Configurar NFS

ONTAP 9

NetApp
January 08, 2026

Tabla de contenidos

Configurar NFS

Obtenga información sobre la configuración de NFS con la CLI de ONTAP

Puede usar comandos de la CLI de ONTAP 9 para configurar el acceso del cliente de NFS a los archivos ubicados en un volumen o un qtree de una máquina virtual de almacenamiento (SVM) nueva o existente.

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

- Desea utilizar cualquier versión de NFS compatible actualmente con ONTAP: NFSv3, NFSv4, NFSv4.1, NFSv4.2 o NFSv4.1 con pNFS.
- Desea usar la interfaz de línea de comandos (CLI), no System Manager ni una herramienta de secuencias de comandos automatizadas.

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

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

  Obtenga más información sobre la sintaxis de comandos en el "Referencia de comandos del ONTAP".

- Se utilizarán permisos de archivo UNIX para proteger el nuevo volumen.
- Tiene privilegios de administrador de clúster, no de administrador de SVM.

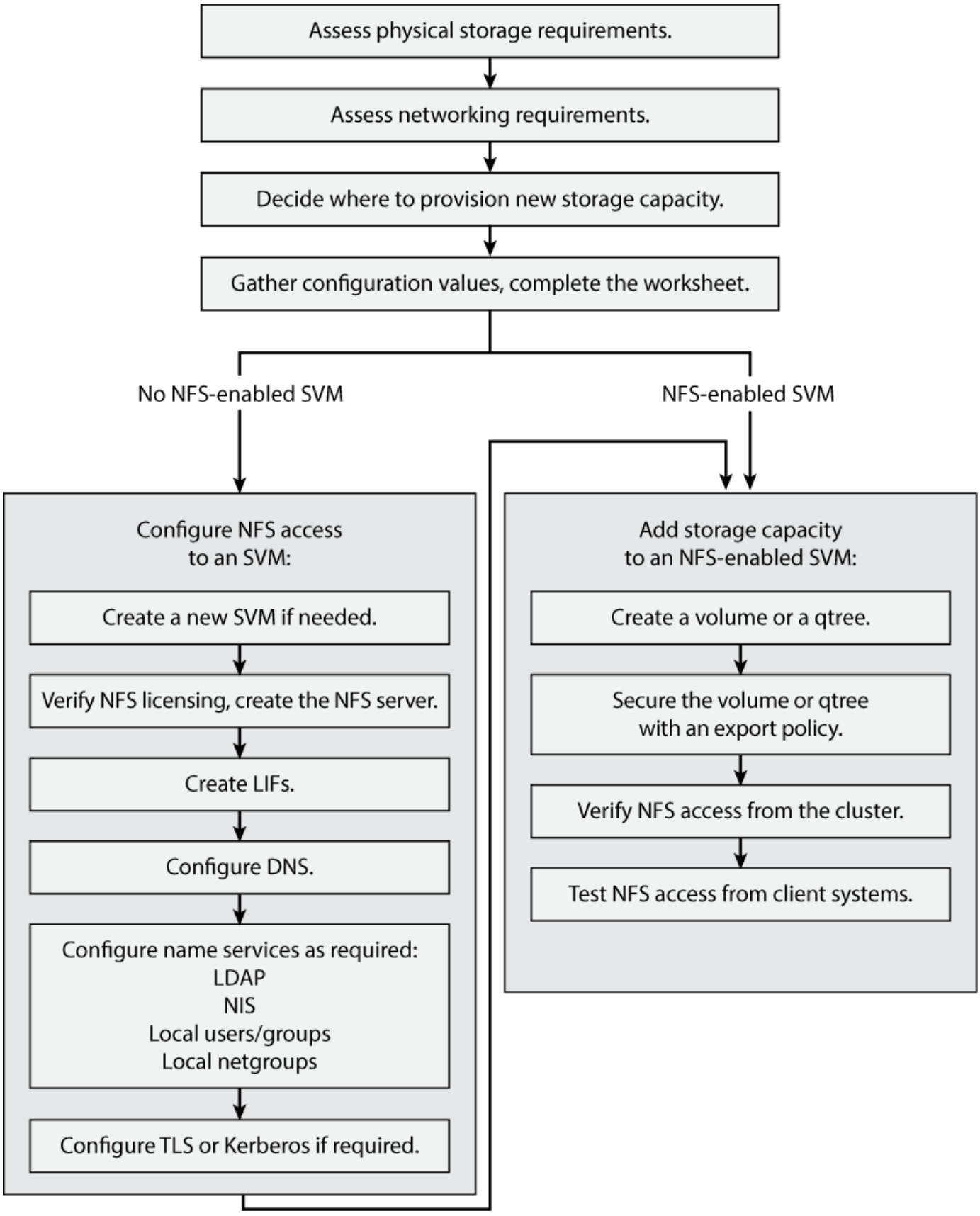
Si desea obtener más información sobre la gama de capacidades del protocolo NFS de ONTAP, consulte la "Obtenga información sobre el acceso a archivos ONTAP para el protocolo NFS".

Otras maneras de hacerlo en ONTAP

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

Obtenga más información sobre el flujo de trabajo de configuración de NFS de ONTAP

La configuración de NFS implica la evaluación de los requisitos de almacenamiento físico y de red, y la selección de un flujo de trabajo específico para el objetivo; entre otras, la configuración del acceso NFS a una SVM nueva o existente, o la adición de un volumen o un qtree a una SVM existente que ya esté completamente configurada para el acceso NFS.



Preparación

Evaluar los requisitos de almacenamiento físico de ONTAP NFS

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

Pasos

1. Mostrar el espacio disponible en los agregados existentes:

   `storage aggregate show`

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

   ```
   cluster::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
   --------- -------- --------- ----- ------- ------ ------ -----------
   aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                             normal
   aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                             normal
   6 entries were displayed.
   ```

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

Información relacionada

- "Añadir discos a un nivel local (agregado)"
- "agregado de almacenamiento, agregar discos"
- "creación de agregados de almacenamiento"

Evaluar los requisitos de configuración de la red NFS de ONTAP

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

Antes de empezar

Deben configurarse los siguientes objetos de red de clúster:

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

Pasos

1. Mostrar los puertos físicos y virtuales disponibles:

   `network port show`

   - Cuando sea posible, debe utilizar el puerto con la velocidad más alta para la red de datos.
   - Todos los componentes de la red de datos deben tener la misma configuración de MTU para obtener el mejor rendimiento.
   - Obtenga más información sobre `network port show` en el "Referencia de comandos del ONTAP".

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

   `network subnet show`

   Obtenga más información sobre `network subnet show` en el "Referencia de comandos del ONTAP".

