Administrar NFS

ONTAP 9

NetApp
January 08, 2026

Tabla de contenidos

Administrar NFS

Obtenga información sobre el acceso a archivos ONTAP para el protocolo NFS

ONTAP incluye funciones de acceso a archivos disponibles para el protocolo NFS. Puede habilitar un servidor NFS y exportar volúmenes o qtrees.

Este procedimiento se realiza en las siguientes circunstancias:

- Desea comprender la gama de funcionalidades del protocolo NFS de ONTAP.
- Desea realizar tareas de configuración y mantenimiento menos comunes, no una configuración NFS básica.
- Desea usar la interfaz de línea de comandos (CLI), no System Manager ni una herramienta de secuencias de comandos automatizadas.

Comprender el acceso a archivos NAS

Espacios de nombres y puntos de unión

Obtenga información sobre los espacios de nombres y puntos de unión de ONTAP NAS

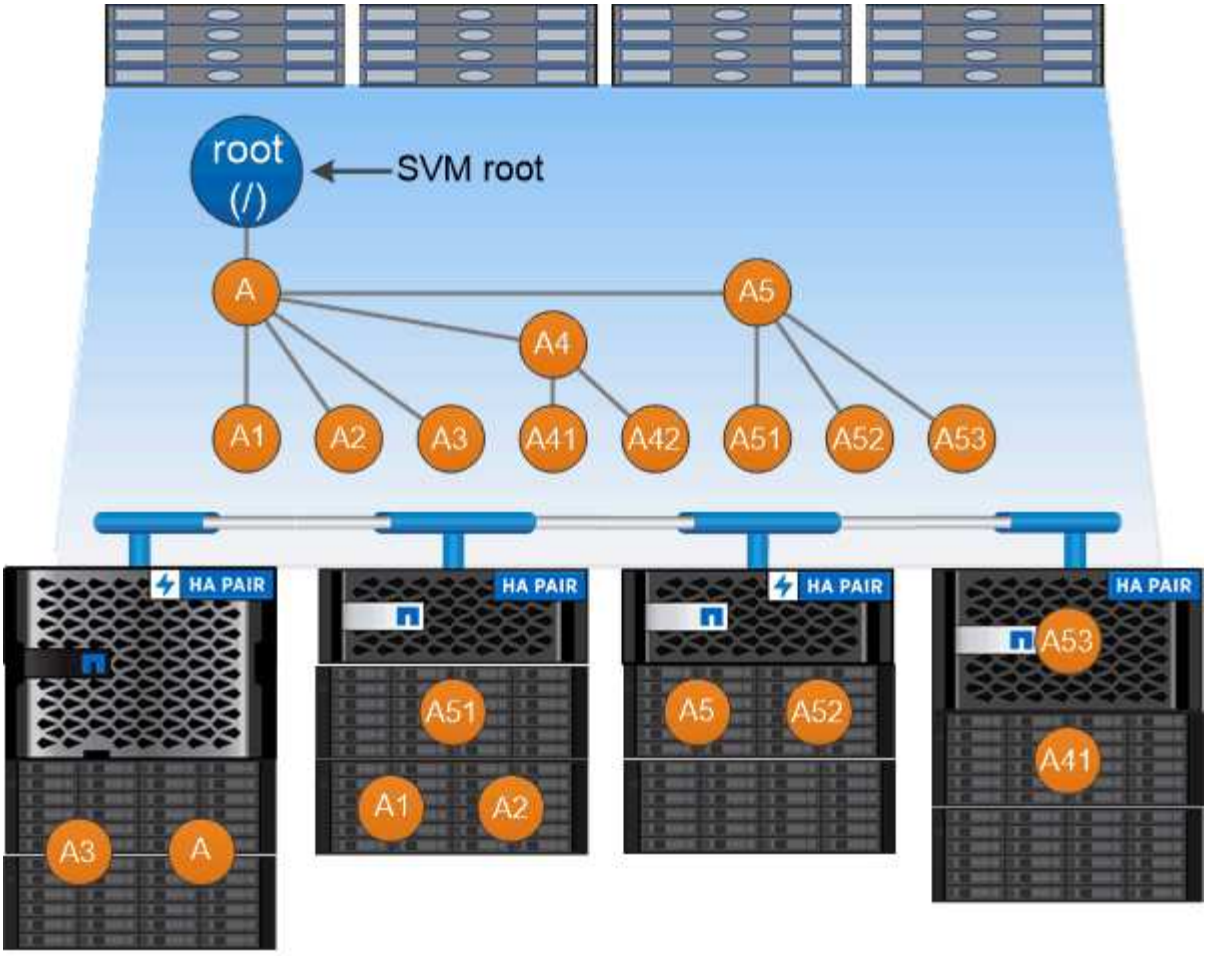
Un NAS *Namespace* es una agrupación lógica de volúmenes Unidos en *Junction points* para crear una única jerarquía de sistemas de archivos. Un cliente con permisos suficientes puede acceder a los archivos del espacio de nombres sin especificar la ubicación de los archivos en el almacenamiento. Los volúmenes que se han Unido pueden residir en cualquier parte del clúster.

En lugar de montar cada volumen que contenga un archivo de interés, los clientes NAS montan un NFS *export* o acceden a un SMB *share.* la exportación o el recurso compartido representan todo el espacio de nombres o una ubicación intermedia dentro del espacio de nombres. El cliente solo accede a los volúmenes montados por debajo de su punto de acceso.

Es posible añadir volúmenes al espacio de nombres según sea necesario. Puede crear puntos de unión directamente debajo de una unión de volumen principal o en un directorio dentro de un volumen. Una ruta de acceso a una unión de volumen para un volumen denominado «`vol3 » puede ser `/vol1/vol2/vol3`, o `/vol1/dir2/vol3`, o incluso `/dir1/dir2/vol3`. La ruta se llama la *ruta de unión.*

Cada SVM tiene un espacio de nombres único. El volumen raíz de la SVM es el punto de entrada de la jerarquía del espacio de nombres.

Para garantizar que los datos sigan estando disponibles en caso de que se produzca una interrupción o conmutación al nodo de respaldo, debe crear una copia *mirror* de uso compartido de la carga para el volumen raíz de la SVM.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

Ejemplo

En el ejemplo siguiente se crea un volumen llamado «`home4`» ubicado en la SVM VS1 que tiene una ruta de unión `/eng/home`:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

Obtenga más información sobre las arquitecturas de espacios de nombres de ONTAP NAS

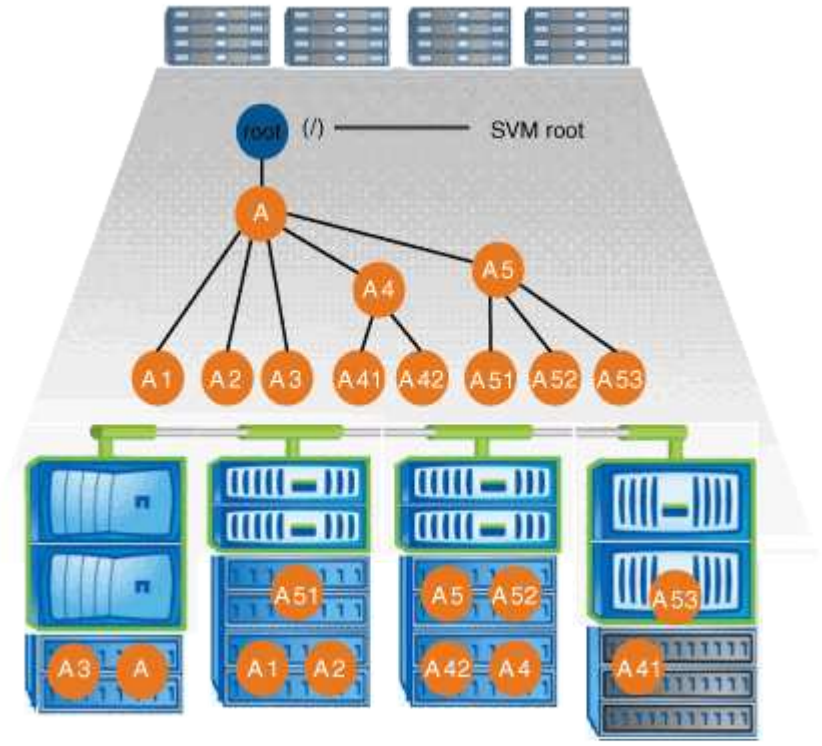
Existen varias arquitecturas de espacio de nombres NAS típicas que se pueden usar a medida que se crea el espacio de nombres de la SVM. Puede elegir la arquitectura de espacio de nombres que se ajuste a sus necesidades empresariales y de flujos de trabajo.

El principio del espacio de nombres siempre es el volumen raíz, que se representa mediante una barra diagonal (/). La arquitectura del espacio de nombres en la raíz se divide en tres categorías básicas:

- Un árbol ramificado único, con una única unión a la raíz del espacio de nombres
- Múltiples árboles ramificados, con varios puntos de unión en la raíz del espacio de nombres
- Varios volúmenes independientes, cada uno con un punto de unión separado en la raíz del espacio de nombres

Espacio de nombres con árbol ramificado único

Una arquitectura con un único árbol ramificado tiene un único punto de inserción en la raíz del espacio de nombres de SVM. El único punto de inserción puede ser un volumen junted o un directorio debajo de la raíz. Los demás volúmenes se montan en puntos de unión debajo del punto de inserción único (que puede ser un volumen o un directorio).

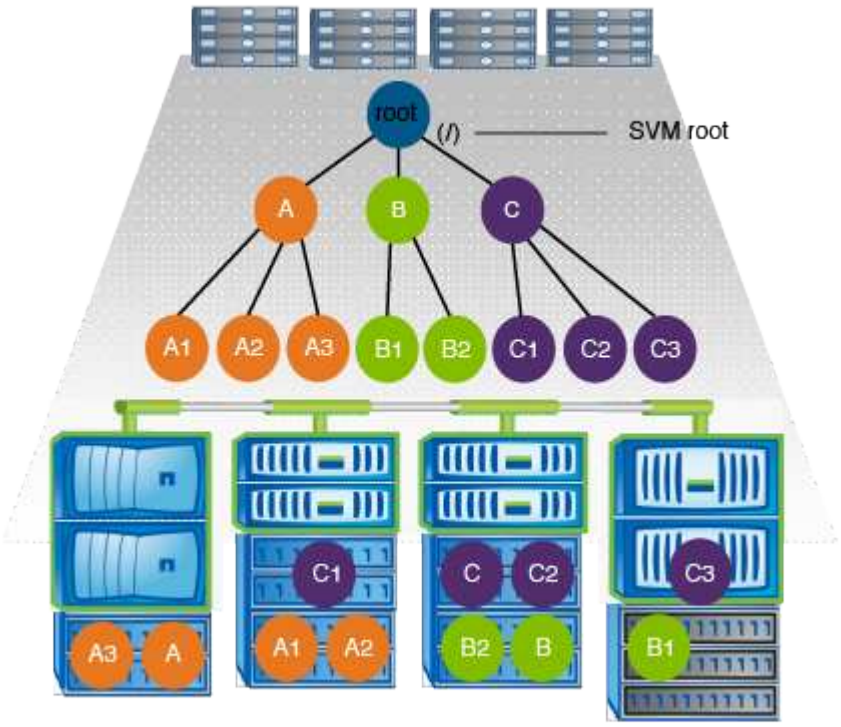


Por ejemplo, una configuración de unión de volúmenes típica con la arquitectura de espacio de nombres anterior podría tener el aspecto de la siguiente configuración, donde todos los volúmenes se unen por debajo del punto de inserción único, que es un directorio denominado «data»:

