder a los datos en el espacio IP ipspaceA:

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

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

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: unix
              LDAP Client: -
              Default Volume Language Code: C.UTF-8
              Snapshot Policy: default
              Comment:
              Quota Policy: default
              List of Aggregates Assigned: -
              Limit on Maximum Number of Volumes allowed: unlimited
              Vserver Admin State: running
              Vserver Operational State: running
              Vserver Operational State Stopped Reason: -
              Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
              Disallowed Protocols: -
              QoS Policy Group: -
              Config Lock: false
              IPspace Name: ipspaceA
```

 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](#).

## Verificar la habilitación del protocolo NFS en ONTAP SVM

Antes de poder configurar y utilizar NFS 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 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 NFS:

```
vserver add-protocols -vserver vserver_name -protocols nfs
```

- 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    nfs                  cifs, fcp, iscsi, ndmp
```

El siguiente comando permite el acceso a través de NFS agregando `nfs` a la lista de protocolos habilitados en la SVM llamada VS1:

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

## Abrir el acceso del cliente NFS en ONTAP 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 NFS. Sin esta regla, se deniega el acceso a la SVM y a sus volúmenes a todos los clientes NFS.

### 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 el acceso está abierto a todos los clientes NFS de 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
-policynname default -instance

          Vserver: vs1.example.com
          Policy Name: default
          Rule Index: 1
          Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
          RO Access Rule: any
          RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
          Superuser Security Types: any
          Honor SetUID Bits in SETATTR: true
          Allow Creation of Devices: true
```

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 -policynname default
-ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any
-superuser any
```

Si la SVM solo contendrá volúmenes protegidos por Kerberos, puede establecer las opciones de la regla de exportación `-rorule`, `-rwrule` y `-superuser` para el volumen raíz en `krb5` o `krb5i`. Por ejemplo:

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

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

## Resultado

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

# Crear servidores NFS de ONTAP

Después de verificar que NFS tiene licencia en el clúster, puede utilizar `vserver nfs create` el comando para crear un servidor NFS en la SVM y especificar las versiones de

## NFS compatibles.

### Acerca de esta tarea

Es posible configurar SVM para que admita una o varias versiones de NFS. Si admite NFSv4 o posteriores:

- El nombre de dominio de asignación del ID de usuario de NFSv4 debe ser igual en el servidor NFSv4 y en los clientes de destino.

No necesariamente debe ser el mismo que un nombre de dominio LDAP o NIS siempre que el servidor NFSv4 y los clientes utilicen el mismo nombre.

- Los clientes de destino deben admitir la configuración de ID numérico de NFSv4.
- Por motivos de seguridad, debe utilizar LDAP para los servicios de nombres en las puestas en marcha de NFSv4.

### Antes de empezar

Debe haber configurado la SVM para permitir el protocolo NFS.

### Pasos

1. Compruebe que NFS tiene licencia en el clúster:

```
system license show -package nfs
```

Si no lo está, póngase en contacto con su representante de ventas.

2. Cree un servidor NFS:

```
vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0
{enabled|disabled} -v4-id-domain nfv4_id_domain -v4-numeric-ids
{enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
```

Puede optar por habilitar cualquier combinación de versiones de NFS. Si desea ser compatible con pNFS, debe habilitar las dos -v4.1 opciones y -v4.1-pnfs.

Si activa v4 o posterior, también debe estar seguro de que las siguientes opciones están configuradas correctamente:

- -v4-id-domain

Este parámetro opcional especifica la parte de dominio del formulario de cadena de nombres de usuario y de grupo, tal como lo define el protocolo NFSv4. De forma predeterminada, ONTAP utiliza el dominio NIS si se establece uno; si no es así, se utiliza el dominio DNS. Debe proporcionar un valor que coincida con el nombre de dominio utilizado por los clientes de destino.

- -v4-numeric-ids

Este parámetro opcional especifica si la compatibilidad con identificadores de cadena numéricos en los atributos de propietario de NFSv4 está habilitada. La configuración predeterminada está habilitada, pero debe verificar que los clientes de destino lo admitan.

Puede habilitar funciones adicionales de NFS más adelante con `vserver nfs modify` el comando.

3. Compruebe que NFS está ejecutando:

```
vserver nfs status -vserver vserver_name
```

4. Compruebe que NFS está configurado como se desea:

```
vserver nfs show -vserver vserver_name
```

## Ejemplos

El siguiente comando crea un servidor NFS en la SVM llamada vs1 con NFSv3 y NFSv4.0 habilitado:

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id  
-domain my_domain.com
```

Los siguientes comandos verifican el estado y los valores de configuración del nuevo servidor NFS llamado vs1:

```
vs1::> vserver nfs status -vserver vs1  
The NFS server is running on Vserver "vs1".  
  
vs1::> vserver nfs show -vserver vs1  
  
          Vserver: vs1  
          General NFS Access: true  
          NFS v3: enabled  
          NFS v4.0: enabled  
          UDP Protocol: enabled  
          TCP Protocol: enabled  
          Default Windows User: -  
          NFSv4.0 ACL Support: disabled  
          NFSv4.0 Read Delegation Support: disabled  
          NFSv4.0 Write Delegation Support: disabled  
          NFSv4 ID Mapping Domain: my_domain.com  
...
```

## Crear LIF de ONTAP NFS

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 utiliza la autenticación de Kerberos, habilite Kerberos en varias LIF.
- 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 capacity show` y `network interface capacity details show` 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.

A partir de la versión 9.4 de ONTAP, se admite FC-NVMe. Si crea una LIF FC-NVMe, debe tener en cuenta lo siguiente:

- El protocolo NVMe debe ser compatible con el adaptador de FC en el que se crea la LIF.
- FC-NVMe puede ser el único protocolo de datos en las LIF de datos.
- Debe configurarse un LIF que gestiona el tráfico de gestión para cada máquina virtual de almacenamiento (SVM) compatible con SAN.
- Las LIF y los espacios de nombres de NVMe deben alojarse en el mismo nodo.
- Solo se puede configurar una LIF NVMe que gestiona el tráfico de datos por SVM

#### Pasos

1. Cree una LIF:

```
network interface create -vserver vserver_name -lif lif_name -role data -data
-protocol nfs -home-node node_name -home-port port_name {-address IP_address
-netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
-revert {true|false}
```

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

Opción	Descripción
--------	-------------

<b>ONTAP 9.5 y anteriores</b>	<pre>'network interface create -vserver vserver_name -lif lif_name -role data -data-protocol nfs -home-node node_name -home-port port_name {-address IP_address -netmask IP_address</pre>
<code>-subnet-name subnet_name} -firewall-policy data -auto-revert {true</code>	<code>false}`</code>
<b>ONTAP 9.6 y posterior</b>	<pre>'network interface create -vserver vserver_name -lif lif_name -role data -data-protocol nfs -home-node node_name -home-port port_name {-address IP_address -netmask IP_address</pre>
<code>-subnet-name subnet_name} -firewall-policy data -auto-revert {true</code>	<code>false}`</code>

- `'-role`` No es necesario utilizar el parámetro cuando se crea una LIF mediante una política de servicio (a partir de ONTAP 9,6).
- `'-data-protocol`` El parámetro debe especificarse cuando se crea la LIF, y no se puede modificar posteriormente sin destruir ni volver a crear la LIF de datos.

`'-data-protocol`` No es necesario utilizar el parámetro cuando se crea una LIF mediante una política de servicio (empezando por ONTAP 9.6).

- `-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.

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

- `-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 red del entorno.
  - a. Compruebe que la LIF se ha creado correctamente mediante `network interface show` el comando.
  - b. 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>

- c. Si utiliza Kerberos, repita los pasos 1 a 3 para crear LIF adicionales.

Kerberos debe habilitarse por separado en cada uno de estos LIF.

## 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 nfs -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 nfs -home-node node-3 -home-port elc -subnet-name
cliente1_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	cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a
true					
node-1	clus1	up/up	192.0.2.12/24	node-1	e0a
true					
true	clus2	up/up	192.0.2.13/24	node-1	e0b
true					
node-2	mgmt1	up/up	192.0.2.68/24	node-1	e1a
true					
true	clus1	up/up	192.0.2.14/24	node-2	e0a
true					
true	clus2	up/up	192.0.2.15/24	node-2	e0b
true					
true	mgmt1	up/up	192.0.2.69/24	node-2	e1a
vs1.example.com	dataif1	up/down	192.0.2.145/30	node-1	e1c
true					
vs3.example.com	dataif3	up/up	192.0.2.146/30	node-2	e0c
true					
true	dataif4	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"](#)
- ["interfaz de red"](#)

# Habilitar DNS para la resolución de nombres de host de ONTAP NFS SVM

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.

## 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.

## 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
```

Name			
Vserver	State	Domains	Servers
cluster1	enabled	example.com	192.0.2.201, 192.0.2.202
vs1.example.com	enabled	example.com	192.0.2.201, 192.0.2.202

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
```

## Configure los servicios de nombres

### Obtenga más información sobre los servicios de nombres NFS de ONTAP

Según la configuración del sistema de almacenamiento, ONTAP debe poder buscar la información del host, usuario, grupo o grupo de red para proporcionar un acceso adecuado a los clientes. Es necesario configurar los servicios de nombres para permitir que ONTAP acceda a los servicios de nombres locales o externos para obtener esta información.

Debe utilizar un servicio de nombres como NIS o LDAP para facilitar las búsquedas de nombres durante la autenticación del cliente. Se recomienda utilizar LDAP siempre que sea posible para obtener una mayor seguridad, especialmente cuando se pone en marcha NFSv4 o posteriores. También debe configurar usuarios y grupos locales en caso de que los servidores de nombres externos no estén disponibles.

La información del servicio de nombres debe mantenerse sincronizada en todas las fuentes.

### Configurar la tabla de conmutación del servicio de nombres NFS de ONTAP

Debe configurar correctamente la tabla del conmutador del servicio de nombres para permitir que ONTAP consulte servicios de nombres locales o externos para recuperar información de asignación de hosts, usuarios, grupos, netgroup o nombres.

#### Antes de empezar

Debe haber decidido qué servicios de nombre desea utilizar para la asignación de host, usuario, grupo, netgroup o nombre según corresponda a su entorno.

Si planea utilizar netgroups, todas las direcciones IPv6 especificadas en netgroups deben acortarse y comprimirse según se especifica en RFC 5952.

### Acerca de esta tarea

No incluya fuentes de información que no se estén utilizando. Por ejemplo, si no se utiliza NIS en el entorno, no especifique la `-sources nis` opción.

### Pasos

1. Agregue las entradas necesarias a la tabla de cambio de servicio de nombres:

```
vserver services name-service ns-switch create -vserver vserver_name -database database_name -sources source_names
```

2. Compruebe que la tabla de cambio de servicio de nombres contiene las entradas esperadas en el orden deseado:

```
vserver services name-service ns-switch show -vserver vserver_name
```

Si desea realizar alguna corrección, debe usar `vserver services name-service ns-switch modify` `vserver services name-service ns-switch delete` los comandos o.

### Ejemplo

En el siguiente ejemplo se crea una entrada nueva en la tabla de switches del servicio de nombres para la SVM vs1 para utilizar el archivo de netgroup local y un servidor NIS externo para buscar información de netgroup en ese orden:

```
cluster::> vserver services name-service ns-switch create -vserver vs1 -database netgroup -sources files,nis
```

### Después de terminar

- Debe configurar los servicios de nombres que haya especificado para la SVM a fin de proporcionar acceso a los datos.
- Si elimina cualquier servicio de nombres para la SVM, también debe quitarlo de la tabla de switch de servicio de nombres.

Es posible que el acceso del cliente al sistema de almacenamiento no funcione como se espera, si no puede eliminar el servicio de nombres de la tabla de switches de servicio de nombres.

## Configurar usuarios y grupos UNIX locales

### Obtenga información sobre los usuarios y grupos locales de UNIX para SVM NFS de ONTAP

Se pueden usar usuarios y grupos UNIX locales en la SVM para fines de autenticación y asignaciones de nombres. Puede crear usuarios y grupos de UNIX manualmente, o bien cargar un archivo que contenga usuarios o grupos de UNIX a partir de un identificador de recursos (URI) uniforme.

Hay un límite máximo predeterminado de 32,768 grupos de usuarios UNIX locales y miembros de grupo combinados en el clúster. El administrador del clúster puede modificar este límite.

## Crear usuarios locales de UNIX en SVM NFS de ONTAP

Puede utilizar `vserver services name-service unix-user create` el comando para crear usuarios locales de UNIX. Un usuario UNIX local es un usuario de UNIX que se crea en la SVM como una opción de servicios de nombres UNIX que se va a utilizar en el procesamiento de asignaciones de nombres.

### Paso

1. Crear un usuario local de UNIX:

```
vserver services name-service unix-user create -vserver vserver_name -user user_name -id integer -primary-gid integer -full-name full_name
```

`-user user_name` especifica el nombre de usuario. La longitud del nombre de usuario debe ser de 64 caracteres o menos.

`-id integer` Especifica el ID de usuario que se asigna.

`-primary-gid integer` Especifica el ID de grupo principal. Esto agrega el usuario al grupo principal. Después de crear el usuario, puede agregar manualmente el usuario a cualquier grupo adicional deseado.

### Ejemplo

El siguiente comando crea un usuario local de UNIX llamado `johnm` (nombre completo "John Miller") en la SVM llamada `vs1`. El usuario tiene el ID 123 y el ID 100 del grupo principal.