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

   Obtenga más información sobre `network subnet create` en el "Referencia de comandos del ONTAP".

3. Mostrar espacios IP disponibles:

   `network ipspace show`

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

   Obtenga más información sobre `network ipspace show` en el "Referencia de comandos del ONTAP".

4. Si desea usar direcciones IPv6, compruebe que IPv6 esté habilitado en el clúster:

   `network options ipv6 show`

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

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

Obtenga más información sobre el aprovisionamiento de capacidad de almacenamiento NFS de ONTAP

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

Opciones

- Si desea aprovisionar un volumen o qtree en una SVM nueva o en una SVM existente con NFS habilitado pero no configurado, complete los pasos de "Configuración del acceso NFS a una SVM" y "adición de almacenamiento NFS a una SVM habilitada para NFS".

  Configure el acceso de NFS a una SVM

  Añada almacenamiento NFS a una SVM habilitada para NFS

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

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

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

- Si desea aprovisionar un volumen o un qtree en una SVM existente que esté completamente configurada para el acceso NFS, complete los pasos descritos en "Cómo añadir almacenamiento NFS a una SVM habilitada para NFS".

  Adición de almacenamiento NFS a una SVM habilitada para NFS

Hoja de datos de configuración de NFS de ONTAP

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

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

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

- Configurar el acceso de NFS a una SVM
- Se añade capacidad de almacenamiento a una SVM habilitada para NFS

Si va a añadir capacidad de almacenamiento a una SVM habilitada para NFS, solo debe completar:

- Se añade capacidad de almacenamiento a una SVM habilitada para NFS

Configure el acceso de NFS a una SVM

Parámetros para crear una SVM

Debe proporcionar estos valores con `vserver create` el comando si va a crear una SVM nueva.

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

Parámetros para crear un servidor NFS

Debe proporcionar estos valores con el `vserver nfs create` comando al crear un nuevo servidor NFS y especificar versiones NFS compatibles.

Si habilita NFSv4 o posterior, debe utilizar LDAP para mejorar la seguridad.

Campo	Descripción	Su valor

`-v3`, `-v4.0`, `-v4.1`, , `-v4.1 -pnfs`	Habilite las versiones de NFS según sea necesario. v4,2 también es compatible con ONTAP 9.8 y posterior cuando `v4.1` está activado.	
`-v4-id-domain`	ID asignando nombre de dominio.	
`-v4-numeric-ids`	Compatibilidad con ID de propietario numéricos (activado o desactivado).	

Parámetros para crear una LIF

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

Si utiliza Kerberos, debe habilitar Kerberos en varias LIF.

Campo	Descripción	Su valor
`-lif`	Nombre que se proporciona para la nueva LIF.	
`-role`	Utilice el rol de LIF de datos en este flujo de trabajo.	`data`
`-data-protocol`	Utilice solo el protocolo NFS en este flujo de trabajo.	`nfs`
`-home-node`	El nodo al que devuelve la LIF cuando `network interface revert` se ejecuta el comando en la LIF. Obtenga más información sobre `network interface revert` en el "Referencia de comandos del ONTAP".	
`-home-port`	El puerto o grupo de interfaces al que devuelve la LIF cuando `network interface revert` se ejecuta el comando en la LIF.	

`-address`	La dirección IPv4 o IPv6 del clúster que se usará para el acceso a los datos mediante la nueva LIF.	
`-netmask`	La máscara de red y la puerta de enlace para la LIF.	
`-subnet`	Un conjunto de direcciones IP. Se utiliza en lugar de `-address` y `-netmask` para asignar direcciones y máscaras de red automáticamente.	
`-firewall-policy`	Utilice la política de firewall de datos predeterminada en este flujo de trabajo.	`data`

Parámetros para la resolución del nombre de host DNS

Proporcione estos valores con `vserver services name-service dns create` el comando cuando configura DNS.

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

Información del servicio de nombres

Parámetros para crear usuarios locales

Debe proporcionar estos valores si está creando usuarios locales mediante el `vserver services name-service unix-user create` comando. Si va a configurar usuarios locales cargando un archivo que contiene usuarios UNIX de un identificador de recursos uniforme (URI), no es necesario especificar estos valores manualmente.

	Nombre de usuario `(-user)`	ID de usuario `(-id)`	ID de grupo `(-primary-gid)`	Nombre completo `(-full-name)`
Ejemplo	javier martínez	123	100	John Miller
1				
2				

3				
…				
n				

Parámetros para crear grupos locales

Proporcione estos valores si está creando grupos locales mediante el `vserver services name-service unix-group create` comando. Si va a configurar grupos locales cargando un archivo que contiene grupos UNIX de un URI, no es necesario especificar estos valores manualmente.

	Nombre del grupo (`-name`)	ID Grupo (`-id`)
Ejemplo	Ingeniería	100
1		
2		
3		
…		
n		

Parámetros para NIS

Proporcione estos valores con el `vserver services name-service nis-domain create` comando.

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.

Campo	Descripción	Su valor
`-domain`	El dominio NIS que utilizará la SVM para las búsquedas de nombres.	
`-active`	El servidor de dominio NIS activo.	`true` o. `false`
`-nis-servers`	Una lista separada por comas de direcciones IP y nombres de host para los servidores NIS utilizados por la configuración del dominio.	

Parámetros para LDAP

Proporcione estos valores con el `vserver services name-service ldap client create` comando.

También se necesita `.pem` un archivo de certificado de CA raíz autofirmado.

Campo	Descripción	Su valor
`-vserver`	El nombre de la SVM para la cual se creará la configuración de cliente LDAP.	
`-client-config`	El nombre que se asigna para la nueva configuración de cliente LDAP.	
`-ldap-servers`	Lista separada por comas de direcciones IP y nombres de host para los servidores LDAP.	
`-query-timeout`	Utilice los `3` segundos predeterminados para este flujo de trabajo.	`3`
`-min-bind-level`	El nivel de autenticación de enlace mínimo. El valor predeterminado es `anonymous`. Debe establecerse en `sasl` si la firma y el sellado están configuradas.	
`-preferred-ad-servers`	Uno o varios servidores de Active Directory preferidos por dirección IP en una lista delimitada por comas.	
`-ad-domain`	El dominio de Active Directory.	
`-schema`	La plantilla de esquema que se va a utilizar. Puede utilizar un esquema predeterminado o personalizado.	
`-port`	Utilice el puerto del servidor LDAP predeterminado `389` para este flujo de trabajo.	`389`
`-bind-dn`	El nombre distintivo del usuario Bind.	
`-base-dn`	El nombre distintivo de la base. El valor por defecto es `""` (root).	