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- --------------------   -----------
vs1     corp1       true     /data/dir1/corp1       RW_volume
vs1     corp2       true     /data/dir1/corp2       RW_volume
vs1     data1       true     /data/data1            RW_volume
vs1     eng1        true     /data/data1/eng1       RW_volume
vs1     eng2        true     /data/data1/eng2       RW_volume
vs1     sales       true     /data/data1/sales      RW_volume
vs1     vol1        true     /data/vol1             RW_volume
vs1     vol2        true     /data/vol2             RW_volume
vs1     vol3        true     /data/vol3             RW_volume
vs1     vs1_root    -        /                      -
```

Espacio de nombres con varios árboles ramificados

Una arquitectura con varios árboles ramificados tiene varios puntos de inserción en la raíz del espacio de nombres de la SVM. Los puntos de inserción pueden ser volúmenes de juntados o directorios debajo de la raíz. Los demás volúmenes se montan en puntos de unión debajo de los puntos de inserción (que pueden ser volúmenes o directorios).

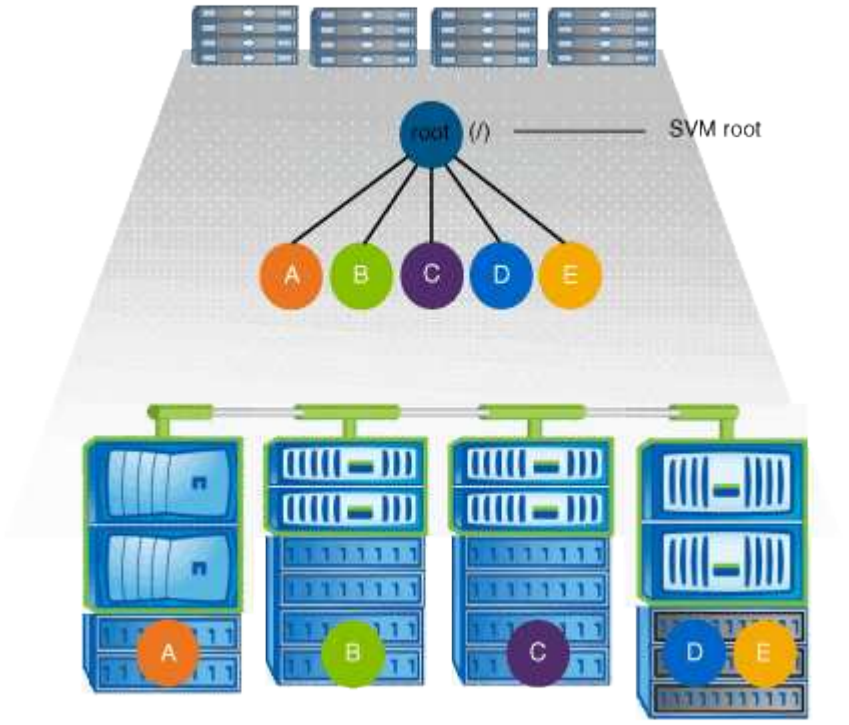


Por ejemplo, una configuración típica de unión de volúmenes con la arquitectura anterior del espacio de nombres puede parecer la siguiente configuración, donde hay tres puntos de inserción en el volumen raíz de la SVM. Dos puntos de inserción son directorios denominados «dé» y «proyectos». Un punto de inserción es un volumen Unido denominado «'audit'»:

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- -------------------    -----------
vs1     audit       true     /audit                 RW_volume
vs1     audit_logs1 true     /audit/logs1           RW_volume
vs1     audit_logs2 true     /audit/logs2           RW_volume
vs1     audit_logs3 true     /audit/logs3           RW_volume
vs1     eng         true     /data/eng              RW_volume
vs1     mktg1       true     /data/mktg1            RW_volume
vs1     mktg2       true     /data/mktg2            RW_volume
vs1     project1    true     /projects/project1     RW_volume
vs1     project2    true     /projects/project2     RW_volume
vs1     vs1_root    -        /                      -
```

Espacio de nombres con varios volúmenes independientes

En una arquitectura con volúmenes independientes, cada volumen tiene un punto de inserción en la raíz del espacio de nombres de SVM; sin embargo, el volumen no se ha Unido por debajo de otro volumen. Cada volumen tiene una ruta única y se conecta directamente debajo de la raíz o se conecta bajo un directorio debajo de la raíz.



Por ejemplo, una configuración típica de unión de volúmenes con la arquitectura anterior del espacio de nombres puede parecer la siguiente configuración, donde hay cinco puntos de inserción en el volumen raíz de la SVM, donde cada punto de inserción representa una ruta a un volumen.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- -------------------    -----------
vs1     eng         true     /eng                   RW_volume
vs1     mktg        true     /vol/mktg              RW_volume
vs1     project1    true     /project1              RW_volume
vs1     project2    true     /project2              RW_volume
vs1     sales       true     /sales                 RW_volume
vs1     vs1_root    -        /                      -
```

Cómo ONTAP controla el acceso a los archivos

Obtenga más información sobre el control de acceso a archivos de ONTAP NAS

ONTAP controla el acceso a los archivos de acuerdo con las restricciones basadas en archivos y en autenticación que especifique.

Cuando un cliente se conecta al sistema de almacenamiento para acceder a los archivos, ONTAP debe realizar dos tareas:

- Autenticación

  ONTAP debe autenticar el cliente verificando la identidad con un origen de confianza. Además, el tipo de autenticación del cliente es un método que puede utilizarse para determinar si un cliente puede acceder a los datos al configurar políticas de exportación (opcional para CIFS).

- Autorización

  ONTAP tiene que autorizar al usuario comparando las credenciales del usuario con los permisos configurados en el archivo o directorio y determinando qué tipo de acceso, si hubiera, proporcionar.

Para administrar correctamente el control de acceso a archivos, ONTAP debe comunicarse con servicios externos como servidores NIS, LDAP y Active Directory. La configuración de un sistema de almacenamiento para el acceso a archivos mediante CIFS o NFS requiere configurar los servicios adecuados en función de su entorno en ONTAP.

Obtenga información sobre las restricciones basadas en autenticación para las SVM de ONTAP NAS

Con las restricciones basadas en la autenticación, puede especificar qué máquinas cliente y qué usuarios se pueden conectar a la máquina virtual de almacenamiento (SVM).

ONTAP es compatible con la autenticación Kerberos desde servidores UNIX y Windows.

Obtenga información sobre las restricciones basadas en archivos para los SVM de ONTAP NAS

ONTAP evalúa tres niveles de seguridad para determinar si una entidad está autorizada para realizar una acción solicitada sobre archivos y directorios que residen en una SVM. El acceso está determinado por los permisos efectivos después de la evaluación de los

tres niveles de seguridad.

Cualquier objeto de almacenamiento puede contener hasta tres tipos de capas de seguridad:

- Seguridad de exportación (NFS) y uso compartido (SMB)

  La seguridad de exportación y uso compartido se aplica al acceso de los clientes a una exportación NFS o un recurso compartido de SMB dado. Los usuarios con privilegios administrativos pueden gestionar la seguridad de exportación y nivel de recurso compartido desde clientes SMB y NFS.

- Seguridad de directorio y archivos del protector de acceso a nivel de almacenamiento

  La seguridad de protección de acceso a nivel de almacenamiento se aplica al acceso de clientes SMB y NFS a volúmenes de SVM. Sólo se admiten permisos de acceso NTFS. Para que ONTAP realice comprobaciones de seguridad en los usuarios de UNIX con el fin de acceder a los datos de los volúmenes para los que se ha aplicado la protección de acceso a nivel de almacenamiento, el usuario de UNIX debe asignar a un usuario de Windows en la SVM propietaria del volumen.

  > Si ve la configuración de seguridad en un archivo o un directorio desde un cliente NFS o SMB, no verá la seguridad de Access Guard a nivel de almacenamiento. La seguridad de protección de acceso a nivel de almacenamiento no se puede revocar de un cliente, ni siquiera por un administrador de sistema (Windows o UNIX).

- Seguridad nativa a nivel de archivo de NTFS, UNIX y NFSv4

  Existe una seguridad nativa a nivel de archivo en el archivo o directorio que representa el objeto de almacenamiento. Puede establecer la seguridad a nivel de archivo desde un cliente. Los permisos de archivos son efectivos independientemente de si se utiliza SMB o NFS para acceder a los datos.

Cómo gestiona ONTAP la autenticación del cliente NFS

Obtenga información sobre la autenticación ONTAP para clientes NAS

Los clientes de NFS deben autenticarse correctamente antes de poder acceder a los datos en la SVM. ONTAP autentica a los clientes al comprobar sus credenciales de UNIX con los servicios de nombres que se configuran.

Cuando un cliente NFS se conecta con la SVM, ONTAP obtiene las credenciales de UNIX del usuario comprobando diferentes servicios de nombre, en función de la configuración de los servicios de nombres de la SVM. ONTAP puede comprobar credenciales para cuentas UNIX locales, dominios NIS y dominios LDAP. Debe haber al menos uno de ellos configurado para que ONTAP pueda autenticar correctamente al usuario. Puede especificar varios servicios de nombres y el orden en el que ONTAP los busca.

En un entorno NFS puro con estilos de seguridad de volúmenes UNIX, esta configuración es suficiente para autenticar y proporcionar el acceso adecuado a los archivos para que los usuarios que se conecten desde un cliente NFS.

Si utiliza estilos de seguridad de volúmenes mixtos, NTFS o unificados, ONTAP debe obtener un nombre de usuario SMB para el usuario UNIX para la autenticación con un controlador de dominio de Windows. Esto puede suceder mediante la asignación de usuarios individuales mediante cuentas de UNIX locales o dominios LDAP, o bien mediante un usuario de SMB predeterminado. Puede especificar los servicios de nombres que ONTAP busca en qué orden, o bien especificar un usuario de SMB predeterminado.

Descubra cómo ONTAP utiliza los servicios de nombres

ONTAP utiliza los servicios de nombres para obtener información acerca de los usuarios y los clientes. ONTAP usa esta información para autenticar a los usuarios que acceden a los datos o administran el sistema de almacenamiento, y para asignar las credenciales de usuario en un entorno mixto.

Al configurar el sistema de almacenamiento, debe especificar los servicios de nombres que desea que ONTAP utilice para obtener credenciales de usuario con fines de autenticación. ONTAP admite los siguientes servicios de nombres:

- Usuarios locales (archivo)
- Dominios NIS externos (NIS)
- Dominios LDAP externos (LDAP)