```
node::> vserver services name-service unix-user create -vserver vs1 -user johnm -id 123 -primary-gid 100 -full-name "John Miller"
```

## Cargar listas de usuarios locales de UNIX en SVM NFS de ONTAP

Como alternativa a la creación manual de usuarios UNIX locales individuales en SVM, puede simplificar la tarea cargando una lista de usuarios UNIX locales en SVM desde un identificador de recursos uniforme (URI) (`vserver services name-service unix-user load-from-uri`).

### Pasos

1. Cree un archivo que contenga la lista de usuarios UNIX locales que desee cargar.

El archivo debe contener información del usuario `/etc/passwd` en formato UNIX:

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

El comando descarta el valor `password` del campo y los valores de los campos después del `full_name` campo (`home_directory` y `shell`).

El tamaño máximo de archivo admitido es de 2.5 MB.

2. Compruebe que la lista no contiene ninguna información duplicada.

Si la lista contiene entradas duplicadas, se produce un error al cargar la lista.

3. Copie el archivo en un servidor.

El sistema de almacenamiento debe acceder al servidor a través de HTTP, HTTPS, FTP o FTPS.

4. Determine cuál es el URI del archivo.

El URI es la dirección que se proporciona al sistema de almacenamiento para indicar dónde se encuentra el archivo.

5. Cargue el archivo que contiene la lista de usuarios UNIX locales en SVM desde el URI:

```
vserver services name-service unix-user load-from-uri -vserver vserver_name  
-uri {ftp|http|ftps|https}://uri -overwrite {true|false}
```

`-overwrite {true|false}` especifica si se sobrescribirán las entradas. El valor predeterminado es `false`.

### Ejemplo

El siguiente comando carga una lista de usuarios UNIX locales del URI `ftp://ftp.example.com/passwd` en la SVM llamada VS1. Los usuarios existentes del SVM no se sobrescriben por información del URI.

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1  
-uri ftp://ftp.example.com/passwd -overwrite false
```

### Crear grupos UNIX locales en SVM NFS de ONTAP

Puede utilizar `vserver services name-service unix-group create` el comando para crear grupos UNIX locales a la SVM. Los grupos UNIX locales se utilizan con usuarios UNIX locales.

#### Paso

1. Crear un grupo UNIX local:

```
vserver services name-service unix-group create -vserver vserver_name -name  
group_name -id integer
```

`-name group_name` especifica el nombre del grupo. La longitud del nombre del grupo debe ser de 64 caracteres o menos.

`-id integer` Especifica el ID de grupo que asigna.

### Ejemplo

El siguiente comando crea un grupo local llamado eng en la SVM llamada vs1. El grupo tiene el ID 101.

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name eng -id 101
```

## Agregar usuarios al grupo local de UNIX en SVM NFS de ONTAP

Puede utilizar `vserver services name-service unix-group adduser` el comando para agregar un usuario a un grupo UNIX complementario local a la SVM.

### Paso

1. Agregar un usuario a un grupo UNIX local:

```
vserver services name-service unix-group adduser -vserver vserver_name -name group_name -username user_name
```

`-name group_name` Especifica el nombre del grupo UNIX al que se agregará el usuario además del grupo primario del usuario.

### Ejemplo

El siguiente comando agrega un usuario llamado max a un grupo UNIX local llamado eng en la SVM llamada vs1:

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name eng -username max
```

## Cargar grupos UNIX locales desde URI en SVM NFS de ONTAP

Como alternativa a la creación manual de grupos UNIX locales individuales, puede cargar una lista de grupos UNIX locales en SVM desde un identificador de recursos uniforme (URI) mediante el `vserver services name-service unix-group load-from-uri` comando.

### Pasos

1. Cree un archivo que contenga la lista de grupos UNIX locales que desee cargar.

El archivo debe contener información del grupo en `/etc/group` formato UNIX:

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

El comando descarta el valor `password` del campo.

El tamaño máximo de archivo admitido es de 1 MB.

La longitud máxima de cada línea del archivo de grupo es de 32,768 caracteres.

2. Compruebe que la lista no contiene ninguna información duplicada.

La lista no debe contener entradas duplicadas o, de lo contrario, se producirá un error al cargar la lista. Si

ya hay entradas presentes en la SVM, debe configurar `-overwrite` el parámetro para `true` que sobrescriba todas las entradas existentes con el nuevo archivo o asegurarse de que el nuevo archivo no contenga ninguna entrada que duplique las entradas existentes.

### 3. Copie el archivo en un servidor.

El sistema de almacenamiento debe acceder al servidor a través de HTTP, HTTPS, FTP o FTPS.

### 4. Determine cuál es el URI del archivo.

El URI es la dirección que se proporciona al sistema de almacenamiento para indicar dónde se encuentra el archivo.

### 5. Cargue el archivo que contiene la lista de grupos UNIX locales en la SVM desde el URI:

```
vserver services name-service unix-group load-from-uri -vserver vserver_name  
-uri {ftp|http|ftps|https}://uri -overwrite {true|false}
```

`-overwrite true|false` especifica si se sobrescribirán las entradas. El valor predeterminado es `false`. Si especifica este parámetro como `true`, ONTAP reemplaza toda la base de datos de grupo UNIX local existente de la SVM especificada por las entradas del archivo que está cargando.

#### Ejemplo

El siguiente comando carga una lista de grupos UNIX locales del URI `ftp://ftp.example.com/group` en la SVM llamada VS1. Los grupos existentes de la SVM no se sobrescriben por información del URI.

```
vsl:::> vserver services name-service unix-group load-from-uri -vserver vs1  
-uri ftp://ftp.example.com/group -overwrite false
```

## Trabajar con netgroups

### Obtenga información sobre los grupos de redes en las SVM NFS de ONTAP

Puede utilizar netgroups para la autenticación de usuarios y para que coincida con los clientes en las reglas de directiva de exportación. Puede proporcionar acceso a netgroups desde servidores de nombres externos (LDAP o NIS), o puede cargar netgroups desde un identificador de recursos uniforme (URI) en SVM mediante el `vserver services name-service netgroup load` comando.

#### Antes de empezar

Antes de trabajar con netgroups, debe asegurarse de que se cumplen las siguientes condiciones:

- Todos los hosts de los grupos de red, independientemente del origen (NIS, LDAP o archivos locales), deben tener registros DNS tanto de reenvío (A) como de retroceso (PTR) para proporcionar búsquedas DNS de reenvío e inversa coherentes.

Además, si una dirección IP de un cliente tiene varios registros PTR, todos esos nombres de host deben ser miembros del netgroup y tener registros Correspondientes.

- Los nombres de todos los hosts de netgroups, independientemente de su origen (NIS, LDAP o archivos

locales), deben estar escritos correctamente y utilizar el caso correcto. Las incoherencias de los casos en los nombres de host utilizados en los grupos de redes pueden dar lugar a un comportamiento inesperado, como las comprobaciones de exportación fallidas.

- Todas las direcciones IPv6 especificadas en los grupos de red deben acortarse y comprimirse como se especifica en RFC 5952.

Por ejemplo, 2011:hu9:0:0:0:0:3:1 debe acortarse a 2011:hu9::3:1.

### **Acerca de esta tarea**

Al trabajar con netgroups, puede realizar las siguientes operaciones:

- Puede utilizar el `vserver export-policy netgroup check-membership` comando para ayudar a determinar si una IP de cliente es miembro de un determinado grupo de red.
- Puede utilizar el `vserver services name-service getxxbyyy netgrp` comando para comprobar si un cliente forma parte de un grupo de red.

El servicio subyacente para realizar la búsqueda se selecciona según el orden de cambio de servicio de nombres configurado.

