Añadir capacidad de almacenamiento a una SVM habilitada para NFS

ONTAP 9

NetApp
April 16, 2024

Tabla de contenidos

Añadir capacidad de almacenamiento a una SVM habilitada para NFS

Añadir capacidad de almacenamiento a una información general de SVM habilitada para NFS

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.

Lo que necesitará

- NFS debe estar configurado por completo 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.

Cree una política de exportación

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

Añada una regla a una política de exportación

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 utilizar la `vserver export-policy rule create` comando para añadir la nueva regla a una política de exportación.

Lo que necesitará

- 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 mediante 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 va a autenticarse con Kerberos y si se accede a todos los volúmenes de la SVM a través de Kerberos, puede configurar las opciones de regla de exportación `-rorule`, `-rwrule`, y. `-superuser` para el volumen raíz a. `krb5`, `krb5i`, o. `krb5p`.

Pasos

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

   La `-clientmatch` 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 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 como `any` 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 se autentica con Kerberos 5i. Autenticación e integridad: Se firma el encabezado y el cuerpo de cada solicitud y respuesta.
`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` acceso a. `sys` además de `krb5`. 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.

   La `-anon` La opción especifica un ID de usuario o nombre de usuario de UNIX que se asigna a las solicitudes de cliente que llegan con un ID de usuario de 0 (cero), que normalmente se asocia 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 por parte de cualquier cliente con un ID de usuario de 0, especifique un valor de `65535`.

4. Seleccione el orden de índice de reglas.

   La `-ruleindex` 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`.
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 de NFS aplicable: {`nfs`|`nfs3`|`nfs4`}.

   `nfs` coincide con cualquier versión, `nfs3` y.. `nfs4` coincidir sólo con aquellas 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 con el nombre vs1 en una política de exportación denominada 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

Cree un volumen

Puede crear un volumen y especificar su punto de unión y otras propiedades mediante la `volume create` 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 mediante el `volume mount` 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 actividades, emita 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.

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 la 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 nueva jerarquía debajo de un nuevo volumen), por ejemplo, `/new_dir/new_vol`, Entonces debe crear primero un nuevo volumen principal que se junte 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 piensa utilizar una política de exportación existente, puede especificarla al crear el volumen. También puede añadir una política de exportación más adelante con el `volume modify` 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 el SVM vs1 y el nuevo volumen estará disponible en `/eng/home`, que se convierte en el directorio principal de `/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
```

Cree un qtree

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

Lo que necesitará

- La SVM y el volumen que contendrán el nuevo qtree ya deben existir.
- El estilo de seguridad de SVM debe ser UNIX y 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 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 añadir una política de exportación más adelante con el `volume qtree modify` 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 siguiente ejemplo 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 NFS seguro mediante políticas de exportación

Acceso NFS seguro 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. La `vserver export-policy config-checker` Los comandos invocan el comprobador y muestran los resultados, que se pueden utilizar para verificar la configuración y eliminar reglas erróneas de la directiva. Los comandos sólo validan la configuración de exportación para los nombres de host, grupos de red y usuarios anónimos.

Gestionar la orden de procesamiento de las reglas de exportación

Puede utilizar el `vserver export-policy rule setindex` comando para establecer 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 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
```

Asigne una política de exportación 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.

Lo que necesitará

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
```

Compruebe el acceso del cliente NFS 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 el `vserver export-policy check-access` ajuste las reglas de exportación según sea necesario.

Pasos

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

Lo que necesitará

- 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`*

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 volumen nuevo en este directorio nuevo:
   `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. Compruebe 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.