```
`vserver services name-service ns-switch`La familia de comandos se utiliza para configurar SVM con los orígenes para buscar información de red y el orden en el que se deben buscar. Estos comandos proporcionan la funcionalidad equivalente del `/etc/nsswitch.conf` archivo en los sistemas UNIX.
```

Cuando un cliente NFS se conecta a la SVM, ONTAP comprueba los servicios de nombre especificados para obtener las credenciales de UNIX del usuario. Si los servicios de nombres están configurados correctamente y ONTAP puede obtener las credenciales de UNIX, ONTAP autentica correctamente el usuario.

En un entorno con estilos de seguridad mixtos, es posible que ONTAP tenga que asignar credenciales de usuario. Debe configurar los servicios de nombres según sea necesario para el entorno de a fin de permitir que ONTAP asigne correctamente las credenciales de usuario.

ONTAP también utiliza servicios de nombres para autenticar cuentas de administrador de SVM. Debe tener esto en cuenta al configurar o modificar el switch del servicio de nombres para evitar deshabilitar accidentalmente la autenticación de las cuentas de administrador de SVM. Para obtener más información sobre los usuarios de administración de SVM, consulte "Autenticación de administrador y RBAC".

Otorgar acceso a archivos SMB de ONTAP desde clientes NFS

ONTAP utiliza la semántica de seguridad del sistema de archivos de Windows NT (NTFS) para determinar si un usuario de UNIX, en un cliente NFS, tiene acceso a un archivo con permisos NTFS.

Para ello, ONTAP convierte el identificador de usuario de UNIX (UID) del usuario en una credencial de SMB y, a continuación, utiliza la credencial de SMB para verificar que el usuario tiene derechos de acceso al archivo. Una credencial SMB consta de un identificador de seguridad principal (SID), normalmente el nombre de usuario de Windows del usuario y uno o más SID de grupo que corresponden a los grupos Windows de los que el usuario es miembro.

El tiempo que tarda ONTAP en convertir el UID de UNIX en una credencial SMB puede ser de decenas de milisegundos a cientos de milisegundos, dado que el proceso implica contactar a un controlador de dominio. ONTAP asigna el UID a la credencial SMB e introduce la asignación en una caché de credenciales para reducir el tiempo de verificación debido a la conversión.

Cómo funciona la caché de credenciales NFS de ONTAP

Cuando un usuario de NFS solicita acceso a exportaciones NFS en el sistema de almacenamiento de, ONTAP debe recuperar las credenciales de usuario desde servidores de nombres externos o desde archivos locales para autenticar el usuario. ONTAP después almacena estas credenciales en la caché de credenciales internas para futuras referencias. Comprender el funcionamiento de la caché de credenciales NFS le permite manejar los posibles problemas de rendimiento y acceso.

Sin la caché de credenciales, ONTAP tendría que consultar los servicios de nombres cada vez que un usuario NFS solicitara acceso. En un sistema de almacenamiento de mucha actividad al que acceden muchos usuarios, se pueden producir rápidamente problemas de rendimiento graves, que provocan retrasos no deseados o incluso la denegación del acceso del cliente NFS.

Con la caché de credenciales, ONTAP recupera las credenciales de usuario y las almacena durante un periodo predeterminado de tiempo para obtener un acceso rápido y sencillo en caso de que el cliente NFS envíe otra solicitud. Este método ofrece las siguientes ventajas:

- Facilita la carga en el sistema de almacenamiento al manejar menos solicitudes a servidores de nombres externos (como NIS o LDAP).
- Facilita la carga de los servidores de nombres externos enviando menos solicitudes.
- Acelera el acceso del usuario al eliminar el tiempo de espera para obtener credenciales de fuentes externas antes de que el usuario pueda autenticarse.

ONTAP almacena las credenciales positivas y negativas en la caché de credenciales. Las credenciales positivas significan que el usuario se ha autenticado y se le ha concedido acceso. Las credenciales negativas indican que el usuario no se ha autenticado y se le ha denegado el acceso.

De forma predeterminada, ONTAP almacena credenciales positivas durante 24 horas, es decir, tras autenticar inicialmente al usuario, ONTAP utiliza las credenciales en caché para cualquier solicitud de acceso por parte de ese usuario durante 24 horas. Si el usuario solicita acceso después de 24 horas, el ciclo se vuelve a iniciar: ONTAP descarta las credenciales en caché y obtiene de nuevo las credenciales del origen del servicio de nombres adecuado. Si las credenciales cambiaron en el servidor de nombres durante las 24 horas anteriores, ONTAP almacenará las credenciales actualizadas para utilizarlas en las próximas 24 horas.

De forma predeterminada, ONTAP almacena credenciales negativas durante dos horas; es decir, después de denegar inicialmente el acceso a un usuario, ONTAP continúa negando cualquier solicitud de acceso por ese usuario durante dos horas. Si el usuario solicita acceso después de 2 horas, el ciclo se inicia de nuevo: ONTAP obtiene las credenciales de nuevo del origen de servicio de nombres apropiado. Si las credenciales cambiaron en el servidor de nombres durante las dos horas anteriores, ONTAP almacena en caché las credenciales actualizadas para utilizarlas en las siguientes dos horas.

Cree y gestione volúmenes de datos en espacios de nombres NAS

Cree volúmenes NAS de ONTAP con puntos de unión específicos

Puede especificar el punto de unión cuando crea un volumen de datos. El volumen resultante se monta automáticamente en el punto de unión y se puede configurar inmediatamente para el acceso NAS.

Antes de empezar

- El agregado en el que desea crear el volumen ya debe existir.
- 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".

Los siguientes caracteres no pueden utilizarse en la ruta de unión: `* # " > < | ? \`

Además, la longitud de la ruta de unión no puede ser superior a 255 caracteres.

Pasos

1. Cree el volumen con un punto de unión:

```
volume create -vserver <vserver_name> -volume <volume_name> -aggregate
<aggregate_name> -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed} -junction-path <junction_path>
```

   La ruta de unión debe comenzar con la raíz (/) y puede contener tanto directorios como volúmenes con conexiones. No es necesario que la ruta de unión contenga el nombre del volumen. Las rutas de unión son independientes del nombre del volumen.

   Es opcional especificar un estilo de seguridad del volumen. Si no se especifica un estilo de seguridad, ONTAP crea el volumen con el mismo estilo de seguridad que se aplica al volumen raíz de la máquina virtual de almacenamiento (SVM). Sin embargo, es posible que el estilo de seguridad del volumen raíz no sea el estilo de seguridad que se desea aplicar al volumen de datos que se crea. La recomendación es especificar el estilo de seguridad al crear el volumen para minimizar los problemas de acceso a archivos difíciles de solucionar.

   La ruta de unión no distingue mayúsculas de minúsculas; `/ENG` es la misma que `/eng`. Si crea un recurso compartido CIFS, Windows trata la ruta de unión como si fuera sensible a mayúsculas de minúsculas. Por ejemplo, si la unión es `/ENG`, la ruta de acceso de un recurso compartido SMB debe empezar por `/ENG`, no `/eng`.

   Existen muchos parámetros opcionales que se pueden usar para personalizar un volumen de datos. Obtenga más información sobre `volume create` en el "Referencia de comandos del ONTAP".

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

```
volume show -vserver <vserver_name> -volume <volume_name> -junction
```

Ejemplo

En el ejemplo siguiente se crea un volumen llamado `home4` ubicado en la SVM VS1 que tiene una ruta de unión `/eng/home`:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

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

Cree volúmenes NAS de ONTAP sin puntos de unión específicos

Puede crear un volumen de datos sin especificar un punto de unión. El volumen resultante no se monta automáticamente y no se puede configurar para acceso NAS. Debe montar el volumen para poder configurar los recursos compartidos de SMB o las exportaciones de NFS de ese volumen.

Antes de empezar

- El agregado en el que desea crear el volumen ya debe existir.
- 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 sin un punto de unión mediante el siguiente comando:

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate
   aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
   {ntfs|unix|mixed}
   ```

   Es opcional especificar un estilo de seguridad del volumen. Si no se especifica un estilo de seguridad, ONTAP crea el volumen con el mismo estilo de seguridad que se aplica al volumen raíz de la máquina virtual de almacenamiento (SVM). Sin embargo, es posible que el estilo de seguridad del volumen raíz no sea el estilo de seguridad que se desea aplicar al volumen de datos. La recomendación es especificar el estilo de seguridad al crear el volumen para minimizar los problemas de acceso a archivos difíciles de solucionar.

   Existen muchos parámetros opcionales que se pueden usar para personalizar un volumen de datos. Obtenga más información sobre `volume create` en el "Referencia de comandos del ONTAP".