### **Cargar grupos de redes desde URI en SVM NFS de ONTAP**

Uno de los métodos que se pueden utilizar para hacer coincidir clientes en las reglas de directiva de exportación es utilizando los hosts enumerados en netgroups. Puede cargar netgroups desde un identificador de recursos uniforme (URI) en SVM como alternativa al uso de netgroups almacenados en servidores de nombres externos (`vserver services name-service netgroup load`).

### **Antes de empezar**

Los archivos de grupos de red deben cumplir los siguientes requisitos antes de cargarlos en una SVM:

- El archivo debe utilizar el mismo formato de archivo de texto de netgroup adecuado que se utiliza para llenar NIS.

ONTAP comprueba el formato del archivo de texto del grupo de red antes de cargarlo. Si el archivo contiene errores, no se cargará y se mostrará un mensaje que indique las correcciones que debe realizar en el archivo. Después de corregir los errores, puede volver a cargar el archivo netgroup en la SVM especificada.

- Los caracteres alfabéticos en los nombres de host del archivo netgroup deben ser en minúscula.
- El tamaño máximo de archivo admitido es de 5 MB.
- El nivel máximo admitido para los grupos de red de anidamiento es 1000.
- Sólo se pueden utilizar nombres de host DNS primarios al definir nombres de host en el archivo de grupo de red.

Para evitar problemas de acceso a la exportación, los nombres de host no deben definirse mediante registros CNAME o round robin de DNS.

- Las porciones de triples del usuario y del dominio en el archivo de netgroup deben mantenerse vacías porque ONTAP no las admite.

Solo se admite la parte host/IP.

### Acerca de esta tarea

ONTAP admite búsquedas netgroup-by-host para el archivo de netgroup local. Después de cargar el archivo netgroup, ONTAP crea automáticamente un mapa netgroup.byhost para habilitar búsquedas netgroup-by-host. Esto puede acelerar significativamente las búsquedas de grupos de red locales al procesar reglas de políticas de exportación para evaluar el acceso de los clientes.

### Paso

1. Cargue los grupos de redes en SVM desde un URI:

```
vserver services name-service netgroup load -vserver vserver_name -source  
{ftp|http|ftps|https}://uri
```

La carga del archivo de netgroup y la creación del mapa netgroup.byhost pueden tardar varios minutos.

Si desea actualizar los grupos de red, puede editar el archivo y cargar el archivo de netgroup actualizado en la SVM.

### Ejemplo

El siguiente comando carga las definiciones de netgroup en la SVM llamada VS1 desde la URL HTTP <http://intranet/downloads/corp-netgroup>:

```
vs1::> vserver services name-service netgroup load -vserver vs1  
-source http://intranet/downloads/corp-netgroup
```

### Verificar las definiciones de grupos de redes SVM de ONTAP NFS

Después de cargar netgroups en la SVM, puede utilizar `vserver services name-service netgroup status` el comando para comprobar el estado de las definiciones de netgroup. Esto permite determinar si las definiciones de grupos de red son consistentes en todos los nodos que forman parte de la SVM.

### Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Compruebe el estado de las definiciones de netgroup:

```
vserver services name-service netgroup status
```

Puede visualizar información adicional en una vista más detallada.

3. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

### Ejemplo

Una vez establecido el nivel de privilegio, el siguiente comando muestra el estado de netgroup para todas las SVM:

```
vs1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when
        directed to do so by technical support.

Do you wish to continue? (y or n): y

vs1::*> vserver services name-service netgroup status
Virtual
Server      Node          Load Time      Hash Value
-----
-----
vs1
      node1          9/20/2006 16:04:53
e6cb38ec1396a280c0d2b77e3a84eda2
      node2          9/20/2006 16:06:26
e6cb38ec1396a280c0d2b77e3a84eda2
      node3          9/20/2006 16:08:08
e6cb38ec1396a280c0d2b77e3a84eda2
      node4          9/20/2006 16:11:33
e6cb38ec1396a280c0d2b77e3a84eda2
```

## Crear configuraciones de dominio NIS para SVM NFS de ONTAP

Si se utiliza un servicio de información de red (NIS) en el entorno para servicios de nombres, debe crear una configuración de dominio NIS para la SVM mediante `vserver services name-service nis-domain create` el comando.

### Antes de empezar

Todos los servidores NIS configurados deben estar disponibles y accesibles antes de configurar el dominio NIS en la SVM.

Si tiene previsto utilizar NIS para búsquedas en directorios, los mapas de sus servidores NIS no pueden tener más de 1,024 caracteres para cada entrada. No especifique el servidor NIS que no cumpla con este límite. De lo contrario, es posible que se produzca un error en el acceso del cliente que depende de las entradas NIS.

### Acerca de esta tarea

Si su base de datos NIS contiene un `netgroup.byhost` mapa, ONTAP puede utilizarlo para búsquedas más rápidas. Los `netgroup.byhost` netgroup mapas y del directorio se deben mantener sincronizados en todo momento para evitar problemas de acceso de los clientes. A partir de ONTAP 9.7, `netgroup.byhost` las entradas NIS se pueden almacenar en caché con los `vserver services name-service nis-domain netgroup-database` comandos.

No se admite el uso de NIS para la resolución del nombre de host.

## Pasos

### 1. Cree una configuración de dominio NIS:

```
vserver services name-service nis-domain create -vserver vs1 -domain <domain_name> -nis-servers <IP_addresses>
```

Puede especificar hasta 10 servidores NIS.



El **-nis-servers** campo reemplaza el **-servers** campo. Puedes utilizar el **-nis-servers** campo para especificar un nombre de host o una dirección IP para el servidor NIS.

### 2. Compruebe que se ha creado el dominio:

```
vserver services name-service nis-domain show
```

## Ejemplo

El siguiente comando crea una configuración de dominio NIS para un dominio NIS llamado en la SVM vs1 llamada nisdomain con un servidor NIS en la dirección IP 192.0.2.180 :

```
vs1::> vserver services name-service nis-domain create -vserver vs1 -domain nisdomain -nis-servers 192.0.2.180
```

## Utilice LDAP

### Obtenga información sobre el uso de servicios de nombres LDAP en SVM NFS de ONTAP

Si se utiliza LDAP en su entorno para servicios de nombre, debe trabajar con el administrador de LDAP para determinar los requisitos y las configuraciones del sistema de almacenamiento adecuadas, habilitar la SVM como cliente LDAP.

A partir de ONTAP 9.10.1, el enlace de canal LDAP se admite de forma predeterminada tanto para las conexiones LDAP de los servicios de nombres como de Active Directory. ONTAP intentará establecer la vinculación de canal con las conexiones LDAP solo si Start-TLS o LDAPS está habilitado junto con la seguridad de la sesión establecida en Sign o Seal. Para deshabilitar o volver a habilitar el enlace de canales LDAP con los servidores de nombres, utilice **-try-channel-binding** el parámetro con **ldap client modify** el comando.

Para obtener más información, consulte ["2020 requisitos de enlace de canal LDAP y firma LDAP para Windows"](#).

