Configure los servicios de nombres

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

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.

```
vs1::> 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 rellenar 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` El 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). 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` El 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	`vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files`

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`