Campo	Descripción	Su valor
`-base-scope`	Utilice el ámbito de búsqueda base por defecto `subnet` para este flujo de trabajo.	`subnet`
`-session-security`	Habilita la firma, firma y sellado LDAP. El valor predeterminado es `none`.	
`-use-start-tls`	Habilita LDAP sobre TLS. El valor predeterminado es `false`.	

Parámetros para la autenticación Kerberos

Proporcione estos valores con el `vserver nfs kerberos realm create` comando. Algunos de los valores variarán dependiendo de si utiliza Microsoft Active Directory como servidor de Key Distribution Center (KDC), o MIT u otro servidor UNIX KDC.

Campo	Descripción	Su valor
`-vserver`	La SVM que se comunicará con el KDC.	
`-realm`	El dominio Kerberos.	
`-clock-skew`	Desfase de reloj permitido entre clientes y servidores.	
`-kdc-ip`	Dirección IP de KDC.	
`-kdc-port`	Número de puerto KDC.	
`-adserver-name`	Sólo Microsoft KDC: Nombre DEL servidor DE ANUNCIOS.	
`-adserver-ip`	Sólo Microsoft KDC: Dirección IP del servidor DE ANUNCIOS.	
`-adminserver-ip`	Sólo UNIX KDC: Dirección IP del servidor de administración.	
`-adminserver-port`	Sólo UNIX KDC: Número de puerto del servidor de administración.	
`-passwordserver-ip`	Sólo UNIX KDC: Dirección IP del servidor de contraseñas.	

`-passwordserver-port`	Sólo UNIX KDC: Puerto del servidor de contraseñas.	
`-kdc-vendor`	Proveedor KDC.	{ `Microsoft`
`Other` }	`-comment`	Cualquier comentario deseado.

Proporcione estos valores con el `vserver nfs kerberos interface enable` comando.

Campo	Descripción	Su valor
`-vserver`	El nombre de la SVM para la cual desea crear una configuración de Kerberos.	
`-lif`	La LIF de datos en la que activará Kerberos. Puede habilitar Kerberos en varias LIF.	
`-spn`	El nombre del principio de servicio (SPN)	
`-permitted-enc-types`	`` `aes-256`Se recomiendan los tipos de cifrado permitidos para Kerberos sobre NFS;, según las capacidades del cliente. ``	
`-admin-username`	Las credenciales de administrador de KDC para recuperar la clave secreta SPN directamente del KDC. Se requiere una contraseña	
`-keytab-uri`	El archivo keytab del KDC que contiene la clave SPN si no tiene credenciales de administrador KDC.	
`-ou`	La unidad organizativa (OU) en la que se creará la cuenta de servidor de Microsoft Active Directory al habilitar Kerberos mediante un Reino para Microsoft KDC.	

Se añade capacidad de almacenamiento a una SVM habilitada para NFS

Parámetros para crear políticas y reglas de exportación

Proporcione estos valores con el `vserver export-policy create` comando.

Campo	Descripción	Su valor
`-vserver`	El nombre de la SVM que alojará el nuevo volumen.	
`-policyname`	Nombre que se proporciona para una nueva política de exportación.	

Proporcione estos valores para cada regla con el `vserver export-policy rule create` comando.

Campo	Descripción	Su valor
`-clientmatch`	Especificación de coincidencia del cliente.	
`-ruleindex`	Posición de la regla de exportación en la lista de reglas.	
`-protocol`	Utilice NFS en este flujo de trabajo.	`nfs`
`-rorule`	Método de autenticación de acceso de solo lectura.	
`-rwrule`	Método de autenticación para acceso de lectura/escritura.	
`-superuser`	Método de autenticación para acceso de superusuario.	
`-anon`	ID de usuario al que se asignan usuarios anónimos.	

Debe crear una o varias reglas para cada política de exportación.

`-ruleindex`	**`-clientmatch`**	**`-rorule`**	**`-rwrule`**	**`-superuser`**	**`-anon`**
Ejemplos	0.0.0.0/0,@rootaccess_netgroup	cualquiera	krb5	act	65534
1					
2					

3					
…					
n					

Parámetros para crear un volumen

Debe introducir estos valores con `volume create` el comando si va a crear un volumen en lugar de un qtree.

Campo	Descripción	Su valor
`-vserver`	El nombre de una SVM nueva o existente que alojará el nuevo volumen.	
`-volume`	Se suministra un nombre descriptivo único para el volumen nuevo.	
`-aggregate`	El nombre de un agregado en el clúster de con espacio suficiente para el nuevo volumen de NFS.	
`-size`	Se proporciona un entero para el tamaño del nuevo volumen.	
`-user`	Nombre o ID del usuario que se establece como el propietario de la raíz del volumen.	
`-group`	Nombre o ID del grupo que se establece como el propietario de la raíz del volumen.	
`--security-style`	Utilice el estilo de seguridad UNIX para este flujo de trabajo.	`unix`
`-junction-path`	Ubicación bajo la raíz (/) donde se va a montar el nuevo volumen.	
`-export-policy`	Si tiene pensado utilizar una política de exportación existente, puede introducir su nombre al crear el volumen.	

Parámetros para crear un qtree

Debe proporcionar estos valores con `volume qtree create` el comando si va a crear un qtree en lugar de un volumen.

Campo	Descripción	Su valor
`-vserver`	El nombre de la SVM en la que reside el volumen que contiene el qtree.	
`-volume`	El nombre del volumen que contendrá el nuevo qtree.	
`-qtree`	Nombre descriptivo único que se proporciona para el nuevo qtree, con 64 caracteres o menos.	
`-qtree-path`	El argumento de la ruta de qtree en el formato `/vol/volume_name/qtree_name\>` se puede especificar en lugar de especificar el volumen y el qtree como argumentos independientes.	
`-unix-permissions`	Optional: Los permisos de UNIX para el qtree.	
`-export-policy`	Si tiene pensado usar una política de exportación existente, puede introducir su nombre al crear el qtree.	

Información relacionada

- "Referencia de comandos del ONTAP"

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
-policyname 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`* `-policyname 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 nfsv4_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
ONTAP 9.5 y anteriores	`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}`
ONTAP 9.6 y posterior	`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}`

- `-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 gestión 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	`network ping`
Dirección IPv6	`network ping6`

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 e1c -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 e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

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

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         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
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
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.

```
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`
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 materian 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	Necesario para la fase DE INICIALIZACIÓN de GSS. El primer componente del SPN de usuario del cliente NFS se utiliza como usuario. El usuario nfs no es necesario si existe una asignación de nombre Kerberos-UNIX para el SPN del usuario cliente NFS.
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	a. Configure los tipos de cifrado permitidos por Kerberos NFS de la SVM: `vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`* Separe varios tipos de cifrado con una coma. b. Compruebe que el cambio se ha realizado correctamente: `vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`

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

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	`-admin-username` *`kdc_admin_username`*
No tiene las credenciales de administrador de KDC, pero tiene un archivo keytab del KDC que contiene la clave	`-keytab-uri` {ftp

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.
```

Añadir capacidad de almacenamiento a una SVM habilitada para NFS

Obtenga información sobre cómo agregar capacidad de almacenamiento a un SVM habilitado para NFS de ONTAP

Para añadir capacidad de almacenamiento a una SVM habilitada para NFS, debe crear un volumen o un qtree para proporcionar un contenedor de almacenamiento y crear o modificar una política de exportación para ese contenedor. Después, puede verificar el acceso del cliente NFS desde el clúster y probar el acceso desde los sistemas cliente.