- Antes de configurar LDAP para ONTAP, debe verificar que la implementación del sitio cumple las prácticas recomendadas para la configuración del cliente y el servidor LDAP. En particular, deben cumplirse las siguientes condiciones:
  - El nombre de dominio del servidor LDAP debe coincidir con la entrada del cliente LDAP.
  - Los tipos hash de contraseña de usuario LDAP compatibles con el servidor LDAP deben incluir los compatibles con ONTAP:
    - CRIPTA (todos los tipos) y SHA-1 (SHA, SSHA).

- A partir de los valores hash de ONTAP 9.8, SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, También se admiten SSHA-384 y SSHA-512).
- Si el servidor LDAP requiere medidas de seguridad de la sesión, debe configurarlas en el cliente LDAP.

Están disponibles las siguientes opciones de seguridad de la sesión:

- La firma LDAP (proporciona comprobación de la integridad de los datos) y la firma y el sellado LDAP (proporciona cifrado y comprobación de la integridad de los datos).
- INICIE TLS
- LDAPS (LDAP sobre TLS o SSL)
- Para habilitar consultas LDAP firmadas y selladas, se deben configurar los siguientes servicios:
  - Los servidores LDAP deben ser compatibles con el mecanismo SASL GSSAPI (Kerberos).
  - Los servidores LDAP deben tener registros DNS A/AAAA, así como registros PTR configurados en el servidor DNS.
  - Los servidores Kerberos deben tener registros SRV presentes en el servidor DNS.
- Para habilitar el INICIO de TLS o LDAPS, se deben tener en cuenta los siguientes puntos.
  - Se trata de una práctica recomendada de NetApp para usar Start TLS en lugar de LDAPS.
  - Si se usa LDAPS, el servidor LDAP debe habilitar para TLS o SSL en ONTAP 9.5 y versiones posteriores. SSL no es compatible con ONTAP 9.0-9.4.
  - Ya debe configurarse un servidor de certificados en el dominio.
- Para habilitar la búsqueda de referencias LDAP (en ONTAP 9.5 y posterior), se deben cumplir las siguientes condiciones:
  - Ambos dominios deben configurarse con una de las siguientes relaciones de confianza:
    - Bidireccional
    - Unidireccional, donde la primaria confía en el dominio de referencia
    - Padre-hijo
  - El DNS debe configurarse de modo que resuelva todos los nombres de servidor a los que se hace referencia.
  - Las contraseñas de dominio deben coincidir para autenticarse cuando --bind-as-cifs-Server se establece en true.

Las siguientes configuraciones no son compatibles con la búsqueda de referencias LDAP.



- Para todas las versiones de ONTAP:
  - Clientes LDAP en una SVM de administrador
- Para ONTAP 9.8 y versiones anteriores (se admiten en la versión 9.9.1 y posteriores):
  - Firma y sellado LDAP ( ` -session-security` opción)
  - Conexiones TLS cifradas (la -use-start-tls opción)
  - Comunicaciones a través del puerto LDAPS 636 (la -use-ldaps-for-ad-ldap opción)
- Debe introducir un esquema de LDAP al configurar el cliente LDAP en la SVM.

En la mayoría de los casos, uno de los esquemas ONTAP predeterminados será apropiado. Sin embargo, si el esquema LDAP del entorno difiere de éste, debe crear un nuevo esquema de cliente LDAP para ONTAP antes de crear el cliente LDAP. Consulte a su administrador LDAP sobre los requisitos de su entorno.

- No se admite el uso de LDAP para la resolución del nombre de host.

#### Si quiere más información

- ["Informe técnico de NetApp 4835: Cómo configurar LDAP en ONTAP"](#)
- ["Instale los certificados de CA raíz autofirmados en la SVM SMB de ONTAP"](#)

#### Crear nuevos esquemas de cliente LDAP para SVM NFS de ONTAP

Si el esquema LDAP del entorno difiere de los valores predeterminados de ONTAP, debe crear un nuevo esquema de cliente LDAP para ONTAP antes de crear la configuración de cliente LDAP.

#### Acerca de esta tarea

La mayoría de los servidores LDAP pueden utilizar los esquemas predeterminados proporcionados por ONTAP:

- MS-AD-BIS (el esquema preferido para la mayoría de los servidores AD de Windows 2012 y posteriores)
- AD-IDMU (Windows 2008, Windows 2012 y servidores AD posteriores)
- AD-SFU (servidores Windows 2003 y anteriores de AD)
- RFC-2307 (SERVIDORES UNIX LDAP)

Si necesita utilizar un esquema LDAP no predeterminado, debe crearlo antes de crear la configuración del cliente LDAP. Consulte con el administrador LDAP antes de crear un nuevo esquema.

Los esquemas LDAP predeterminados proporcionados por ONTAP no se pueden modificar. Para crear un nuevo esquema, cree una copia y, a continuación, modifique la copia en consecuencia.

#### Pasos

1. Mostrar las plantillas de esquema de cliente LDAP existentes para identificar la que desea copiar:

```
vserver services name-service ldap client schema show
```

2. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

3. Haga una copia de un esquema de cliente LDAP existente:

```
vserver services name-service ldap client schema copy -vserver vserver_name  
-schema existing_schema_name -new-schema-name new_schema_name
```

4. Modifique el nuevo esquema y personalícelo para su entorno:

```
vserver services name-service ldap client schema modify
```

5. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

## Crear configuraciones de cliente LDAP para el acceso NFS de ONTAP

Si desea que ONTAP acceda a los servicios LDAP o Active Directory externos en el entorno, primero debe configurar un cliente LDAP en el sistema de almacenamiento.

### Antes de empezar

Uno de los tres primeros servidores de la lista de dominios resueltos de Active Directory debe estar activo y servir datos. De lo contrario, esta tarea falla.



Hay varios servidores, de los cuales más de dos servidores están inactivos en cualquier momento.

### Pasos

1. Consulte al administrador de LDAP para determinar los valores de configuración adecuados para `vserver services name-service ldap client create` el comando:

- a. Especifique una conexión basada en dominio o en dirección a los servidores LDAP.

``-ad-domain` ` -servers` Las opciones y se excluyen mutuamente.`

- Utilice `-ad-domain` la opción para habilitar la detección del servidor LDAP en el dominio de Active Directory.
  - Puede usar la `-restrict-discovery-to-site` opción para restringir la detección del servidor LDAP al sitio predeterminado de CIFS del dominio especificado. Si utiliza esta opción, también debe especificar el sitio predeterminado de CIFS con `-default-site`.
- Puede usar `-preferred-ad-servers` la opción para especificar uno o más servidores de Active Directory preferidos por dirección IP en una lista delimitada por comas. Después de crear el cliente, puede modificar esta lista mediante `vserver services name-service ldap client modify` el comando.
- Utilice `-servers` la opción para especificar uno o más servidores LDAP (Active Directory o UNIX) por dirección IP en una lista delimitada por comas.



opción está obsoleta. `-ldap-servers` El campo reemplaza el `-servers` campo. Este campo puede tomar un nombre de host o una dirección IP para el servidor LDAP.

- b. Especifique un esquema LDAP predeterminado o personalizado.

La mayoría de los servidores LDAP pueden utilizar los esquemas de sólo lectura predeterminados que proporciona ONTAP. Lo mejor es utilizar esos esquemas predeterminados a menos que haya un requisito para hacer lo contrario. Si es así, puede crear su propio esquema copiando un esquema predeterminado (son de sólo lectura) y modificando la copia.