2. Compruebe que el volumen se ha creado sin un punto de unión:

   ```
   volume show -vserver vserver_name -volume volume_name -junction
   ```

Ejemplo

En el siguiente ejemplo se crea un volumen denominado «números» ubicado en la SVM vs1 que no se monta en un punto de unión:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                    Junction                 Junction
Vserver   Volume    Active   Junction Path   Path Source
--------- --------- -------- --------------- -----------
vs1       data      true     /data           RW_volume
vs1       home4     true     /eng/home       RW_volume
vs1       vs1_root  -        /               -
vs1       sales     -        -               -
```

Montar o desmontar volúmenes NFS de ONTAP en el espacio de nombres NAS

Un volumen se debe montar en el espacio de nombres NAS para poder configurar el acceso de clientes NAS a los datos contenidos en los volúmenes de la máquina virtual de almacenamiento (SVM). Puede montar un volumen en un punto de unión si no está montado actualmente. También es posible desmontar volúmenes.

Acerca de esta tarea

Si desmonta y desconecta un volumen, los clientes NAS no pueden acceder a todos los datos dentro del punto de unión, incluidos los datos en los volúmenes con puntos de unión ubicados en el espacio de nombres del volumen sin montar.

> Para interrumpir el acceso de un cliente NAS a un volumen, no basta con desmontar el volumen. Debe desconectar el volumen o realizar otros pasos para garantizar que las cachés del identificador de archivos del cliente se invaliden. Para obtener más información, consulte el siguiente artículo de la base de conocimientos:
>
> "Los clientes NFSv3 siguen teniendo acceso a un volumen después de eliminarse del espacio de nombres de ONTAP"

Al desmontar y desconectar un volumen, no se pierden datos dentro del volumen. Además, se conservan las políticas de exportación de volúmenes existentes y los recursos compartidos de SMB creados en el volumen o en directorios y puntos de unión dentro del volumen desmontado. Si vuelve a montar el volumen desmontado, los clientes NAS pueden acceder a los datos contenidos en el volumen mediante políticas de exportación y recursos compartidos SMB existentes.

Pasos

1. Realice la acción deseada:

Si desea…	Introduzca los comandos…
Montar un volumen	`volume mount -vserver svm_name -volume volume_name -junction-path junction_path`

Desmontar un volumen	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. Compruebe que el volumen esté en el estado de montaje deseado:

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

Ejemplos

El siguiente ejemplo monta un volumen llamado “sales” ubicado en SVM “VS1” al punto de unión “`/sales`”:

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

El siguiente ejemplo desmonta y desconecta un volumen llamado “data” ubicado en la SVM “VS1”:

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

Muestra la información del punto de unión y el montaje de volúmenes de NAS de ONTAP

Puede ver información sobre los volúmenes montados para las máquinas virtuales de almacenamiento (SVM) y los puntos de unión a los que están montados los volúmenes. También puede determinar qué volúmenes no están montados en un punto de unión. Esta información se puede usar para comprender y gestionar el espacio de nombres de la SVM.

Paso

1. Realice la acción deseada:

Si desea mostrar…	Introduzca el comando…
Información resumida sobre los volúmenes montados y desmontados en la SVM	`volume show -vserver` *`vserver_name`* `-junction`
Información detallada sobre los volúmenes montados y desmontados en la SVM	`volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-instance`
Información específica sobre los volúmenes montados y desmontados en la SVM	a. Si es necesario, puede mostrar campos válidos para el `-fields` parámetro mediante el siguiente comando: `volume show -fields ?` b. Visualice la información deseada mediante `-fields` el parámetro: `volume show -vserver` *`vserver_name`* `-fields` *`fieldname`*`,…`

Ejemplos

En el siguiente ejemplo, se muestra un resumen de los volúmenes montados y desmontados en la SVM vs1:

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

En el siguiente ejemplo, se muestra información sobre campos especificados para los volúmenes ubicados en la SVM vs2:

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

Configurar estilos de seguridad

Cómo afectan los estilos de seguridad al acceso a los datos

Conozca los estilos de seguridad de ONTAP NAS

Hay cuatro estilos de seguridad diferentes: UNIX, NTFS, mixto y unificado. Cada estilo de seguridad tiene un efecto diferente sobre cómo se gestionan los permisos para los datos. Debe comprender los diferentes efectos para asegurarse de que selecciona el estilo de seguridad adecuado para sus propósitos.

Es importante entender que los estilos de seguridad no determinan qué tipos de clientes pueden o no pueden tener acceso a los datos. Los estilos de seguridad sólo determinan el tipo de permisos que ONTAP utiliza para controlar el acceso a los datos y qué tipo de cliente puede modificar estos permisos.

Por ejemplo, si un volumen utiliza el estilo de seguridad UNIX, los clientes SMB todavía pueden acceder a los datos (siempre y cuando estos se autentiquen y autoricen correctamente) debido a la naturaleza multiprotocolo de ONTAP. Sin embargo, ONTAP utiliza permisos UNIX que sólo los clientes UNIX pueden modificar mediante herramientas nativas.

Estilo de seguridad	Clientes que pueden modificar permisos	Permisos que pueden utilizar los clientes	El estilo de seguridad efectivo resultante	Clientes que pueden acceder a los ficheros
UNIX	NFS	Bits del modo NFSv3	UNIX	NFS y SMB
		ACL de NFSv4.x		
NTFS	SMB	ACL de NTFS	NTFS	
Mixto	NFS o SMB	Bits del modo NFSv3	UNIX	
		NFSv4.ACLs		
		ACL de NTFS	NTFS	
Unificado (solo para Infinite Volume, en ONTAP 9.4 y versiones anteriores).	NFS o SMB	Bits del modo NFSv3	UNIX	
		ACL de NFSv4.1		
		ACL de NTFS	NTFS	

Los volúmenes de FlexVol son compatibles con UNIX, NTFS y estilos de seguridad mixtos. Cuando el estilo de seguridad es mixto o unificado, los permisos efectivos dependen del tipo de cliente que modificó por última vez los permisos porque los usuarios establecen el estilo de seguridad de forma individual. Si el último cliente que modificó permisos era un cliente NFSv3, los permisos son bits del modo NFSv3 de UNIX. Si el último cliente era un cliente NFSv4, los permisos son ACL de NFSv4. Si el último cliente era un cliente SMB, los permisos son ACL de Windows NTFS.

El estilo de seguridad unificado solo está disponible en Infinite Volume, que ya no son compatibles con ONTAP 9.5 y versiones posteriores. Para obtener más información, consulte Información general de gestión de volúmenes de FlexGroup.

El `show-effective-permissions` parámetro con el `vserver security file-directory` El comando le permite mostrar los permisos efectivos otorgados a un usuario de Windows o UNIX en la ruta de archivo o carpeta especificada. Además, el parámetro opcional `-share-name` le permite mostrar el permiso de uso compartido efectivo. Obtenga más información sobre `vserver security file-directory show-effective-permissions` en el "Referencia de comandos del ONTAP".

> ONTAP establece inicialmente algunos permisos de archivo predeterminados. De forma predeterminada, el estilo de seguridad efectivo de todos los datos de los volúmenes de estilo de seguridad mixto y unificado es UNIX y el tipo de permisos efectivos es bits de modo UNIX (0755 a menos que se especifique lo contrario) hasta que un cliente lo configure como permite el estilo de seguridad predeterminado. De forma predeterminada, el estilo de seguridad efectivo en todos los datos de los volúmenes de estilo de seguridad NTFS es NTFS y tiene una ACL que permite un control total para todos.

Información relacionada

- "Referencia de comandos del ONTAP"

Obtenga información sobre los estilos de seguridad en los volúmenes ONTAP NFS FlexVol

Los estilos de seguridad se pueden establecer en volúmenes de FlexVol (tanto

volúmenes raíz como de datos) y qtrees. Los estilos de seguridad se pueden configurar manualmente en el momento de la creación, heredados automáticamente o modificados posteriormente.

Decide qué estilo de seguridad utilizar en las SVM de ONTAP NAS

Para ayudar a decidir qué estilo de seguridad se debe usar en un volumen, se deben tener en cuenta dos factores. El factor principal es el tipo de administrador que administra el sistema de archivos. El factor secundario es el tipo de usuario o servicio que tiene acceso a los datos del volumen.

Al configurar el estilo de seguridad en un volumen, debe tener en cuenta las necesidades del entorno para garantizar que selecciona el mejor estilo de seguridad y evitar problemas con la gestión de permisos. Las siguientes consideraciones pueden ayudarle a decidir:

Estilo de seguridad	Elija si…
UNIX	• Un administrador de UNIX gestiona el sistema de ficheros. • La mayoría de los usuarios son clientes NFS. • Una aplicación que accede a los datos utiliza un usuario UNIX como cuenta de servicio.
NTFS	• Un administrador de Windows gestiona el sistema de archivos. • La mayoría de los usuarios son clientes SMB. • Una aplicación que accede a los datos utiliza un usuario de Windows como cuenta de servicio.
Mixto	• El sistema de archivos lo gestionan administradores de UNIX y Windows, y los usuarios están formados por clientes NFS y SMB.

Obtenga más información sobre la herencia del estilo de seguridad NFS de ONTAP

Si no especifica el estilo de seguridad al crear un nuevo volumen de FlexVol o un qtree, hereda su estilo de seguridad de formas diferentes.

Los estilos de seguridad se heredan de la siguiente manera:

- Un volumen FlexVol hereda el estilo de seguridad del volumen raíz de su SVM que contiene.
- Un qtree hereda el estilo de seguridad del volumen FlexVol que contiene.
- Un archivo o un directorio hereda el estilo de seguridad de su volumen o qtree de FlexVol.

Obtenga información sobre la conservación de permisos de ONTAP NFS UNIX

Cuando las aplicaciones Windows editan y guardan archivos de un volumen FlexVol que actualmente tienen permisos UNIX, ONTAP puede preservar los permisos UNIX.

Cuando las aplicaciones de clientes de Windows editan y guardan archivos, leen las propiedades de seguridad del archivo, crean un nuevo archivo temporal, aplican esas propiedades al archivo temporal y, a

continuación, asignan al archivo temporal el nombre de archivo original.

Cuando los clientes de Windows realizan una consulta para las propiedades de seguridad, reciben una ACL construida que representa exactamente los permisos de UNIX. El único propósito de esta ACL construida es preservar los permisos UNIX del archivo a medida que las aplicaciones de Windows actualizan los archivos para garantizar que los archivos resultantes tengan los mismos permisos UNIX. ONTAP no establece ninguna ACL de NTFS usando la ACL construida.

Administre los permisos de UNIX en las SVM NFS de ONTAP mediante la pestaña Seguridad de Windows

Si desea manipular los permisos de UNIX de archivos o carpetas en volúmenes o qtrees de estilo de seguridad mixtos en las SVM, puede utilizar la pestaña Seguridad en clientes de Windows. También puede utilizar aplicaciones que puedan consultar y establecer ACL de Windows.

- Modificación de permisos de UNIX

  Puede usar la pestaña Seguridad de Windows para ver y cambiar los permisos de UNIX para un volumen o un qtree de estilo de seguridad mixto. Si utiliza la ficha Seguridad de Windows principal para cambiar los permisos de UNIX, primero debe quitar la ACE existente que desea editar (esto establece los bits de modo en 0) antes de realizar los cambios. De forma alternativa, puede utilizar el editor avanzado para cambiar los permisos.

  Si se utilizan permisos de modo, puede cambiar directamente los permisos de modo para el UID, GID y otros (todos los demás con una cuenta en el equipo) de la lista. Por ejemplo, si el UID mostrado tiene permisos r-x, puede cambiar los permisos de UID a rwx.

- Cambiar los permisos de UNIX a los permisos NTFS

  Puede usar la pestaña Seguridad de Windows para reemplazar objetos de seguridad UNIX por objetos de seguridad de Windows en un volumen o qtree de estilo de seguridad mixto donde los archivos y carpetas tienen un estilo de seguridad efectivo de UNIX.

  Primero debe quitar todas las entradas de permisos de UNIX enumeradas antes de que pueda reemplazarlas con los objetos de usuario y grupo de Windows deseados. A continuación, puede configurar ACL basados en NTFS en los objetos Usuario y Grupo de Windows. Si quita todos los objetos de seguridad de UNIX y agrega sólo usuarios y grupos de Windows a un archivo o carpeta de un volumen o qtree de estilo de seguridad mixto, cambie el estilo de seguridad efectivo del archivo o carpeta de UNIX a NTFS.

  Al cambiar los permisos de una carpeta, el comportamiento predeterminado de Windows es propagar estos cambios a todas las subcarpetas y archivos. Por lo tanto, debe cambiar la opción de propagación a la configuración deseada si no desea propagar un cambio en el estilo de seguridad a todas las carpetas secundarias, subcarpetas y archivos.

Configurar estilos de seguridad en volúmenes raíz SVM de ONTAP NFS

El estilo de seguridad del volumen raíz de la máquina virtual de almacenamiento (SVM) se configura para determinar el tipo de permisos utilizados para los datos en el volumen raíz de la SVM.

Pasos

1. Utilice `vserver create` el comando con `-rootvolume-security-style` el parámetro para definir el estilo de seguridad.

   Las posibles opciones para el estilo de seguridad del volumen raíz son `unix` `ntfs` , , o `mixed`.

2. Mostrar y verificar la configuración, incluido el estilo de seguridad del volumen raíz de la SVM que creó:

   `vserver show -vserver` *`vserver_name`*

Configurar estilos de seguridad en volúmenes ONTAP NFS FlexVol

El estilo de seguridad del volumen FlexVol se configura para determinar el tipo de permisos utilizados para los datos en volúmenes FlexVol de la máquina virtual de almacenamiento (SVM).

Pasos

1. Ejecute una de las siguientes acciones:

Si el volumen de FlexVol…	Usar el comando…
Aún no existe	`volume create` e incluya el `-security-style` parámetro para especificar el estilo de seguridad.
Ya existe	`volume modify` e incluya el `-security-style` parámetro para especificar el estilo de seguridad.

   Las opciones posibles para el estilo de seguridad de FlexVol volume son `unix` `ntfs` , o `mixed`.

   Si no se especifica un estilo de seguridad al crear un volumen FlexVol, el volumen hereda el estilo de seguridad del volumen raíz.

   Para obtener más información acerca de los `volume create` `volume modify` comandos o, consulte "Gestión de almacenamiento lógico".

2. Para ver la configuración, incluido el estilo de seguridad del volumen FlexVol que se creó, escriba el siguiente comando:

   `volume show -volume volume_name -instance`

Configurar estilos de seguridad en qtrees de ONTAP NFS

El estilo de seguridad del volumen de qtrees se configura para determinar el tipo de permisos utilizados para los datos en qtrees.

Pasos

1. Ejecute una de las siguientes acciones:

Si el qtree…	Usar el comando…

Aún no existe	`volume qtree create` e incluya el `-security-style` parámetro para especificar el estilo de seguridad.
Ya existe	`volume qtree modify` e incluya el `-security-style` parámetro para especificar el estilo de seguridad.

Las posibles opciones para el estilo de seguridad de qtree son `unix` `ntfs` , o `mixed`.

Si no se especifica un estilo de seguridad al crear un qtree, el estilo de seguridad predeterminado es `mixed`.

Para obtener más información acerca de los `volume qtree create` `volume qtree modify` comandos o, consulte "Gestión de almacenamiento lógico".

2. Para mostrar la configuración, incluido el estilo de seguridad del qtree creado, escriba el siguiente comando: `volume qtree show -qtree` *`qtree_name`* `-instance`

Configurar el acceso a archivos mediante NFS

Obtenga información sobre cómo configurar el acceso a archivos NFS en las SVM de ONTAP

Debe completar una serie de pasos para permitir que los clientes accedan a archivos de máquinas virtuales de almacenamiento (SVM) mediante NFS. Existen algunos pasos adicionales que son opcionales en función de la configuración actual de su entorno.

Para que los clientes puedan acceder a los archivos de las SVM mediante NFS, debe realizar las siguientes tareas:

1. Habilite el protocolo NFS en la SVM.

   Debe configurar la SVM para permitir el acceso a los datos desde clientes a través de NFS.

2. Cree un servidor NFS en la SVM.

   Un servidor NFS es una entidad lógica en la SVM que permite que la SVM sirva archivos a través de NFS. Debe crear el servidor NFS y especificar las versiones de protocolo NFS que desea permitir.

3. Configure las políticas de exportación en la SVM.

   Es necesario configurar las políticas de exportación para que los volúmenes y qtrees estén disponibles para los clientes.