Antes de empezar

- NFS debe estar configurado completamente en la SVM.
- La política de exportación predeterminada del volumen raíz de la SVM debe contener una regla que permita el acceso a todos los clientes.
- Se debe completar cualquier actualización de la configuración de los servicios de nombres.
- Deben completarse todas las adiciones o modificaciones que se realicen en una configuración de Kerberos.

Crear una política de exportación de NFS de ONTAP

Antes de crear reglas de exportación, debe crear una política de exportación para mantenerlas. Puede utilizar `vserver export-policy create` el comando para crear una política de exportación.

Pasos

1. Cree una política de exportación:

   `vserver export-policy create -vserver` *`vserver_name`* `-policyname` *`policy_name`*

   El nombre de la política puede tener hasta 256 caracteres.

2. Compruebe que se ha creado la política de exportación:

   `vserver export-policy show -policyname policy_name`

Ejemplo

Los siguientes comandos crean y verifican la creación de una política de exportación llamada exp1 en la SVM llamada vs1:

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
---------------  -------------------
vs1              exp1
```

Agregar una regla a una política de exportación de NFS de ONTAP

Sin reglas, la política de exportación no puede ofrecer a los clientes acceso a los datos. Para crear una nueva regla de exportación, debe identificar los clientes y seleccionar un formato de coincidencia de cliente, seleccionar los tipos de acceso y seguridad, especificar una asignación de ID de usuario anónimo, seleccionar un número de índice de regla y seleccionar el protocolo de acceso. A continuación, puede usar `vserver export-policy rule create` el comando para añadir la nueva regla a una política de exportación.

Antes de empezar

- La política de exportación a la que desea añadir las reglas de exportación ya debe existir.
- DNS debe haberse configurado correctamente en la SVM de datos y los servidores DNS deben tener entradas correctas para los clientes NFS.

  Esto se debe a que ONTAP realiza búsquedas de DNS mediante la configuración de DNS de la SVM de datos para determinados formatos de coincidencia del cliente. Además, si se produce un error en la coincidencia de reglas de política de exportación, se puede evitar el acceso a los datos del cliente.

- Si va a autenticarse con Kerberos, debe haber determinado cuál de los siguientes métodos de seguridad se utiliza en sus clientes 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)

Acerca de esta tarea

No es necesario crear una nueva regla si una regla existente en una política de exportación cubre las coincidencias del cliente y los requisitos de acceso.

Si se autentica con Kerberos y se accede a todos los volúmenes de la SVM mediante Kerberos, puede establecer las opciones de regla de exportación `-rorule` , `-rwrule` y `-superuser` para el volumen raíz en

`krb5`, `krb5i` o `krb5p`.

Pasos

1. Identifique los clientes y el formato de coincidencia del cliente para la nueva regla.

   `-clientmatch`La opción especifica los clientes a los que se aplica la regla. Se pueden especificar valores de coincidencia de clientes individuales o múltiples; las especificaciones de varios valores deben estar separadas por comas. Puede especificar la coincidencia en cualquiera de los siguientes formatos:

Formato de coincidencia del cliente	Ejemplo
Nombre de dominio precedido por "." carácter	`.example.com` o. `.example.com,.example.net,...`
Nombre de host	`host1` o. `host1,host2, ...`
Dirección IPv4	`10.1.12.24` o. `10.1.12.24,10.1.12.25, ...`
Dirección IPv4 con una máscara de subred expresada como un número de bits	`10.1.12.10/4` o. `10.1.12.10/4,10.1.12.11/4,...`
La dirección IPv4 con una máscara de red	`10.1.16.0/255.255.255.0` o. `10.1.16.0/255.255.255.0,10.1.17.0/255.255.255.0,...`
Dirección IPv6 en formato punteado	`::1.2.3.4` o. `::1.2.3.4,::1.2.3.5,...`
Dirección IPv6 con una máscara de subred expresada como un número de bits	`ff::00/32` o. `ff::00/32,ff::01/32,...`
Un solo netgroup con el nombre del netgroup precedido por el carácter @	`@netgroup1` o. `@netgroup1,@netgroup2,...`

   También puede combinar tipos de definiciones de cliente; por ejemplo, `.example.com,@netgroup1`.

   Al especificar direcciones IP, tenga en cuenta lo siguiente:

   - No se permite introducir un rango de direcciones IP, como 10.1.12.10-10.1.12.70.

     Las entradas con este formato se interpretan como cadenas de texto y se consideran nombres de host.

   - Al especificar direcciones IP individuales en reglas de exportación para la gestión granular del acceso a clientes, no especifique direcciones IP que se encuentren asignadas de forma dinámica (por ejemplo, DHCP) o temporalmente (por ejemplo, IPv6).

De lo contrario, el cliente pierde el acceso cuando cambia su dirección IP.

- No se permite introducir una dirección IPv6 con una máscara de red, como ff::12/ff::00.

2. Seleccione los tipos de acceso y seguridad de las coincidencias del cliente.

Puede especificar uno o varios de los siguientes modos de acceso a los clientes que se autentican con los tipos de seguridad especificados:

- `-rorule` (acceso de solo lectura)
- `-rwrule` (acceso de lectura y escritura)
- `-superuser` (acceso a raíz)

> Un cliente solo puede obtener acceso de lectura y escritura para un tipo de seguridad específico si la regla de exportación permite también el acceso de solo lectura para ese tipo de seguridad. Si el parámetro de solo lectura es más restrictivo para un tipo de seguridad que el parámetro de lectura y escritura, es posible que el cliente no obtenga acceso de lectura/escritura. Lo mismo es cierto para el acceso de superusuario.

Puede especificar una lista separada por comas de varios tipos de seguridad para una regla. Si especifica el tipo de seguridad `any` como o `never`, no especifique ningún otro tipo de seguridad. Elija entre los siguientes tipos de seguridad válidos:

Cuando el tipo de seguridad se establece en…	Un cliente coincidente puede acceder a los datos exportados…
`any`	Siempre, independientemente del tipo de seguridad entrante.
`none`	Si se enumera solo, a los clientes con cualquier tipo de seguridad se les concede acceso como anónimos. Si se enumera con otros tipos de seguridad, se concede acceso a los clientes con un tipo de seguridad especificado y se concede acceso como anónimos a los clientes con cualquier otro tipo de seguridad.
`never`	Nunca, independientemente del tipo de seguridad entrante.
`krb5`	Si está autenticada por Kerberos 5. Sólo autenticación: El encabezado de cada solicitud y respuesta está firmado.
`krb5i`	Si está autenticada por Kerberos 5i. Autenticación e integridad: Se firma el encabezado y el cuerpo de cada solicitud y respuesta.

Cuando el tipo de seguridad se establece en…	Un cliente coincidente puede acceder a los datos exportados…
`krb5p`	Si está autenticada por Kerberos 5p. Autenticación, integridad y privacidad: Se firma el encabezado y el cuerpo de cada solicitud y respuesta, y la carga útil de datos NFS está cifrada.
`ntlm`	Si se autentica con CIFS NTLM.
`sys`	Si se autentica mediante NFS AUTH_SYS.

El tipo de seguridad recomendado es `sys`, o si se utiliza Kerberos, `krb5`, `krb5i` o `krb5p`.

Si utiliza Kerberos con NFSv3, la regla de política de exportación debe permitir `-rorule` y `-rwrule` acceder a `sys` además `krb5` de . Esto se debe a la necesidad de permitir el acceso de Network Lock Manager (NLM) a la exportación.

3. Especifique una asignación de ID de usuario anónimo.