Esquemas predeterminados:

- MS-AD-BIS

Basado en RFC-2307bis, este es el esquema LDAP preferido para la mayoría de implementaciones LDAP estándar de Windows 2012 y posteriores.

- **AD-IDMU**

Basado en Administración de identidades de Active Directory para UNIX, este esquema es apropiado para la mayoría de servidores AD de Windows 2008, Windows 2012 y posteriores.

- **AD-SFU**

Basado en los Servicios de Active Directory para UNIX, este esquema es apropiado para la mayoría de servidores de AD anteriores y Windows 2003.

- **RFC-2307**

Basado en RFC-2307 (*an Approach for using LDAP as a Network Information Service*), este esquema es apropiado para la mayoría de servidores UNIX AD.

c. Seleccione valores de enlace.

- `-min-bind-level {anonymous|simple|sasl}` especifica el nivel de autenticación de enlace mínimo.

El valor predeterminado es **anonymous**.

- `-bind-dn LDAP_DN` especifica el usuario de enlace.

Para los servidores de Active Directory, debe especificar el usuario en el formulario de cuenta (DOMINIO\usuario) o principal ([user@domain.com](mailto:user@domain.com)). De lo contrario, debe especificar el usuario en el formulario Nombre completo (CN=user,DC=domain,DC=com).

- `-bind-password password` especifica la contraseña de enlace.

d. Seleccione las opciones de seguridad de la sesión, si es necesario.

Puede habilitar la firma y el sellado LDAP o LDAP over TLS si lo requiere el servidor LDAP.

- `--session-security {none|sign|seal}`

Puede activar la firma (sign, integridad de datos), la firma y el sellado (seal, la integridad y el cifrado de los datos), o ninguno none, sin firma ni sellado). El valor predeterminado es none.

También debe definir `-min-bind-level {sasl}` a menos que desee que la autenticación de enlace se retroceda **anonymous** o **simple** si el enlace de firma y sellado falla.

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

Si se establece en **true** y el servidor LDAP lo admite, el cliente LDAP utiliza una conexión TLS cifrada con el servidor. El valor predeterminado es **false**. Debe instalar un certificado de CA raíz autofirmado del servidor LDAP para usar esta opción.



Si la máquina virtual de almacenamiento tiene un servidor SMB añadido a un dominio y el servidor LDAP es uno de los controladores de dominio del dominio inicial del servidor SMB, puede modificar la `-session-security-for-ad-ldap` opción mediante `vserver cifs security modify` el comando.

e. Seleccione los valores de puerto, consulta y base.

Se recomiendan los valores predeterminados, pero debe verificar con el administrador de LDAP que son adecuados para su entorno.

- `-port port` Especifica el puerto del servidor LDAP.

El valor predeterminado es 389.

Si tiene pensado utilizar Start TLS para proteger la conexión LDAP, debe utilizar el puerto predeterminado 389. Start TLS comienza como una conexión de texto sin formato sobre el puerto 389 predeterminado LDAP y esa conexión se actualiza a TLS. Si cambia el puerto, Start TLS falla.

- `-query-timeout integer` especifica el tiempo de espera de la consulta en segundos.

El intervalo permitido es de 1 a 10 segundos. El valor predeterminado es 3 segundos.

- `-base-dn LDAP_DN` Especifica el DN base.

Se pueden introducir varios valores si es necesario (por ejemplo, si la búsqueda de referencias LDAP está activada). El valor predeterminado es "" (root).

- `-base-scope {base|onelevel|subtree}` especifica el ámbito de búsqueda base.

El valor predeterminado es subtree.

- `-referral-enabled {true|false}` Especifica si el seguimiento de referencias LDAP está activado.

A partir de ONTAP 9.5, esto permite al cliente LDAP de ONTAP remitir solicitudes de búsqueda a otros servidores LDAP si el servidor LDAP principal devuelve una respuesta de referencia LDAP que indica que los registros deseados están presentes en los servidores LDAP remitidos. El valor predeterminado es **false**.

Para buscar registros presentes en los servidores LDAP a los que se hace referencia, se debe agregar la base-dn de los registros referidos a la base-dn como parte de la configuración del cliente LDAP.

2. Cree una configuración de cliente LDAP en la máquina virtual de almacenamiento:

```
vserver services name-service ldap client create -vserver vserver_name -client -config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain} -preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site {true|false} -default-site CIFS_default_site -schema schema -port 389 -query -timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind -password password -base-dn LDAP_DN -base-scope subtree -session-security {none|sign|seal} [-referral-enabled {true|false}]
```



Debe proporcionar el nombre de la máquina virtual de almacenamiento al crear una configuración de cliente LDAP.

### 3. Compruebe que la configuración del cliente LDAP se ha creado correctamente:

```
vserver services name-service ldap client show -client-config  
client_config_name
```

#### Ejemplos

El siguiente comando crea una nueva configuración de cliente LDAP llamada `ldap1` para que la máquina virtual de almacenamiento VS1 funcione con un servidor de Active Directory para LDAP:

```
cluster1::> vserver services name-service ldap client create -vserver vs1  
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU  
-port 389 -query-timeout 3 -min-bind-level simple -base-dn  
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers  
172.17.32.100
```

El siguiente comando crea una nueva configuración de cliente LDAP denominada `ldap1` para la máquina virtual de almacenamiento VS1 con el fin de funcionar con un servidor de Active Directory para LDAP en el que se requiere firma y sellado, y la detección del servidor LDAP está restringida a un sitio determinado para el dominio especificado:

```
cluster1::> vserver services name-service ldap client create -vserver vs1  
-client-config ldapclient1 -ad-domain addomain.example.com -restrict  
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU  
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn  
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers  
172.17.32.100 -session-security seal
```

El siguiente comando crea una nueva configuración de cliente LDAP denominada `ldap1` para que la máquina virtual de almacenamiento VS1 funcione con un servidor de Active Directory para LDAP en el que se requiere la búsqueda de referencias de LDAP:

```
cluster1::> vserver services name-service ldap client create -vserver vs1  
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU  
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn  
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"  
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled  
true
```

El siguiente comando modifica la configuración de cliente LDAP llamada `ldap1` para la máquina virtual de almacenamiento VS1 especificando el DN base:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1  
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

El siguiente comando modifica la configuración de cliente LDAP denominada `ldap1` para la máquina virtual de almacenamiento `VS1` habilitando la búsqueda de referencias:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1  
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;  
DC=adrefdomain,DC=example2,DC=com" -referral-enabled true
```

## Asociar configuraciones de cliente LDAP con SVM NFS de ONTAP

Para habilitar LDAP en una SVM, debe usar `vserver services name-service ldap create` el comando para asociar una configuración de cliente LDAP con la SVM.

### Antes de empezar

- Debe haber un dominio de LDAP dentro de la red y estar accesible para el clúster en el que está ubicada la SVM.
- Debe haber una configuración de cliente LDAP en la SVM.

### Pasos

1. Habilite LDAP en la SVM:

```
vserver services name-service ldap create -vserver vserver_name -client-config  
client_config_name
```



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

El siguiente comando habilita LDAP en el SVM "vs1" SVM y lo configura para utilizar la configuración del cliente LDAP "ldap1":

```
cluster1::> vserver services name-service ldap create -vserver vs1  
-client-config ldap1 -client-enabled true
```

2. Validar el estado de los servidores de nombres mediante el comando `vserver Services NAME-service ldap check`.

El siguiente comando valida los servidores LDAP en la SVM VS1.