4. Configuración del servidor NFS con la seguridad y otras opciones adecuadas en función de la red y el entorno de almacenamiento.

   Este paso puede incluir la configuración de Kerberos, LDAP, NIS, asignaciones de nombres y usuarios locales.

Acceso seguro a NFS mediante políticas de exportación

Cómo las políticas de exportación controlan el acceso de los clientes a los volúmenes NFS o qtrees de ONTAP

Las políticas de exportación contienen una o varias *reglas de exportación* que procesan cada solicitud de acceso de cliente. El resultado del proceso determina si se deniega o se concede acceso al cliente y qué nivel de acceso. Para que los clientes accedan a los datos, debe haber una política de exportación con reglas de exportación en la máquina virtual de almacenamiento (SVM).

Se asocia exactamente una política de exportación a cada volumen o qtree para configurar el acceso de los clientes al volumen o qtree. La SVM puede contener varias políticas de exportación. Esto le permite hacer lo siguiente para las SVM con varios volúmenes o qtrees:

- Asigne diferentes políticas de exportación a cada volumen o qtree de la SVM para controlar el acceso de cliente individual a cada volumen o qtree de la SVM.
- Asigne la misma política de exportación a varios volúmenes o qtrees de la SVM para un control de acceso del cliente idéntico sin que tenga que crear una nueva política de exportación para cada volumen o qtree.

Si un cliente realiza una solicitud de acceso que no está permitida por la política de exportación aplicable, la solicitud falla con un mensaje de permiso denegado. Si un cliente no coincide con ninguna regla de la política de exportación, se deniega el acceso. Si una política de exportación está vacía, se deniegan implícitamente todos los accesos.

Puede modificar dinámicamente una política de exportación en un sistema que ejecuta ONTAP.

Políticas de exportación predeterminadas para SVM NFS de ONTAP

Cada SVM tiene una política de exportación predeterminada que no contiene reglas. Para que los clientes puedan acceder a los datos en la SVM, debe haber una política de exportación con reglas. Cada volumen FlexVol que contiene la SVM debe estar asociado a una política de exportación.

Al crear una SVM, el sistema de almacenamiento crea automáticamente una política de exportación predeterminada denominada `default` 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. También puede crear una política de exportación personalizada con reglas. Puede modificar y cambiar el nombre de la política de exportación predeterminada, pero no puede eliminar la política de exportación predeterminada.

Cuando se crea un volumen FlexVol en la SVM que contiene, el sistema de almacenamiento crea el volumen y asocia el volumen con la política de exportación predeterminada para el volumen raíz de la SVM. De manera predeterminada, cada volumen creado en la SVM está asociado con la política de exportación predeterminada para el volumen raíz. Puede usar la política de exportación predeterminada para todos los volúmenes contenidos en la SVM, o bien puede crear una política de exportación única para cada volumen. Es posible asociar varios volúmenes con la misma política de exportación.

Cómo funcionan las reglas de exportación de NFS de ONTAP

Las reglas de exportación son los elementos funcionales de una política de exportación. Las reglas de exportación coinciden con las solicitudes de acceso de los clientes a un

volumen con los parámetros específicos que se configuran para determinar cómo se manejan las solicitudes de acceso de los clientes.

La política de exportación debe contener al menos una regla de exportación para permitir el acceso a los clientes. Si una política de exportación contiene más de una regla, se procesan las reglas en el orden en que aparecen en la política de exportación. El orden de las reglas viene determinado por el número de índice de reglas. Si una regla coincide con un cliente, se utilizan los permisos de esa regla y no se procesan otras reglas. Si no hay reglas que coincidan, se deniega el acceso al cliente.

Puede configurar reglas de exportación para determinar los permisos de acceso de clientes con los siguientes criterios:

- El protocolo de acceso a archivos que utiliza el cliente para enviar la solicitud, por ejemplo, NFSv4 o SMB.
- Un identificador de cliente, por ejemplo, un nombre de host o una dirección IP.

  El tamaño máximo del `-clientmatch` campo es de 4096 caracteres.

- Tipo de seguridad utilizado por el cliente para autenticar, por ejemplo, Kerberos v5, NTLM o AUTH_SYS.

Si una regla especifica varios criterios, el cliente debe coincidir con todos ellos para que se aplique la regla.

> 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 al 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 los nombres de host, grupos de red y usuarios anónimos.

Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La solicitud de acceso del cliente se envía con el protocolo NFSv3 y el cliente tiene la dirección IP 10,1.17,37.

Aunque el protocolo de acceso del cliente coincida, la dirección IP del cliente se encuentra en una subred diferente de la especificada en la regla de exportación. Por lo tanto, la coincidencia de cliente falla y esta regla no se aplica a este cliente.

Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`

- `-rwrule any`

La solicitud de acceso del cliente se envía con el protocolo NFSv4 y el cliente tiene la dirección IP 10,1.16,54.

El protocolo de acceso del cliente coincide y la dirección IP del cliente se encuentra en la subred especificada. Por lo tanto, la coincidencia de cliente es correcta y esta regla se aplica a este cliente. El cliente obtiene acceso de lectura y escritura independientemente de su tipo de seguridad.

Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

El cliente n.o 1 tiene la dirección IP 10.1.16.207, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con Kerberos v5.

El cliente #2 tiene la dirección IP 10.1.16.211, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con AUTH_SYS.

El protocolo de acceso del cliente y la dirección IP coinciden con los dos clientes. El parámetro de solo lectura permite un acceso de solo lectura a todos los clientes independientemente del tipo de seguridad con el que se autentiquen. Por lo tanto, ambos clientes obtienen acceso de solo lectura. Sin embargo, sólo el cliente #1 obtiene acceso de lectura y escritura porque utilizó el tipo de seguridad aprobado Kerberos v5 para autenticar. El cliente n.o 2 no obtiene acceso de lectura/escritura.

Administrar el acceso a ONTAP SVM para clientes NFS con tipos de seguridad no listados

Cuando un cliente se presenta con un tipo de seguridad que no aparece en un parámetro de acceso de una regla de exportación, puede denegar el acceso al cliente o asignarlo al ID de usuario anónimo mediante la opción `none` del parámetro de acceso.

Es posible que un cliente se presente a sí mismo con un tipo de seguridad que no aparece en un parámetro de acceso porque se autentica con un tipo de seguridad diferente o que no se haya autenticado en absoluto (tipo de seguridad AUTH_NONE). De forma predeterminada, al cliente se le deniega automáticamente el acceso a ese nivel. Sin embargo, puede agregar la opción `none` al parámetro de acceso. Como resultado, los clientes con un estilo de seguridad no enumerado se asignan al ID de usuario anónimo en su lugar. `-anon`El parámetro determina qué ID de usuario se asigna a esos clientes. El ID de usuario especificado para el `-anon` parámetro debe ser un usuario válido que esté configurado con los permisos que considere adecuados para el usuario anónimo.

Valores válidos para el `-anon` rango de parámetros de `0` a `65535`.

ID de usuario asignado a. `-anon`	**Tratamiento resultante de las solicitudes de acceso de los clientes**
`0 - 65533`	La solicitud de acceso de cliente se asigna al ID de usuario anónimo y obtiene acceso en función de los permisos configurados para este usuario.
`65534`	La solicitud de acceso de cliente no se asigna al usuario y obtiene acceso en función de los permisos configurados para este usuario. Este es el valor predeterminado.
`65535`	La solicitud de acceso de cualquier cliente se deniega cuando se asigna a este ID y el cliente se presenta con el tipo de seguridad AUTH_NONE. La solicitud de acceso de los clientes con ID de usuario 0 se deniega cuando se asigna a este ID y el cliente se presenta a sí mismo con cualquier otro tipo de seguridad.

Al utilizar la opción `none`, es importante recordar que el parámetro de sólo lectura se procesa primero. Tenga en cuenta las siguientes directrices al configurar reglas de exportación para clientes con tipos de seguridad no listados:

Solo lectura incluye `none`	**Lectura y escritura incluidas** `none`	**Acceso resultante para clientes con tipos de seguridad no listados**
No	No	Denegada
No	Sí	Denegado porque sólo lectura se procesa primero
Sí	No	Sólo lectura como anónimo
Sí	Sí	Lectura y escritura como anónimo

Ejemplos

El siguiente ejemplo muestra una política de exportación con una `-rwrule any` parámetro:

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

El cliente n.o 1 tiene la dirección IP 10.1.16.207, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con Kerberos v5.

El cliente #2 tiene la dirección IP 10.1.16.211, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con AUTH_SYS.

El cliente #3 tiene la dirección IP 10.1.16.234, envía una solicitud de acceso con el protocolo NFSv3 y no se autentica (es decir, el tipo de seguridad AUTH_NONE).

El protocolo de acceso del cliente y la dirección IP coinciden con los tres clientes. El parámetro de sólo lectura permite el acceso de sólo lectura a clientes con su propio ID de usuario que se autentica con AUTH_SYS. El parámetro de sólo lectura permite el acceso de sólo lectura como usuario anónimo con ID de usuario 70 a clientes autenticados mediante cualquier otro tipo de seguridad. El parámetro de lectura y escritura permite acceso de lectura y escritura a cualquier tipo de seguridad, pero en este caso solo se aplica a los clientes ya filtrados por la regla de solo lectura.

Por lo tanto, los clientes #1 y #3 obtienen acceso de lectura y escritura sólo como el usuario anónimo con ID de usuario 70. El cliente #2 obtiene acceso de lectura y escritura con su propio ID de usuario.

El siguiente ejemplo muestra una política de exportación con una `-rwrule none` parámetro:

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule none`
- `-anon 70`

El cliente n.o 1 tiene la dirección IP 10.1.16.207, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con Kerberos v5.

El cliente #2 tiene la dirección IP 10.1.16.211, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con AUTH_SYS.

El cliente #3 tiene la dirección IP 10.1.16.234, envía una solicitud de acceso con el protocolo NFSv3 y no se autentica (es decir, el tipo de seguridad AUTH_NONE).

El protocolo de acceso del cliente y la dirección IP coinciden con los tres clientes. El parámetro de sólo lectura permite el acceso de sólo lectura a clientes con su propio ID de usuario que se autentica con AUTH_SYS. El parámetro de sólo lectura permite el acceso de sólo lectura como usuario anónimo con ID de usuario 70 a clientes autenticados mediante cualquier otro tipo de seguridad. El parámetro de lectura y escritura permite el acceso de lectura y escritura sólo como el usuario anónimo.

Por lo tanto, el cliente #1 y el cliente #3 obtienen acceso de lectura y escritura sólo como el usuario anónimo con el ID de usuario 70. El cliente #2 obtiene acceso de sólo lectura con su propio ID de usuario pero se le deniega el acceso de lectura y escritura.

Cómo los tipos de seguridad de ONTAP determinan los niveles de acceso del cliente NFS

El tipo de seguridad con el que el cliente autenticado desempeña un rol especial en las reglas de exportación. Debe entender la manera en que el tipo de seguridad determina

los niveles de acceso que el cliente obtiene a un volumen o un qtree.

Los tres niveles de acceso posibles son los siguientes:

1. Solo lectura
2. Lectura-escritura
3. Superusuario (para clientes con ID de usuario 0)

Dado que el nivel de acceso por tipo de seguridad se evalúa en este orden, debe observar las siguientes reglas al construir parámetros de nivel de acceso en las reglas de exportación:

Para que un cliente obtenga el nivel de acceso…	**Estos parámetros de acceso deben coincidir con el tipo de seguridad del cliente…**
Usuario normal de solo lectura	Sólo lectura (`-rorule`)
Lectura y escritura normal del usuario	Sólo lectura (`-rorule`) y lectura-escritura (`-rwrule`)
Sólo lectura de superusuario	Sólo lectura (`-rorule`) y. `-superuser`
Lectura y escritura de superusuario	Sólo lectura (`-rorule`) y lectura-escritura (`-rwrule`) y. `-superuser`

A continuación, se muestran tipos de seguridad válidos para cada uno de estos tres parámetros de acceso:

- `any`
- `none`
- `never`

  Este tipo de seguridad no es válido para su uso con el `-superuser` parámetro.

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`
- `sys`

Al hacer coincidir el tipo de seguridad de un cliente con cada uno de los tres parámetros de acceso, hay tres resultados posibles:

Si el tipo de seguridad del cliente…	**A continuación, el cliente…**
Coincide con el especificado en el parámetro access.	Obtiene acceso para ese nivel con su propio ID de usuario.

Si el tipo de seguridad del cliente…	A continuación, el cliente…
No coincide con el especificado, pero el parámetro de acceso incluye la opción `none`.	Obtiene acceso para ese nivel pero como usuario anónimo con el ID de usuario especificado por el `-anon` parámetro.
No coincide con el especificado y el parámetro de acceso no incluye la opción `none`.	No obtiene ningún acceso para ese nivel.Esto no se aplica al `-superuser` parámetro porque siempre incluye `none` incluso cuando no se especifica.

Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule sys,krb5`
- `-superuser krb5`

El cliente #1 tiene la dirección IP 10,1.16,207, tiene el ID de usuario 0, envía una solicitud de acceso mediante el protocolo NFSv3 y se autentica con Kerberos v5.

El cliente #2 tiene la dirección IP 10.1.16.211, tiene el ID de usuario 0, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con AUTH_SYS.

El cliente #3 tiene la dirección IP 10.1.16.234, tiene el ID de usuario 0, envía una solicitud de acceso con el protocolo NFSv3 y no se autentica (AUTH_NONE).

El protocolo de acceso del cliente y la dirección IP coinciden con los tres clientes. El parámetro de solo lectura permite el acceso de solo lectura a todos los clientes independientemente del tipo de seguridad. El parámetro de lectura y escritura permite acceder de lectura y escritura a clientes con su propio ID de usuario que se autentica con AUTH_SYS o Kerberos v5. El parámetro superusuario permite el acceso de superusuario a clientes con ID de usuario 0 que se autentiquen con Kerberos v5.

Por lo tanto, el cliente #1 obtiene acceso de lectura y escritura de superusuario porque coincide con los tres parámetros de acceso. El cliente #2 obtiene acceso de lectura y escritura, pero no acceso de superusuario. El cliente #3 obtiene acceso de sólo lectura pero no acceso de superusuario.

Obtenga información sobre cómo administrar las solicitudes de acceso de superusuario de ONTAP NFS

Cuando configura políticas de exportación, debe tener en cuenta lo que desea que suceda si el sistema de almacenamiento recibe una solicitud de acceso de cliente con ID de usuario 0, lo que significa como superusuario y configure las reglas de exportación según corresponda.

En el mundo UNIX, un usuario con el ID de usuario 0 se conoce como superusuario, normalmente llamado root, que tiene derechos de acceso ilimitados en un sistema. El uso de privilegios de superusuario puede ser peligroso por varias razones, como la violación de la seguridad del sistema y de los datos.

De forma predeterminada, ONTAP asigna los clientes que presentan el ID de usuario 0 al usuario anónimo. Sin embargo, puede especificar el `- superuser` parámetro en las reglas de exportación para determinar cómo manejar los clientes que presentan el ID de usuario 0 en función de su tipo de seguridad. Las siguientes son opciones válidas para `-superuser` el parámetro:

- `any`
- `none`

  Este es el valor predeterminado si no se especifica `-superuser` el parámetro.

- `krb5`
- `ntlm`
- `sys`

Hay dos formas diferentes de manejar los clientes que presentan el ID de usuario 0, dependiendo de la `-superuser` configuración del parámetro:

Si el `-superuser` parámetro y el tipo de seguridad del cliente…	**A continuación, el cliente…**
Coincidencia	Obtiene acceso de superusuario con ID de usuario 0.
No coinciden	Obtiene acceso como usuario anónimo con el ID de usuario especificado por el `-anon` parámetro y sus permisos asignados. Esto es independientemente de si el parámetro de sólo lectura o de lectura y escritura especifica la opción `none`.

Si un cliente se presenta con el ID de usuario 0 para acceder a un volumen con estilo de seguridad NTFS y `-superuser` el parámetro se establece en `none`, ONTAP usará la asignación de nombres para que el usuario anónimo obtenga las credenciales adecuadas.

Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-anon 127`

El cliente #1 tiene la dirección IP 10,1.16,207, tiene el ID de usuario 746, envía una solicitud de acceso mediante el protocolo NFSv3 y se autentica con Kerberos v5.

El cliente #2 tiene la dirección IP 10.1.16.211, tiene el ID de usuario 0, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con AUTH_SYS.

El protocolo de acceso del cliente y la dirección IP coinciden con los dos clientes. El parámetro de solo lectura

permite un acceso de solo lectura a todos los clientes independientemente del tipo de seguridad con el que se autentiquen. Sin embargo, sólo el cliente #1 obtiene acceso de lectura y escritura porque utilizó el tipo de seguridad aprobado Kerberos v5 para autenticar.

El cliente #2 no obtiene acceso de superusuario. En su lugar, se asigna a Anonymous porque `-superuser` no se especifica el parámetro. Esto significa que `none` asigna de forma predeterminada y automáticamente el ID de usuario 0 a anónimo. El cliente #2 sólo obtiene acceso de sólo lectura porque su tipo de seguridad no coincide con el parámetro de lectura y escritura.

Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

El cliente #1 tiene la dirección IP 10,1.16,207, tiene el ID de usuario 0, envía una solicitud de acceso mediante el protocolo NFSv3 y se autentica con Kerberos v5.

El cliente #2 tiene la dirección IP 10.1.16.211, tiene el ID de usuario 0, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con AUTH_SYS.

El protocolo de acceso del cliente y la dirección IP coinciden con los dos clientes. El parámetro de solo lectura permite un acceso de solo lectura a todos los clientes independientemente del tipo de seguridad con el que se autentiquen. Sin embargo, sólo el cliente #1 obtiene acceso de lectura y escritura porque utilizó el tipo de seguridad aprobado Kerberos v5 para autenticar. El cliente n.o 2 no obtiene acceso de lectura/escritura.

La regla de exportación permite el acceso de superusuario para clientes con ID de usuario 0. El cliente #1 obtiene acceso de superusuario porque coincide con el ID de usuario y el tipo de seguridad para los `-superuser` parámetros de solo lectura y. El cliente #2 no obtiene acceso de lectura-escritura ni de superusuario porque su tipo de seguridad no coincide con el parámetro de lectura-escritura o `-superuser` el parámetro. En su lugar, el cliente #2 está asignado al usuario anónimo, que en este caso tiene el ID de usuario 0.

Obtenga información sobre los cachés de políticas de exportación de NFS de ONTAP

Para mejorar el rendimiento del sistema, ONTAP utiliza cachés locales para almacenar información como nombres de host y grupos de redes. De este modo, ONTAP puede procesar reglas de política de exportación más rápidamente que recuperar la información de fuentes externas. Comprender qué son las cachés y qué hacen puede ayudarlo a solucionar los problemas de acceso de los clientes.

Puede configurar políticas de exportación para controlar el acceso de los clientes a las exportaciones de NFS. Cada política de exportación contiene reglas y cada regla contiene parámetros que coincidan con los de los clientes que soliciten acceso. Algunos de estos parámetros requieren que ONTAP se ponga en contacto con un origen externo, como los servidores DNS o NIS, para resolver objetos como nombres de dominio, nombres de host o grupos de red.

Estas comunicaciones con fuentes externas tardan una pequeña cantidad de tiempo. Para aumentar el rendimiento, ONTAP reduce la cantidad de tiempo que se necesita para resolver los objetos de reglas de políticas de exportación almacenando la información localmente en cada nodo en varias cachés.

Nombre de caché	Tipo de información almacenada
Acceso	Asignaciones de clientes a las correspondientes políticas de exportación
Nombre	Se asignan los nombres de usuario UNIX a los correspondientes ID de usuario UNIX
ID	Mapeos de ID de usuario de UNIX a ID de usuario de UNIX correspondientes e ID de grupo de UNIX ampliado
Host	Asignación de los nombres de host a las direcciones IP correspondientes
Grupo de red	Asignaciones de grupos de red a las direcciones IP correspondientes de los miembros
Showmount	Lista de directorios exportados desde el espacio de nombres de SVM

Si cambia información de los servidores de nombres externos de su entorno después de que ONTAP haya recuperado y almacenado localmente, es posible que las cachés contengan información obsoleta. Aunque las actualizaciones de ONTAP se actualizan automáticamente en caché tras ciertos periodos de tiempo, diferentes cachés tienen tiempos y algoritmos de caducidad y actualización diferentes.

Otra posible razón para que las cachés contengan información obsoleta es cuando ONTAP intenta actualizar la información almacenada en caché pero encuentra un error al intentar comunicarse con servidores de nombres. Si esto sucede, ONTAP sigue usando la información actualmente almacenada en la caché local para evitar que se produzca una interrupción del cliente.

Como resultado, las solicitudes de acceso a clientes que se supone que tienen éxito pueden fallar y las solicitudes de acceso de clientes que se supone que fallan se pueden realizar correctamente. Puede ver y purgar manualmente algunas de las cachés de políticas de exportación al solucionar los problemas de acceso de los clientes.

Obtenga más información sobre los cachés de acceso NFS de ONTAP

ONTAP usa una caché de acceso para almacenar los resultados de la evaluación de las reglas de política de exportación para las operaciones de acceso de los clientes a un volumen o un qtree. Esto genera mejoras en el rendimiento porque la información se puede recuperar mucho más rápido de la caché de acceso que pasar por el proceso de evaluación de las reglas de la política de exportación cada vez que un cliente envía una solicitud de I/O.

Siempre que un cliente NFS envía una solicitud de I/o para acceder a los datos de un volumen o un qtree,

ONTAP debe evaluar cada solicitud de I/o para determinar si desea conceder o denegar la solicitud de I/O. Esta evaluación implica la comprobación de cada regla de política de exportación de la política de exportación asociada con el volumen o el qtree. Si la ruta al volumen o qtree implica cruzar uno o más puntos de unión, puede ser necesario realizar esta comprobación en busca de varias políticas de exportación por la ruta.

Tenga en cuenta que esta evaluación se produce para cada solicitud de I/o que se envía desde un cliente NFS, como operaciones de lectura, escritura, lista, copia y otras, y no solo para solicitudes de montaje iniciales.

Una vez que ONTAP ha identificado las reglas de política de exportación aplicables y ha decidido si permitir o denegar la solicitud, ONTAP creará una entrada en la caché de acceso para almacenar dicha información.

Cuando un cliente NFS envía una solicitud de I/o, ONTAP señala la dirección IP del cliente, el ID de la SVM y la política de exportación asociada con el volumen o qtree de destino, y, primero, comprueba la caché de acceso para ver si existe una entrada correspondiente. Si existe una entrada coincidente en la caché de acceso, ONTAP utiliza la información almacenada para permitir o denegar la solicitud de E/S. Si no existe una entrada coincidente, ONTAP pasa por el proceso normal de evaluación de todas las reglas de política aplicables como se ha explicado anteriormente.

Las entradas de la caché de acceso que no se utilizan activamente no se actualizan. Esto reduce la comunicación innecesaria y innecesaria con servicios de nombres externos.

La recuperación de la información de la caché de acceso es mucho más rápida que pasar por todo el proceso de evaluación de las reglas de política de exportación para cada solicitud de I/O. Por lo tanto, el uso de la caché de acceso mejora considerablemente el rendimiento, ya que reduce la sobrecarga de las comprobaciones del acceso de los clientes.

Obtenga información sobre los parámetros de caché de acceso NFS de ONTAP

Varios parámetros controlan los períodos de actualización de las entradas de la caché de acceso. Comprender cómo funcionan estos parámetros le permite modificarlos para ajustar la caché de acceso y equilibrar el rendimiento con lo reciente que es la información almacenada.

La caché de acceso almacena entradas que constan de una o varias reglas de exportación que se aplican a los clientes que intentan acceder a volúmenes o qtrees. Estas entradas se almacenan durante cierto tiempo antes de que se actualicen. El tiempo de actualización viene determinado por los parámetros de la caché de acceso y depende del tipo de entrada de la caché de acceso.

Puede especificar parámetros de caché de acceso para SVM individuales. Esto permite que los parámetros difieren de acuerdo con los requisitos de acceso de la SVM. Las entradas de la caché de acceso que no se utilizan activamente no se actualizan, lo que reduce la comunicación innecesaria y innecesaria con servicios de nombres externos.

Tipo de entrada de la caché de acceso	Descripción	Actualice el periodo en segundos
Entradas positivas	Acceso a las entradas de caché que no han dado lugar a una denegación de acceso a los clientes.	Mínimo: 300 Máximo: 86,400 El valor predeterminado es 3,600

Entradas negativas	Las entradas de caché de acceso que han dado lugar a una denegación de acceso a los clientes.	Mínimo: 60 Máximo: 86,400 El valor predeterminado es 3,600

Ejemplo

Un cliente NFS intenta acceder a un volumen de un clúster de. ONTAP coincide con el cliente con una regla de política de exportación y determina que el cliente obtiene acceso en función de la configuración de la regla de la política de exportación. ONTAP almacena la regla de política de exportación en la caché de acceso como una entrada positiva. De forma predeterminada, ONTAP mantiene la entrada positiva de la caché de acceso durante una hora (3,600 segundos) y, a continuación, actualiza automáticamente la entrada para mantener la información actualizada.

Para evitar que la caché de acceso se llene innecesariamente, hay un parámetro adicional para borrar las entradas existentes de la caché de acceso que no se han utilizado durante un determinado período de tiempo para decidir el acceso de cliente. `-harvest-timeout`Este parámetro tiene un rango permitido de 60 a 2.592.000 segundos y un ajuste predeterminado de 86.400 segundos.

Eliminar políticas de exportación de qtrees de ONTAP NFS

Si decide que ya no desea asignar una política de exportación específica a un qtree, puede eliminar la política de exportación modificando el qtree para que herede la política de exportación del volumen que lo contiene. Puede hacerlo mediante el `volume qtree modify` comando con el `-export-policy` parámetro y una cadena de nombre vacía ('').

Pasos

1. Para quitar una política de exportación de un qtree, introduzca el siguiente comando:

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

2. Compruebe que el qtree se ha modificado en consecuencia:

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

Validar los identificadores de qtree de ONTAP NFS para operaciones con archivos qtree

ONTAP puede realizar una validación adicional opcional de identificadores de qtree. Esta validación garantiza que las solicitudes de operaciones de archivos cliente utilicen un identificador de qtree válido y que los clientes solo puedan mover archivos dentro del mismo qtree. Puede habilitar o deshabilitar esta validación modificando `-validate -qtree-export` el parámetro. Este parámetro está habilitado de forma predeterminada.

Acerca de esta tarea

Este parámetro solo es eficaz cuando se ha asignado una política de exportación directamente a uno o varios qtrees de la máquina virtual de almacenamiento (SVM).

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Ejecute una de las siguientes acciones:

Si desea que la validación de ID de qtree sea…	Introduzca el siguiente comando…
Activado	`vserver nfs modify -vserver vserver_name -validate-qtree-export enabled`
Deshabilitado	`vserver nfs modify -vserver vserver_name -validate-qtree-export disabled`

3. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Restricciones de políticas de exportación y uniones anidadas para volúmenes ONTAP NFS FlexVol

Si ha configurado políticas de exportación para establecer una política menos restrictiva en una unión anidada, pero una política más restrictiva en una unión de nivel superior, puede que no se pueda acceder a la unión de nivel inferior.

Debe asegurarse de que las uniones de nivel superior tienen políticas de exportación menos restrictivas que las uniones de nivel inferior.

Uso de Kerberos con NFS para una mayor seguridad

Compatibilidad de ONTAP NFS con Kerberos

Kerberos proporciona una autenticación segura y segura para aplicaciones cliente/servidor. La autenticación permite verificar las identidades de usuario y proceso a un servidor. En el entorno de ONTAP, Kerberos proporciona autenticación entre máquinas virtuales de almacenamiento (SVM) y clientes NFS.

En ONTAP 9, se admiten las siguientes funcionalidades de Kerberos:

- Autenticación Kerberos 5 con comprobación de integridad (krb5i)

  Krb5i utiliza sumas de comprobación para verificar la integridad de cada mensaje de NFS transferido entre el cliente y el servidor. Esto resulta útil por motivos de seguridad (por ejemplo, para garantizar que los datos no se han alterado) y por motivos de integridad de los datos (por ejemplo, para evitar que se dañen los datos cuando se utilizan NFS en redes no fiables).

- Autenticación Kerberos 5 con comprobación de privacidad (krb5p)

Krb5p utiliza sumas de comprobación para cifrar todo el tráfico entre cliente y servidor. Esto es más seguro y también implica más carga.

- Cifrado AES de 128 bits y 256 bits

  El estándar de cifrado avanzado (AES) es un algoritmo de cifrado para proteger los datos electrónicos. ONTAP admite AES con claves de 128 bits (AES-128) y AES con cifrado de claves de 256 bits (AES-256) para Kerberos para mayor seguridad.

- Configuraciones en dominio de Kerberos a nivel de SVM

  Los administradores de SVM ahora pueden crear configuraciones de dominio de Kerberos en el nivel de SVM. Esto significa que los administradores de SVM ya no tienen que depender del administrador de clúster para la configuración de dominio de Kerberos y pueden crear configuraciones de dominio de Kerberos individuales en un entorno multi-tenancy.

Requisitos para configurar Kerberos con ONTAP NFS

Antes de configurar Kerberos con NFS en el sistema, debe comprobar que determinados elementos de la red y el entorno de almacenamiento están configurados correctamente.

> Los pasos para configurar su entorno dependen de qué versión y tipo del sistema operativo cliente, controlador de dominio, Kerberos, DNS, etc., que usted está usando. La documentación de todas estas variables está fuera del alcance de este documento. Para obtener más información, consulte la documentación correspondiente de cada componente.
>
> Para obtener un ejemplo detallado de cómo configurar ONTAP y Kerberos 5 con NFSv3 y NFSv4 en un entorno mediante hosts de Windows Server 2008 R2 Active Directory y Linux, consulte el informe técnico 4073.

Primero deben configurarse los siguientes elementos:

Requisitos del entorno de red

- Kerberos

  Debe tener una configuración Kerberos en funcionamiento con un centro de distribución de claves (KDC), como Kerberos basado en Windows Active Directory o MIT Kerberos.

  Los servidores NFS deben `nfs` utilizar como componente principal de su principal máquina.

- 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.

- 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.

- Cuentas de usuario

  Cada cliente debe tener una cuenta de usuario en el dominio Kerberos. Los servidores NFS deberán utilizar «'nfs» como componente principal de su principal equipo.

Requisitos del cliente NFS

- NFS

  Cada cliente debe estar configurado correctamente para comunicarse a través de la red mediante NFSv3 o NFSv4.

  Los clientes deben admitir RFC1964 y RFC2203.

- Kerberos

  Cada cliente debe estar configurado correctamente para utilizar la autenticación Kerberos, incluidos los siguientes detalles:

  - El cifrado para la comunicación TGS está activado.

    AES-256 para obtener la máxima seguridad.

  - El tipo de cifrado más seguro para la comunicación TGT está activado.
  - El dominio y el dominio de Kerberos están configurados correctamente.
  - GSS está activado.

    Al utilizar las credenciales de la máquina:

  - No se debe ejecutar `gssd` con el `-n` parámetro.
  - No ejecute `kinit` como usuario root.
- Cada cliente debe utilizar la versión más reciente y actualizada del sistema operativo.

  Esto proporciona la mejor compatibilidad y fiabilidad para el cifrado AES con Kerberos.

- DNS

  Cada cliente debe estar configurado correctamente para utilizar DNS con la resolución de nombres correcta.

- NTP

  Cada cliente debe sincronizarse con el servidor NTP.

- Información sobre el host y el dominio