```
`-anon`La opción especifica un ID de usuario de UNIX o un nombre de
usuario asignado a solicitudes de cliente que llegan con un ID de
usuario de 0 (cero), que normalmente está asociado con el nombre de
usuario root. El valor predeterminado es `65534`. Los clientes NFS
normalmente asocian el ID de usuario 65534 con el nombre de usuario
nobody (también conocido como _root squashing_). En ONTAP, este ID de
usuario está asociado con el usuario pcuser. Para desactivar el acceso
de cualquier cliente con un ID de usuario de 0, especifique un valor de
`65535`.
```

4. Seleccione el orden de índice de reglas.

```
`-ruleindex`La opción especifica el número de índice de la regla. Las
reglas se evalúan según su orden en la lista de números de índice; las
reglas con números de índice más bajos se evalúan primero. Por ejemplo,
la regla con el número de índice 1 se evalúa antes que la regla con el
número de índice 2.
```

Si va a añadir…	Realice lo siguiente…
La primera regla a una política de exportación	Introduzca `1`.

Si va a añadir…	Realice lo siguiente…
Reglas adicionales a una política de exportación	a. Mostrar reglas existentes en la política: `vserver export-policy rule show -instance -policyname your_policy` b. Seleccione un número de índice para la nueva regla dependiendo de la orden en la que se debe evaluar.

5. Seleccione el valor de acceso NFS aplicable{`nfs`|`nfs3`|`nfs4`: }.

   `nfs` coincide con cualquier versión y `nfs3` `nfs4` solo coincide con esas versiones específicas.

6. Cree la regla de exportación y añádala a una política de exportación existente:

   `vserver export-policy rule create -vserver vserver_name -policyname policy_name -ruleindex integer -protocol {nfs|nfs3|nfs4} -clientmatch { text | "text,text,…" } -rorule security_type -rwrule security_type -superuser security_type -anon user_ID`

7. Muestre las reglas de la política de exportación para verificar que la nueva regla esté presente:

   `vserver export-policy rule show -policyname policy_name`

   El comando muestra un resumen de esa política de exportación, incluida una lista de reglas aplicadas a esa política. ONTAP asigna a cada regla un número de índice de regla. Una vez que conozca el número de índice de regla, puede utilizarlo para mostrar información detallada acerca de la regla de exportación especificada.

8. Compruebe que las reglas aplicadas a la política de exportación se han configurado correctamente:

   `vserver export-policy rule show -policyname policy_name -vserver vserver_name -ruleindex integer`

Ejemplos

Los siguientes comandos crean y verifican la creación de una regla de exportación en la SVM llamada vs1 en una política de exportación llamada rs1. La regla tiene el número de índice 1. La regla coincide con cualquier cliente del dominio eng.company.com y el netgroup @netgroup1. La regla habilita todo el acceso NFS. Permite el acceso de solo lectura y de lectura y escritura a los usuarios autenticados con AUTH_SYS. Los clientes con el ID de usuario de UNIX 0 (cero) se anóniman a menos que se autentiquen con Kerberos.

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname exp1
-ruleindex 1 -protocol nfs
-clientmatch .eng.company.com,@netgoup1 -rorule sys -rwrule sys -anon
65534 -superuser krb5

vs1::> vserver export-policy rule show -policyname nfs_policy
Virtual      Policy         Rule    Access    Client           RO
Server       Name           Index   Protocol  Match            Rule
------------ -------------- ------  --------  ---------------- ------
vs1          exp1           1       nfs       eng.company.com, sys
                                              @netgroup1

vs1::> vserver export-policy rule show -policyname exp1 -vserver vs1
-ruleindex 1

                                Vserver: vs1
                            Policy Name: exp1
                             Rule Index: 1
                          Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
                           RO Access Rule: sys
                           RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
                  Superuser Security Types: krb5
              Honor SetUID Bits in SETATTR: true
                 Allow Creation of Devices: true
```

Los siguientes comandos crean y verifican la creación de una regla de exportación en la SVM llamada vs2 en una política de exportación llamada expol2. La regla tiene el número de índice 21. La regla coincide con los clientes con los miembros del netgroup dev_netgroup_main. La regla habilita todo el acceso NFS. Permite el acceso de solo lectura para los usuarios que se autentican con AUTH_SYS y requiere autenticación de Kerberos para acceso de lectura/escritura y raíz. A los clientes con el ID de usuario de UNIX 0 (cero) se les deniega el acceso raíz a menos que se autentiquen con Kerberos.

```
vs2::> vserver export-policy rule create -vserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5

vs2::> vserver export-policy rule show -policyname nfs_policy
Virtual  Policy       Rule    Access    Client              RO
Server   Name         Index   Protocol  Match               Rule
-------- ------------ ------  --------  ------------------  ------
vs2      expol2       21       nfs      @dev_netgroup_main  sys

vs2::> vserver export-policy rule show -policyname expol2 -vserver vs1
-ruleindex 21

                                  Vserver: vs2
                              Policy Name: expol2
                               Rule Index: 21
                           Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
                                           @dev_netgroup_main
                            RO Access Rule: sys
                            RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
                  Superuser Security Types: krb5
              Honor SetUID Bits in SETATTR: true
                 Allow Creation of Devices: true
```

Cree un volumen o un contenedor de almacenamiento Qtree

Crear un volumen NFS de ONTAP

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

Acerca de esta tarea

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

Antes de empezar

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

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

Pasos

1. Cree el volumen con un punto de unión:

   `volume create -vserver` *`svm_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {`*`integer`*`[KB|MB|GB|TB|PB]} -security-style unix -user` *`user_name_or_number`* `-group` *`group_name_or_number`* `-junction-path` *`junction_path`* `[-policy` *`export_policy_name`*`]`

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

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

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

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

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

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

   + Si planea utilizar una política de exportación existente, puede especificarla al crear el volumen. También puede agregar una política de exportación más adelante con `volume modify` el comando.