```
cluster1::> vserver services name-service ldap check -vserver vs1

| Vserver: vs1
| Client Configuration Name: c1
| LDAP Status: up
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".
```

## Verificar fuentes LDAP para SVM NFS de ONTAP

Debe comprobar que los orígenes LDAP para servicios de nombres figuran correctamente en la tabla de switches de servicio de nombres para la SVM.

### Pasos

1. Mostrar el contenido de la tabla de cambio de servicio de nombres actual:

```
vserver services name-service ns-switch show -vserver svm_name
```

El siguiente comando muestra los resultados de la SVM My\_SVM:

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
                                         Source
Vserver          Database      Order
-----
My_SVM          hosts        files,
                           dns
My_SVM          group        files,ldap
My_SVM          passwd       files,ldap
My_SVM          netgroup     files
My_SVM          namemap     files
5 entries were displayed.
```

namemap especifica los orígenes para buscar información de asignación de nombres y en qué orden. En un entorno únicamente UNIX, esta entrada no es necesaria. La asignación de nombres sólo es necesaria en un entorno mixto que utilice UNIX y Windows.

2. Actualice la ns-switch entrada según corresponda:

Si desea actualizar la entrada del interruptor ns para...	Introduzca el comando...
Información del usuario	<pre>vserver services name-service ns- switch modify -vserver <i>vserver_name</i> -database passwd -sources ldap,files</pre>

Si desea actualizar la entrada del interruptor ns para...	Introduzca el comando...
Información de grupo	vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files
Información de netgroup	vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files

## Utilice Kerberos con NFS para una mayor seguridad

### Obtenga información sobre el uso de Kerberos con ONTAP NFS para la autenticación de seguridad

Si se utiliza Kerberos en su entorno para autenticación segura, debe trabajar con el administrador de Kerberos para determinar requisitos y configuraciones del sistema de almacenamiento apropiadas y, a continuación, habilitar la SVM como cliente Kerberos.

Su entorno debe cumplir las siguientes directrices:

- La implementación de su sitio debe seguir las prácticas recomendadas para la configuración del servidor Kerberos y del cliente antes de configurar Kerberos para ONTAP.
- Si es posible, utilice NFSv4 o posteriores si es necesaria la autenticación de Kerberos.

NFSv3 se puede utilizar con Kerberos. Sin embargo, todas las ventajas de seguridad de Kerberos solo se materializan en puestas en marcha de ONTAP de NFSv4 o posteriores.

- Para promover el acceso redundante al servidor, se debe habilitar Kerberos en varias LIF de datos en varios nodos del clúster mediante el mismo SPN.
- Cuando se habilita Kerberos en la SVM, debe especificarse uno de los siguientes métodos de seguridad en las reglas de exportación para volúmenes o qtrees en función de la configuración del cliente NFS.
  - krb5 (Protocolo Kerberos v5)
  - krb5i (Protocolo Kerberos v5 con comprobación de integridad con sumas de comprobación)
  - krb5p (Protocolo Kerberos v5 con servicio de privacidad)

Además del servidor Kerberos y los clientes, para ONTAP se deben configurar los siguientes servicios externos con el fin de admitir Kerberos:

- Servicio de directorio

Debe utilizar un servicio de directorio seguro en su entorno, como Active Directory u OpenLDAP, que esté configurado para usar LDAP sobre SSL/TLS. No utilice NIS, cuyas solicitudes se envían en texto claro y, por lo tanto, no son seguras.

- NTP

Debe tener un servidor de tiempo de trabajo que ejecute NTP. Esto es necesario para evitar errores de autenticación de Kerberos debido a una desviación de tiempo.

- Resolución de nombres de dominio (DNS)

Cada cliente UNIX y cada LIF de SVM deben tener un registro de servicio (SRV) adecuado registrado con el KDC en zonas de búsqueda inversa y de reenvío. Todos los participantes deben poder resolverse correctamente a través de DNS.

## Verificar los permisos de UNIX para las configuraciones NFS Kerberos en las SVM de ONTAP

Kerberos requiere que se establezcan determinados permisos de UNIX para el volumen raíz de la SVM y para los usuarios y grupos locales.

### Pasos

1. Visualice los permisos relevantes en el volumen raíz de la SVM:

```
volume show -volume root_vol_name-fields user,group,unix-permissions
```

El volumen raíz de la SVM debe tener la siguiente configuración:

Nombre...	Estableciendo...
UID	Raíz o ID 0
GID	Raíz o ID 0
Permisos de UNIX	755

Si no se muestran estos valores, utilice `volume modify` el comando para actualizarlos.

2. Mostrar los usuarios UNIX locales:

```
vserver services name-service unix-user show -vserver vserver_name
```

La SVM debe tener configurados los siguientes usuarios de UNIX:

Nombre de usuario	ID de usuario	ID del grupo principal	Comentar
nfs	500	0	<p>Necesario para la fase DE INICIALIZACIÓN de GSS.</p> <p>El primer componente del SPN de usuario del cliente NFS se utiliza como usuario.</p> <p>El usuario nfs no es necesario si existe una asignación de nombre Kerberos-UNIX para el SPN del usuario cliente NFS.</p>
raíz	0	0	Necesario para el montaje.

Si no se muestran estos valores, puede usar `vserver services name-service unix-user modify` el comando para actualizarlos.

### 3. Mostrar los grupos UNIX locales:

```
vserver services name-service unix-group show -vserver vserver _name
```

La SVM debe tener configurados los siguientes grupos UNIX:

Nombre del grupo	ID de grupo
daemon	1
raíz	0

Si no se muestran estos valores, puede usar `vserver services name-service unix-group modify` el comando para actualizarlos.

## Crear configuraciones de dominio Kerberos de NFS en SVM de ONTAP

Si desea que ONTAP acceda a servidores Kerberos externos en su entorno, primero debe configurar la SVM para que utilice un Reino de Kerberos existente. Para ello, debe recopilar valores de configuración para el servidor KDC de Kerberos y, a continuación, utilizar el `vserver nfs kerberos realm create` comando para crear la configuración del dominio de Kerberos en una SVM.

### Antes de empezar

El administrador del clúster debe haber configurado NTP en el sistema de almacenamiento, el cliente y el servidor KDC para evitar problemas de autenticación. Las diferencias de tiempo entre un cliente y un servidor

(desfase de reloj) son una causa común de fallos de autenticación.