```
`/etc/hosts` `/etc/resolv.conf`Los archivos y de cada cliente deben
contener el nombre de host e información de DNS correctos,
respectivamente.
```

- Archivos keytab

  Cada cliente debe tener un archivo keytab del KDC. El Reino debe estar en letras mayúsculas. El tipo de cifrado debe ser AES-256 para obtener una seguridad más potente.

- Opcional: Para obtener el mejor rendimiento, los clientes se benefician de tener al menos dos interfaces de red: Una para comunicarse con la red de área local y otra para comunicarse con la red de almacenamiento.

Requisitos del sistema de almacenamiento

- Licencia de NFS

  El sistema de almacenamiento debe tener instalada una licencia NFS válida.

- Licencia CIFS

  La licencia CIFS es opcional. Sólo es necesario comprobar las credenciales de Windows cuando se utiliza la asignación de nombres multiprotocolo. No es necesario en entornos estrictos sólo UNIX.

- SVM

  Debe tener al menos una SVM configurada en el sistema.

- DNS en la SVM

  Debe haber configurado DNS en cada SVM.

- Servidor NFS

  Debe haber configurado NFS en la SVM.

- Cifrado AES

  Para obtener la mayor seguridad, debe configurar el servidor NFS para permitir solo el cifrado AES-256 para Kerberos.

- Servidor SMB

  Si ejecuta un entorno multiprotocolo, debe haber configurado SMB en la SVM. Se requiere el servidor SMB para la asignación de nombres multiprotocolo.

- Volúmenes

  Debe tener un volumen raíz y, al menos, un volumen de datos configurado para que lo utilice la SVM.

- Volumen raíz

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

Nombre	Ajuste
Estilo de seguridad	UNIX
UID	Raíz o ID 0
GID	Raíz o ID 0
Permisos de UNIX	777

A diferencia del volumen raíz, los volúmenes de datos pueden tener cualquier estilo de seguridad.

- Grupos UNIX

  La SVM debe tener configurados los siguientes grupos UNIX:

Nombre del grupo	ID de grupo
daemon	1
raíz	0
pcuser	65534 (creado automáticamente por ONTAP cuando se crea la SVM)

- Usuarios de UNIX

  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 INICIO DE GSS El primer componente del SPN de usuario del cliente NFS se utiliza como usuario.
pcuser	65534	65534	Necesario para el uso multiprotocolo de NFS y CIFS ONTAP lo crea y añade automáticamente al grupo pcuser cuando crea la SVM.

Nombre de usuario	ID de usuario	ID del grupo principal	Comentar
raíz	0	0	Necesario para el montaje

El usuario nfs no es necesario si existe una asignación de nombre Kerberos-UNIX para el SPN del usuario cliente NFS.

- Reglas y políticas de exportación

  Debe haber configurado políticas de exportación con las reglas de exportación necesarias para los volúmenes raíz y de datos y qtrees. Si se accede a todos los volúmenes de SVM mediante Kerberos, puede establecer las opciones de la regla de exportación `-rorule` , `-rwrule` y `-superuser` para el volumen raíz en `krb5` , `krb5i` o `krb5p`.

- Asignación de nombres Kerberos-UNIX

  Si desea que el usuario identificado por el SPN de usuario del cliente NFS tenga permisos raíz, debe crear una asignación de nombre a root.

Información relacionada

"Informe técnico de NetApp 4073: Autenticación unificada segura"

"Herramienta de matriz de interoperabilidad de NetApp"

"Administración del sistema"

"Gestión de almacenamiento lógico"

Especifique el dominio de ID de usuario de ONTAP para NFSv4

Para especificar el dominio de ID de usuario, puede establecer la `-v4-id-domain` opción.

Acerca de esta tarea

De forma predeterminada, ONTAP utiliza el dominio NIS para la asignación del ID de usuario de NFSv4, si hay algún establecido. Si no se establece un dominio NIS, se utiliza el dominio DNS. Es posible que deba establecer el dominio de ID de usuario si, por ejemplo, tiene varios dominios de ID de usuario. El nombre de dominio debe coincidir con la configuración de dominio del controlador de dominio. No es necesaria para NFSv3.

Paso

1. Introduzca el siguiente comando:

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

Configure los servicios de nombres

Obtenga más información sobre la configuración del switch del servicio de nombres NFS de ONTAP

ONTAP almacena la información de configuración del servicio de nombres en una tabla

que es el equivalente al `/etc/nsswitch.conf` archivo en sistemas UNIX. Debe comprender la función de la tabla y cómo la utiliza ONTAP para poder configurarla de forma adecuada para su entorno.

La tabla de conmutador de servicio de nombres ONTAP determina qué orígenes de servicio de nombres consulta ONTAP para recuperar información de un determinado tipo de información del servicio de nombres. ONTAP mantiene una tabla de switch de servicio de nombres independiente para cada SVM.

Tipos de base de datos

La tabla almacena una lista de servicios de nombres independiente para cada uno de los siguientes tipos de base de datos:

Tipo de base de datos	Define orígenes de servicio de nombres para…	Los orígenes válidos son…
hosts	Conversión de nombres de host a direcciones IP	archivos, dns
grupo	Búsqueda de información de grupo de usuarios	archivos, nis, ldap
passwd	Búsqueda de información de usuario	archivos, nis, ldap
grupo de red	Buscando información de netgroup	archivos, nis, ldap
mapa de nombres	Asignando los nombres de usuario	archivos, ldap

Tipos de origen

Los orígenes especifican el nombre de origen de servicio que se utilizará para recuperar la información adecuada.

Especificar tipo de origen…	Para buscar información en…	Administrado por las familias de comandos…

archivos	Archivos de origen local	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

Especificar tipo de origen…	Para buscar información en…	Administrado por las familias de comandos…
nis	Servidores NIS externos tal como se especifica en la configuración de dominio NIS de la SVM	`vserver services name-service nis-domain`
ldap	Servidores LDAP externos tal como se especifica en la configuración del cliente LDAP de la SVM	`vserver services name-service ldap`
dns	Servidores DNS externos como se especifica en la configuración de DNS de la SVM	`vserver services name-service dns`

Aunque tenga pensado utilizar NIS o LDAP para el acceso a los datos y la autenticación de administración de SVM, deberá incluir `files` y configurar usuarios locales como recuperación en caso de que falle la autenticación NIS o LDAP.

Protocolos utilizados para acceder a fuentes externas

Para acceder a los servidores de fuentes externas, ONTAP utiliza los siguientes protocolos:

Fuente externa del servicio de nombres	Protocolo utilizado para acceder
NIS	UDP
DNS	UDP
LDAP	TCP

Ejemplo

En el ejemplo siguiente se muestra el nombre de configuración del switch de servicio para la SVM svm svm_1:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                 Source
Vserver         Database         Order
--------------- ------------   ---------
svm_1           hosts          files,
                               dns
svm_1           group          files
svm_1           passwd         files
svm_1           netgroup       nis,
                               files
```