2. Compruebe que el volumen se ha creado con el punto de unión deseado:

   `volume show -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction`

Ejemplos

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

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

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver          Volume    Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  users1    true     /users          RW_volume
```

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

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

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                          Junction                 Junction
Vserver          Volume   Active   Junction Path   Path Source
---------------- -------  -------- --------------- -----------
vs1.example.com  home4    true     /eng/home       RW_volume
```

Crear un qtree NFS de ONTAP

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

Antes de empezar

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

Pasos

1. Cree el qtree:

   `volume qtree create -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `} -security-style unix [-policy` *`export_policy_name`*`]`

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

   De forma predeterminada, los qtrees heredan las políticas de exportación de su volumen principal, pero se pueden configurar para que utilicen las suyas propias. Si piensa utilizar una política de exportación existente, puede especificarla al crear el qtree. También puede agregar una política de exportación más adelante con `volume qtree modify` el comando.

2. Compruebe que el qtree se ha creado con la ruta de unión que desee:

   `volume qtree show -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `}`

Ejemplo

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

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

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

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

Acceso seguro a NFS mediante políticas de exportación

Obtenga información sobre cómo proteger el acceso a ONTAP NFS mediante políticas de exportación

Puede utilizar las políticas de exportación para restringir el acceso de NFS a volúmenes o qtrees a clientes que coincidan con parámetros específicos. Al aprovisionar almacenamiento nuevo, puede usar una política y reglas existentes, agregar reglas a una política existente o crear una nueva política y reglas. También puede comprobar la configuración de las políticas de exportación

> A partir de ONTAP 9.3, puede habilitar la comprobación de la configuración de la política de exportación como un trabajo en segundo plano que registra cualquier infracción de reglas en una lista de reglas de error. `vserver export-policy config-checker`Los comandos invocan el comprobador y muestran los resultados, que puede utilizar para verificar la configuración y eliminar reglas erróneas de la política.Los comandos solo validan la configuración de exportación para nombres de host, grupos de red y usuarios anónimos.

Administrar el orden de procesamiento de las reglas de exportación de ONTAP NFS

Puede utilizar `vserver export-policy rule setindex` el comando para definir manualmente el número de índice de una regla de exportación existente. Esto le permite especificar la prioridad mediante la cual ONTAP aplica reglas de exportación a las solicitudes de clientes.

Acerca de esta tarea

Si el nuevo número de índice ya está en uso, el comando inserta la regla en el punto especificado y vuelve a ordenar la lista en consecuencia.

Paso

1. Modifique el número de índice de una regla de exportación especificada:

   ```
   vserver export-policy rule setindex -vserver virtual_server_name -policyname
   policy_name -ruleindex integer -newruleindex integer
   ```

Ejemplo

El siguiente comando cambia el número de índice de una regla de exportación en el número de índice 3 al número de índice 2 de una política de exportación denominada r1 en la SVM denominada vs1:

```
vs1::> vserver export-policy rule setindex -vserver vs1
-policyname rs1 -ruleindex 3 -newruleindex 2
```

Asignar una política de exportación NFS de ONTAP a un volumen

Cada volumen incluido en la SVM debe estar asociado a una política de exportación que contenga reglas de exportación para que los clientes accedan a los datos del volumen.

Acerca de esta tarea

Es posible asociar una política de exportación a un volumen cuando se crea el volumen o en cualquier momento después de crearlo. Es posible asociar una política de exportación al volumen, aunque otra se puede asociar a muchos volúmenes.

Pasos

1. Si no se especificó una política de exportación cuando se creó el volumen, asigne una política de exportación al volumen:

   ```
   volume modify -vserver vserver_name -volume volume_name -policy
   export_policy_name
   ```

2. Compruebe que la política se haya asignado al volumen:

   ```
   volume show -volume volume_name -fields policy
   ```

Ejemplo

Los siguientes comandos asignan la política de exportación nfs_policy al volumen vol1 en la SVM vs1 y verifican la asignación:

```
cluster::> volume modify -v1server vs1 -volume vol1 -policy nfs_policy

cluster::>volume show -volume vol -fields policy
vserver volume       policy
------- ------------ ----------------
vs1     vol1         nfs_policy
```

Asignar una política de exportación NFS de ONTAP a un qtree

En lugar de exportar un volumen completo, también puede exportar un qtree concreto de un volumen para que los clientes puedan acceder a él directamente. Puede asignar una política de exportación a un qtree para exportarlo. Puede asignar la política de exportación al crear un qtree nuevo o al modificar un qtree existente.

Antes de empezar

Debe existir la política de exportación.

Acerca de esta tarea

De forma predeterminada, los qtrees heredan la política de exportación principal del volumen que contiene si no se especifica de otro modo en el momento de la creación.

Puede asociar una política de exportación a un qtree al crear el qtree o en cualquier momento después de crearlo. Puede asociar una política de exportación al qtree, aunque otra se puede asociar con muchos qtrees.

Pasos

1. Si no se especificó una política de exportación al crear el qtree, asigne una política de exportación al qtree:

   `volume qtree modify -vserver` *`vserver_name`* `-qtree-path /vol/`*`volume_name/qtree_name`* `-export-policy` *`export_policy_name`*

2. Compruebe que la política se ha asignado al qtree:

   `volume qtree show -qtree` *`qtree_name`* `-fields export-policy`

Ejemplo

Los siguientes comandos asignan la política de exportación nfs_policy al qtree qt1 en la SVM vs1 y verifican la asignación:

```
cluster::> volume modify -v1server vs1 -qtree-path /vol/vol1/qt1 -policy
nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy
------- ------ ----- -------------
vs1     data1  qt01  nfs_policy
```

Verificar el acceso del cliente NFS de ONTAP desde el clúster

Para proporcionar acceso a un recurso compartido a clientes seleccionados, debe establecer permisos de archivo UNIX en un host de administración UNIX. Puede comprobar el acceso del cliente mediante `vserver export-policy check-access` el comando y ajustar las reglas de exportación según sea necesario.