## Pasos

1. Consulte con su administrador de Kerberos para determinar los valores de configuración adecuados que se deben proporcionar con el vserver nfs kerberos realm create comando.
2. Cree una configuración de dominio de Kerberos en la SVM:

```
vserver nfs kerberos realm create -vserver vserver_name -realm realm_name  
{AD_KDC_server_values |AD_KDC_server_values} -comment "text"
```

3. Compruebe que la configuración de dominio Kerberos se ha creado correctamente:

```
vserver nfs kerberos realm show
```

## Ejemplos

El siguiente comando crea una configuración de dominio Kerberos para NFS para la SVM vs1 que utiliza un servidor de Microsoft Active Directory como servidor KDC. El dominio Kerberos es AUTH.EXAMPLE.COM. El servidor de Active Directory se denomina ad-1 y su dirección IP es 10.10.8.14. La desviación del reloj permitida es de 300 segundos (valor predeterminado). La dirección IP del servidor KDC es 10.10.8.14 y su número de puerto es 88 (el valor predeterminado). "Microsoft Kerberos config" es el comentario.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm  
AUTH.EXAMPLE.COM -adserver-name ad-1  
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88  
-kdc-vendor Microsoft  
-comment "Microsoft Kerberos config"
```

El siguiente comando crea una configuración de dominio de Kerberos para NFS para la SVM vs1 que utiliza un MIT KDC. El dominio Kerberos es SECURITY.EXAMPLE.COM. La desviación del reloj permitida es de 300 segundos. La dirección IP del servidor KDC es 10.10.9.1 y su número de puerto es 88. El proveedor de KDC es otro que indica un proveedor de UNIX. La dirección IP del servidor de administración es 10.10.9.1 y su número de puerto es 749 (el valor predeterminado). La dirección IP del servidor de contraseñas es 10.10.9.1 y su número de puerto es 464 (el valor predeterminado). "UNIX Kerberos config" es el comentario.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm  
SECURITY.EXAMPLE.COM. -clock-skew 300  
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1  
-adminserver-port 749  
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX  
Kerberos config"
```

## Configurar los tipos de cifrado permitidos por NFS Kerberos para las SVM de ONTAP

De forma predeterminada, ONTAP admite los siguientes tipos de cifrado para NFS Kerberos: DES, 3DES, AES-128 y AES-256. Puede configurar los tipos de cifrado permitidos para cada SVM de modo que se adapten a los requisitos de seguridad de su

entorno en particular mediante `vserver nfs modify` el comando con el `-permitted-enc-types` parámetro.

#### Acerca de esta tarea

Para obtener la mayor compatibilidad del cliente, ONTAP admite de forma predeterminada tanto el cifrado des débil como el AES sólido. Esto significa, por ejemplo, que si desea aumentar la seguridad y su entorno lo admite, puede utilizar este procedimiento para deshabilitar DES y 3DES y requerir que los clientes utilicen sólo el cifrado AES.

Debería utilizar el cifrado más potente disponible. Para ONTAP, esto es AES-256. Debe confirmar con el administrador de KDC que este nivel de cifrado es compatible con su entorno.

- Habilitar o deshabilitar completamente AES (tanto AES-128 como AES-256) en las SVM es disruptivo porque destruye el archivo ORIGINAL DE DES principal/keytab, lo que requiere que se deshabilite la configuración de Kerberos en todos los LIF para la SVM.

Antes de realizar este cambio, debe comprobar que los clientes NFS no utilizan el cifrado AES en la SVM.

- La habilitación o deshabilitación DE DES o 3DES no requiere ningún cambio en la configuración de Kerberos en las LIF.

#### Paso

1. Habilite o deshabilite el tipo de cifrado permitido que desee:

Si desea habilitar o deshabilitar...	Siga estos pasos...
DES o 3DES	<ol style="list-style-type: none"><li>Configure los tipos de cifrado permitidos por Kerberos NFS de la SVM: <code>vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types</code> Separe varios tipos de cifrado con una coma.</li><li>Compruebe que el cambio se ha realizado correctamente: <code>vserver nfs show -vserver vserver_name -fields permitted-enc-types</code></li></ol>

Si desea habilitar o deshabilitar...	Siga estos pasos...
AES-128 o AES-256	<p>a. Identifique en qué SVM y LIF Kerberos se han habilitado:</p> <pre>vserver nfs kerberos interface show</pre> <p>b. Deshabilite Kerberos en todas las LIF de la SVM cuyo Kerberos NFS permitió el tipo de cifrado que desee modificar:</p> <pre>vserver nfs kerberos interface disable -lif <i>lif_name</i></pre> <p>c. Configure los tipos de cifrado permitidos por Kerberos NFS de la SVM:</p> <pre>vserver nfs modify -vserver <i>vserver_name</i> -permitted-enc-types <i>encryption_types</i></pre> <p>Separé varios tipos de cifrado con una coma.</p> <p>d. Compruebe que el cambio se ha realizado correctamente:</p> <pre>vserver nfs show -vserver <i>vserver_name</i> -fields permitted-enc-types</pre> <p>e. Vuelva a habilitar Kerberos en todas las LIF en la SVM:</p> <pre>vserver nfs kerberos interface enable -lif <i>lif_name</i> -spn <i>service_principal_name</i></pre> <p>f. Compruebe que Kerberos está habilitado en todas las LIF:</p> <pre>vserver nfs kerberos interface show</pre>

## Habilitar NFS Kerberos en LIF de ONTAP

Puede usar `vserver nfs kerberos interface enable` el comando para habilitar Kerberos en una LIF de datos. Esto permite que la SVM utilice servicios de seguridad Kerberos para NFS.

### Acerca de esta tarea

Si utiliza un KDC de Active Directory, los primeros 15 caracteres de los SPN utilizados deben ser únicos entre las SVM dentro de un dominio o dominio.

### Pasos

1. Cree la configuración de Kerberos NFS:

```
vserver nfs kerberos interface enable -vserver vserver_name -lif logical_interface -spn service_principal_name
```

ONTAP requiere la clave secreta del SPN desde el KDC para habilitar la interfaz Kerberos.

Para los KDC de Microsoft, se contacta con el KDC y se emite un mensaje de nombre de usuario y contraseña en la CLI para obtener la clave secreta. Si necesita crear el SPN en una OU diferente del dominio Kerberos, puede especificar el `-ou` parámetro opcional.

Para los KDC que no son de Microsoft, la clave secreta se puede obtener utilizando uno de los dos métodos:

Si...	También debe incluir el siguiente parámetro con el comando...
Tenga las credenciales de administrador de KDC para recuperar la clave directamente desde el KDC	<code>-admin-username kdc_admin_username</code>
No tiene las credenciales de administrador de KDC, pero tiene un archivo keytab del KDC que contiene la clave	<code>-keytab-uri {ftp}</code>

2. Compruebe que Kerberos estaba habilitado en la LIF:

```
vserver nfs kerberos-config show
```

3. Repita los pasos 1 y 2 para habilitar Kerberos en varios LIF.

### Ejemplo

El siguiente comando crea y verifica una configuración Kerberos de NFS para la SVM denominada vs1 en la interfaz lógica ves03-d1, con el SPN nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM en la OU lab2ou:

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
Logical
Vserver Interface Address          Kerberos   SPN
-----  -----  -----
vs0      ves01-a1                10.10.10.30  disabled  -
vs2      ves01-d1                10.10.10.40  enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

## Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Impreso 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.