Pasos

1. En el clúster, compruebe el acceso del cliente a las exportaciones mediante `vserver export-policy check-access` el comando.

   El siguiente comando comprueba el acceso de lectura/escritura de un cliente NFSv3 con la dirección IP 1.2.3.4 en el volumen home2. El resultado del comando muestra que el volumen utiliza la política de exportación `exp-home-dir` y que el acceso es denegado.

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
-type read-write
                                    Policy    Policy     Rule
Path                    Policy      Owner     Owner Type Index  Access
----------------------- ----------- --------- ---------- ------
----------
/                       default     vs1_root  volume          1 read
/eng                    default     vs1_root  volume          1 read
/eng/home2              exp-home-dir home2    volume          1 denied

3 entries were displayed.
```

2. Examine el resultado para determinar si la política de exportación funciona según lo previsto y el acceso al cliente se comporta como se espera.

   Específicamente, debe comprobar qué política de exportación usa el volumen o el qtree y el tipo de acceso al cliente como resultado.

3. Si es necesario, vuelva a configurar las reglas de política de exportación.

Probar el acceso a ONTAP NFS desde los sistemas cliente

Después de verificar el acceso de NFS al nuevo objeto de almacenamiento, debe probar la configuración iniciando sesión en un host de administración NFS y leyendo datos desde y escribiendo datos en la SVM. A continuación, debe repetir el proceso como usuario que no sea raíz en un sistema cliente.

Antes de empezar

- El sistema cliente debe tener una dirección IP permitida por la regla de exportación especificada anteriormente.
- Debe tener la información de inicio de sesión para el usuario raíz.

Pasos

1. En el clúster, compruebe la dirección IP de la LIF que aloja el nuevo volumen:

   `network interface show –vserver` *`svm_name`*

   Obtenga más información sobre `network interface show` en el "Referencia de comandos del ONTAP".

2. Inicie sesión como usuario raíz en el sistema cliente host de administración.
3. Cambie el directorio a la carpeta de montaje:

   ```
   cd /mnt/
   ```

4. Cree y monte una nueva carpeta con la dirección IP de la SVM:

   a. Crear una nueva carpeta:
   `mkdir /mnt/folder`

   b. Monte el nuevo volumen en este nuevo directorio:
   `mount -t nfs -o hard IPAddress:/volume_name /mnt/folder`

   c. Cambie el directorio a la nueva carpeta:
   `cd folder`

   Los siguientes comandos crean una carpeta llamada test1, montan el volumen vol1 en la dirección IP 192.0.2.130 de la carpeta de montaje test1 y cambian al nuevo directorio test1:

   ```
   host# mkdir /mnt/test1
   host# mount -t nfs -o hard 192.0.2.130:/vol1 /mnt/test1
   host# cd /mnt/test1
   ```

5. Cree un archivo nuevo, compruebe que existe y escriba texto en él:

   a. Cree un archivo de prueba:
   `touch filename`

   b. Verifique que el archivo existe.:
   `ls -l filename`

   c. Introduzca:
   `cat > filename`

   Escriba algún texto y, a continuación, presione Ctrl+D para escribir texto en el archivo de prueba.

   d. Muestra el contenido del archivo de prueba.
   `cat filename`

   e. Elimine el archivo de prueba:
   `rm filename`

   f. Vuelva al directorio principal:
   `cd ..`

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

6. Como raíz, se pueden establecer los permisos y la propiedad de UNIX que se desee en el volumen montado.
7. En un sistema cliente UNIX identificado en las reglas de exportación, inicie sesión como uno de los usuarios autorizados que ahora tienen acceso al nuevo volumen y repita los procedimientos descritos en los pasos 3 a 5 para verificar que puede montar el volumen y crear un archivo.

Dónde encontrar información adicional sobre ONTAP NFS

Una vez que haya probado correctamente el acceso al cliente NFS, puede realizar una configuración de NFS adicional o añadir acceso SAN. Cuando se completa el acceso al protocolo, debe proteger el volumen raíz de la máquina virtual de almacenamiento (SVM).

Configuración de NFS

El acceso a NFS se puede configurar más utilizando la siguiente información e informes técnicos:

- "Gestión de NFS"

  Describe cómo configurar y gestionar el acceso a archivos mediante NFS.

- "Informe técnico de NetApp 4067: Guía de prácticas recomendadas e implementación de NFS"

  Sirve de guía de funcionamiento de NFSv3 y NFSv4 y ofrece una descripción general del sistema operativo de ONTAP haciendo hincapié en NFSv4.

- "Informe técnico de NetApp 4073: Autenticación unificada segura"

  Explica cómo configurar ONTAP para su uso con los servidores Kerberos versión 5 (krb5) basados en UNIX para la autenticación de almacenamiento NFS y Active Directory de Windows Server (AD) como proveedor de identidades KDC y Lightweight Directory Access Protocol (LDAP).

- "Informe técnico de NetApp 3580: Guía de mejoras y prácticas recomendadas de NFSv4: Implementación de Data ONTAP"

  Describe las prácticas recomendadas que se deben seguir mientras implementa componentes de NFSv4 en clientes AIX, Linux o Solaris conectados a sistemas que ejecutan ONTAP.

Configuración de redes

Además, puede configurar las funciones de red y los servicios de nombres mediante los siguientes informes técnicos e informati:

- "Gestión de NFS"

  Describe cómo configurar y gestionar las redes de ONTAP.

- "Informe técnico de NetApp 4182: Consideraciones de diseño y prácticas recomendadas de almacenamiento Ethernet para las configuraciones de Data ONTAP en clúster"

  Describe la implementación de las configuraciones de red de ONTAP, y proporciona escenarios comunes de puesta en marcha de redes y recomendaciones de prácticas recomendadas.

- "Informe técnico de NetApp 4668: Guía de prácticas recomendadas de servicios de nombres"

  Explica cómo configurar la configuración de LDAP, NIS, DNS y archivos locales con fines de autenticación.

Configuración del protocolo SAN

Si desea proporcionar o modificar el acceso SAN a la SVM nueva, puede usar la información de configuración de FC o iSCSI, que está disponible para varios sistemas operativos host.

Protección de volúmenes raíz

Después de configurar los protocolos en la SVM, debe asegurarse de que su volumen raíz esté protegido:

- "Protección de datos"

  Describe cómo crear un reflejo de uso compartido de carga para proteger el volumen raíz de SVM, que es una práctica recomendada por NetApp para SVM habilitadas para NAS. También describe cómo recuperarse rápidamente de fallos o pérdidas de volúmenes mediante la promoción del volumen raíz de SVM desde un reflejo de uso compartido de carga.

En qué se diferencian las exportaciones de ONTAP de las exportaciones de 7-Mode

En qué se diferencian las exportaciones de ONTAP de las exportaciones de 7-Mode

Si no conoce cómo implementa ONTAP las exportaciones de NFS, puede comparar las herramientas de configuración de exportación de ONTAP y 7-Mode, así como `/etc/exports` archivos de muestra de 7-Mode con reglas y políticas en clúster.

En ONTAP no hay `/etc/exports` ningún archivo ni `exportfs` comando. En su lugar, debe definir una política de exportación. Las políticas de exportación le permiten controlar el acceso de los clientes de la misma forma que en 7-Mode, pero le proporcionan funcionalidades adicionales como la capacidad de reutilizar la misma política de exportación para varios volúmenes.

Información relacionada

"Gestión de NFS"

"Informe técnico de NetApp 4067: Guía de prácticas recomendadas e implementación de NFS"

Obtenga información sobre las comparaciones de exportación de NFS de 7-Mode y ONTAP

Las exportaciones en ONTAP se definen y utilizan de forma diferente a las que se utilizan en entornos de 7-Mode.

Áreas de diferencia	7-Mode	ONTAP
Cómo se definen las exportaciones	Las exportaciones se definen en el `/etc/exports` archivo.	Las exportaciones se definen mediante la creación de una política de exportación dentro de una SVM. Una SVM puede incluir más de una política de exportación.
Ámbito de exportación	• Las exportaciones se aplican a una ruta de archivo o qtree especificados. • Debe crear una entrada separada en `/etc/exports` para cada ruta o qtree del archivo. • Las exportaciones son persistentes solo si están definidas en el `/etc/exports` archivo.	• Las políticas de exportación se aplican a un volumen completo, incluidos todos los qtrees y rutas de archivos contenidos en el volumen. • Las políticas de exportación se pueden aplicar a más de un volumen si se desea. • Todas las políticas de exportación son persistentes a través de reinicios del sistema.
Cercado (especificando un acceso diferente para clientes específicos a los mismos recursos)	Para proporcionar a clientes específicos un acceso diferente a un único recurso exportado, debe enumerar cada cliente y su acceso permitido en el `/etc/exports` archivo.	Las políticas de exportación están compuestas por varias reglas individuales de exportación. Cada regla de exportación define permisos de acceso específicos para un recurso y enumera los clientes que tienen dichos permisos. Para especificar un acceso diferente para clientes específicos, debe crear una regla de exportación para cada conjunto específico de permisos de acceso, enumerar los clientes que tienen esos permisos y, a continuación, agregar las reglas a la directiva de exportación.

Alias de nombre	Al definir una exportación, puede elegir que el nombre de la exportación sea diferente del nombre de la ruta de acceso del archivo. Debe utilizar el `-actual` parámetro al definir dicha exportación en el `/etc/exports` archivo.	Es posible optar por que el nombre del volumen exportado sea diferente del nombre del volumen real. Para ello, debe montar el volumen con un nombre de ruta de unión personalizado dentro del espacio de nombres de la SVM. De manera predeterminada, los volúmenes se montan con su nombre de volumen. Para personalizar el nombre de ruta de unión de un volumen, debe desmontarlo, cambiarle el nombre y, a continuación, volver a montarlo.

Conozca los ejemplos de políticas de exportación de NFS de ONTAP

Puede revisar el ejemplo de políticas de exportación para comprender mejor cómo funcionan las políticas de exportación en ONTAP.

Implementación de ONTAP de ejemplo para una exportación de 7-Mode

El siguiente ejemplo muestra una exportación de 7-Mode tal como aparece en el `/etc/export` archivo:

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

Para reproducir esta exportación como una política de exportación en clúster, debe crear una política de exportación con tres reglas de exportación y, a continuación, asignar la política de exportación al volumen vol1.

Regla	Elemento	Valor
Regla 1	`-clientmatch` (especificación del cliente)	`@readonly_netgroup`
`-ruleindex`(posición de la regla de exportación en la lista de reglas)	`1`	`-protocol`
`nfs`	`-rorule`(permitir acceso de sólo lectura)	`sys` (Cliente autenticado con AUTH_SYS)

Regla	Elemento	Valor
`-rwrule`(permitir acceso de lectura y escritura)	`never`	`-superuser`(permitir acceso de superusuario)
`none`(root *squashed* a anon)	Regla 2	`-clientmatch`
`@rootaccess_netgroup`	`-ruleindex`	`2`
`-protocol`	`nfs`	`-rorule`
`sys`	`-rwrule`	`sys`
`-superuser`	`sys`	Regla 3
`-clientmatch`	`@readwrite_netgroup1,@readwrite_netgroup2`	`-ruleindex`
`3`	`-protocol`	`nfs`
`-rorule`	`sys`	`-rwrule`
`sys`	`-superuser`	`none`

1. Cree una política de exportación denominada exp_vol1:

   ```
   vserver export-policy create -vserver NewSVM -policyname exp_vol1
   ```

2. Cree tres reglas con los siguientes parámetros en el comando base:
   - Comando base:
     `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1`
   - Parámetros de regla:
     `-clientmatch @readonly_netgroup -ruleindex 1 -protocol nfs -rorule sys -rwrule never -superuser none + + -clientmatch @rootaccess_netgroup -ruleindex 2 -protocol nfs -rorule sys -rwrule sys -superuser sys -clientmatch @readwrite_netgroup1,@readwrite_netgroup2 -ruleindex 3 -protocol nfs -rorule sys -rwrule sys -superuser none`
3. Asigne la política al volumen vol1:

   ```
   volume modify -vserver NewSVM -volume vol1 -policy exp_vol1
   ```

Consolidación de muestras de exportaciones de 7-Mode

En el siguiente ejemplo, se muestra `/etc/export` un archivo de 7-Mode con una línea para cada 10 qtrees:

```
/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s
```

En ONTAP, se necesita una de estas dos políticas para cada qtree: Una con una regla que incluya `-clientmatch host1519s`, o una con una regla que incluya `-clientmatch host2057s`.

1. Cree dos políticas de exportación llamadas exp_vol1q1 y exp_vol1q2:
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q1`
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q2`
2. Crear una regla para cada política:
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q1 -clientmatch host1519s -rwrule sys -superuser sys`
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q2 -clientmatch host1519s -rwrule sys -superuser sys`
3. Aplique las políticas a los qtrees:
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_1472 -export -policy exp_vol1q1`
   - [4 qtrees siguientes…]
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_2237 -export -policy exp_vol1q2`
   - [4 qtrees siguientes…]

Si posteriormente necesita añadir qtrees adicionales para esos hosts, deberá usar las mismas políticas de exportación.