Para buscar direcciones IP para hosts, ONTAP consulta primero los archivos de origen local. Si la consulta no

devuelve ningún resultado, los servidores DNS se comprueban a continuación.

Para buscar información de usuarios o grupos, ONTAP sólo consulta archivos de fuentes locales. Si la consulta no devuelve ningún resultado, la búsqueda fallará.

Para buscar información de grupos de red, ONTAP consulta primero los servidores NIS externos. Si la consulta no devuelve ningún resultado, el archivo de netgroup local se activa a continuación.

No hay entradas del servicio de nombres para la asignación de nombres en la tabla de la SVM svm svm_1. Por lo tanto, ONTAP sólo consulta archivos de origen local de forma predeterminada.

Información relacionada

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

Utilice LDAP

Obtenga más información sobre LDAP para SVM NFS de ONTAP

Un servidor LDAP (protocolo ligero de acceso a directorios) le permite mantener la información de usuario de forma centralizada. Si almacena su base de datos de usuario en un servidor LDAP del entorno, puede configurar el sistema de almacenamiento para buscar información de usuario en su base de datos LDAP existente.

- 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 utiliza LDAPS, el servidor LDAP debe estar habilitado para TLS o para SSL en ONTAP 9.5 y versiones posteriores. SSL no es compatible con ONTAP 9.4 - 9.0.
        - 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 ser las mismas para autenticarse cuando `--bind-as-cifs-server` se definen 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)

- A partir de ONTAP 9.11,1, puede usar "Utilice el enlace rápido LDAP para la autenticación nsswitch para SVM NFS de ONTAP."
- 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.

Para obtener más información, consulte "Informe técnico de NetApp 4835: Cómo configurar LDAP en ONTAP".

Obtenga información sobre la firma y el sellado LDAP para SVM NFS de ONTAP

A partir de ONTAP 9, puede configurar la firma y el sellado para habilitar la seguridad de la sesión LDAP en consultas a un servidor de Active Directory (AD). Debe configurar los ajustes de seguridad del servidor NFS en la máquina virtual de almacenamiento (SVM) para corresponder a los del servidor LDAP.

La firma comprueba la integridad de la carga de datos LDAP mediante una tecnología de clave secreta. El sellado cifra la carga de datos LDAP para impedir la transmisión de información confidencial en texto sin cifrar. Una opción *LDAP Security Level* indica si es necesario firmar, firmar y sellar el tráfico LDAP o no. El valor por defecto es `none`. test

La firma y el sellado LDAP en el tráfico SMB se habilitan en la SVM con `-session-security-for-ad-ldap` la opción del `vserver cifs security modify` comando.

Obtenga más información sobre LDAPS para SVM NFS de ONTAP

Debe comprender ciertos términos y conceptos sobre cómo ONTAP protege la comunicación LDAP. ONTAP puede usar START TLS o LDAPS para configurar sesiones autenticadas entre servidores LDAP integrados de Active Directory o servidores LDAP basados en UNIX.

Terminología

Existen ciertos términos que se deben entender de qué manera ONTAP utiliza LDAPS para proteger la comunicación de LDAP.

- **LDAP**

  (Protocolo ligero de acceso a directorios) Protocolo para acceder y administrar directorios de información. LDAP se utiliza como directorio de información para almacenar objetos como usuarios, grupos y netgroups. LDAP también proporciona servicios de directorio que administran estos objetos y satisfacen las solicitudes LDAP de los clientes LDAP.

- **SSL**

  (Capa de sockets seguros) Protocolo desarrollado para enviar información de forma segura a través de Internet. SSL es compatible con ONTAP 9 y posterior, pero ha sido anticuado a favor de TLS.

- **TLS**

  (Transport Layer Security) Protocolo de seguimiento de estándares IETF basado en las especificaciones anteriores de SSL. Es el sucesor de SSL. ONTAP 9,5 y versiones posteriores es compatible con TLS.

- **LDAPS (LDAP sobre SSL o TLS)**

  Protocolo que utiliza TLS o SSL para proteger la comunicación entre clientes LDAP y servidores LDAP. Los términos *ldap sobre SSL* y *ldap sobre TLS* a veces se utilizan indistintamente. ONTAP 9,5 y versiones posteriores es compatible con LDAPS.

  - En ONTAP 9.8-9.5, LDAPS solo se puede habilitar en el puerto 636. Para ello, utilice el `-use-ldaps-for-ad-ldap` parámetro con el `vserver cifs security modify` dominio.
  - A partir de ONTAP 9.9.1, LDAPS puede habilitar LDAPS en cualquier puerto, aunque el puerto 636 sigue siendo el predeterminado. Para ello, establezca el `-ldaps-enabled` parámetro en `true` y especifique el `-port` parámetro deseado. Obtenga más información sobre `vserver services name-service ldap client create` en el "Referencia de comandos del ONTAP".

  Se trata de una práctica recomendada de NetApp para usar Start TLS en lugar de LDAPS.

- **Iniciar TLS**

(También conocido como *start_tls*, *STARTTLS* y *StartTLS*) un mecanismo para proporcionar una comunicación segura mediante el uso de los protocolos TLS.

ONTAP utiliza STARTTLS para garantizar la comunicación LDAP y utiliza el puerto LDAP predeterminado (389) para comunicarse con el servidor LDAP. El servidor LDAP debe configurarse para permitir conexiones a través del puerto LDAP 389; de lo contrario, se producirá un error en las conexiones LDAP TLS desde la SVM al servidor LDAP.

Cómo utiliza ONTAP LDAPS

ONTAP admite la autenticación del servidor TLS, lo que permite que el cliente LDAP de SVM confirme la identidad del servidor LDAP durante la operación de enlace. Los clientes LDAP habilitados para TLS pueden utilizar técnicas estándar de criptografía de clave pública para comprobar que el certificado y el ID público de un servidor son válidos y que han sido emitidos por una entidad emisora de certificados (CA) que aparece en la lista de entidades emisoras de certificados de confianza del cliente.

LDAP admite STARTTLS para cifrar las comunicaciones mediante TLS. STARTTLS comienza como una conexión de texto sin formato a través del puerto LDAP estándar (389), y esa conexión se actualiza a TLS.

ONTAP admite lo siguiente:

- LDAPS para tráfico relacionado con SMB entre los servidores LDAP integrados de Active Directory y la SVM
- LDAPS para el tráfico LDAP para la asignación de nombres y otra información de UNIX

  Los servidores LDAP integrados en Active Directory o los servidores LDAP basados en UNIX se pueden utilizar para almacenar información para la asignación de nombres LDAP y otra información UNIX, como usuarios, grupos y netgroups.

- Certificados de CA raíz autofirmados

  Cuando se utiliza un LDAP integrado de Active Directory, el certificado raíz autofirmado se genera cuando el servicio de certificados de Windows Server está instalado en el dominio. Cuando se utiliza un servidor LDAP basado en UNIX para asignar nombres LDAP, se genera el certificado raíz autofirmado y se guarda mediante medios adecuados para esa aplicación LDAP.

De forma predeterminada, LDAPS está desactivado.

Habilitar la compatibilidad con LDAP RFC2307bis para SVM NFS de ONTAP

Si desea utilizar LDAP y necesita la capacidad adicional para utilizar pertenencias a grupos anidados, puede configurar ONTAP para habilitar la compatibilidad con RFC2307bis LDAP.

Antes de empezar

Debe haber creado una copia de uno de los esquemas de cliente LDAP predeterminados que desea utilizar.

Acerca de esta tarea

En los esquemas de cliente LDAP, los objetos de grupo utilizan el atributo memberUid. Este atributo puede contener varios valores y enumera los nombres de los usuarios que pertenecen a ese grupo. En los esquemas de cliente LDAP habilitados para RFC2307bis, los objetos de grupo utilizan el atributo uniqueMember. Este atributo puede contener el nombre completo (DN) de otro objeto del directorio LDAP. Esto le permite utilizar grupos anidados porque los grupos pueden tener otros grupos como miembros.

El usuario no debe ser miembro de más de 256 grupos, incluidos los grupos anidados. ONTAP ignora los grupos por encima del límite de 256 grupos.

De forma predeterminada, la compatibilidad con RFC2307bis está desactivada.

> La compatibilidad con RFC2307bis se habilita automáticamente en ONTAP cuando se crea un cliente LDAP con el esquema MS-AD-BIS.

Para obtener más información, consulte "Informe técnico de NetApp 4835: Cómo configurar LDAP en ONTAP".

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Modifique el esquema de cliente LDAP RFC2307 copiado para habilitar la compatibilidad con RFC2307bis:

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   -schema schema-name -enable-rfc2307bis true
   ```

3. Modifique el esquema para que coincida con la clase de objeto admitida en el servidor LDAP:

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -group-of-unique-names-object-class object_class
   ```

4. Modifique el esquema para que coincida con el nombre de atributo admitido en el servidor LDAP:

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -unique-member-attribute attribute_name
   ```

5. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Opciones de configuración de ONTAP NFS para búsquedas en directorios LDAP

Puede optimizar las búsquedas de directorios LDAP, incluida la información de usuario, grupo y grupo de red, configurando el cliente LDAP de ONTAP para que se conecte a servidores LDAP de la forma más adecuada para su entorno. Es necesario entender cuándo son suficientes los valores predeterminados de la base LDAP y de la búsqueda de ámbito y qué parámetros especificar cuando los valores personalizados son más apropiados.

Las opciones de búsqueda de clientes LDAP para información de usuarios, grupos y netgroup pueden ayudar a evitar consultas LDAP que han fallado y, por lo tanto, permitir que el cliente acceda a los sistemas de almacenamiento con errores. También ayudan a garantizar que las búsquedas sean lo más eficientes posible para evitar problemas de rendimiento de los clientes.

Valores de búsqueda base y ámbito predeterminados

La base LDAP es el DN base predeterminado que utiliza el cliente LDAP para realizar consultas LDAP. Todas las búsquedas, incluidas las búsquedas de usuario, grupo y netgroup, se realizan utilizando el DN base. Esta opción es apropiada cuando el directorio LDAP es relativamente pequeño y todas las entradas relevantes se encuentran en el mismo DN.

Si no especifica un DN base personalizado, el valor por defecto es `root`. Esto significa que cada consulta busca en todo el directorio. A pesar de que esto maximiza las posibilidades de éxito de la consulta LDAP, puede resultar ineficiente y producir una reducción significativa del rendimiento con grandes directorios LDAP.

El ámbito de base LDAP es el ámbito de búsqueda predeterminado que utiliza el cliente LDAP para realizar consultas LDAP. Todas las búsquedas, incluidas las de usuario, grupo y netgroup, se realizan utilizando el ámbito base. Determina si la consulta LDAP busca sólo la entrada con nombre, las entradas de un nivel por debajo del DN o el subárbol entero por debajo del DN.

Si no especifica un ámbito base personalizado, el valor por defecto es `subtree`. Esto significa que cada consulta busca todo el subárbol que se encuentra debajo del DN. A pesar de que esto maximiza las posibilidades de éxito de la consulta LDAP, puede resultar ineficiente y producir una reducción significativa del rendimiento con grandes directorios LDAP.

Valores de búsqueda de base y ámbito personalizados

Opcionalmente, puede especificar valores de base y ámbito independientes para búsquedas de usuarios, grupos y grupos de red. Limitar la base de búsqueda y el ámbito de las consultas de esta manera puede mejorar significativamente el rendimiento porque limita la búsqueda a una subsección más pequeña del directorio LDAP.

Si se especifican valores de base y ámbito personalizados, se reemplazan la base de búsqueda y el ámbito predeterminados generales para las búsquedas de usuarios, grupos y grupos de red. Los parámetros para especificar valores de base y ámbito personalizados están disponibles en el nivel de privilegio avanzado.

Parámetro de cliente LDAP…	Especifica el valor personalizado…
`-base-dn`	DN base para todas las búsquedas LDAP. Se pueden introducir varios valores si es necesario (por ejemplo, si la búsqueda de referencias LDAP está habilitada en ONTAP 9.5 y versiones posteriores).
`-base-scope`	Ámbito base para todas las búsquedas LDAP.
`-user-dn`	DN base para todas las búsquedas de usuarios LDAP. Este parámetro también se aplica a las búsquedas de asignación de nombres de usuario.
`-user-scope`	Ámbito base para todas las búsquedas de usuarios LDAP. Este parámetro también se aplica a las búsquedas de asignación de nombres de usuario.
`-group-dn`	DN base para todas las búsquedas de grupos LDAP.
`-group-scope`	Ámbito base para todas las búsquedas de grupos LDAP.

`-netgroup-dn`	DN base para todas las búsquedas de grupos de redes LDAP.
`-netgroup-scope`	Ámbito base para todas las búsquedas de grupos de redes LDAP.

Varios valores DN base personalizados

Si su estructura de directorios LDAP es más compleja, puede ser necesario especificar varios DNS base para buscar varias partes del directorio LDAP para cierta información. Puede especificar varios DNS para los parámetros de DN de usuario, grupo y grupo de red separándolos con punto y coma (;) y encerrando toda la lista de búsqueda de DN con comillas dobles ("). Si un DN contiene un punto y coma, debe agregar un carácter de escape (\) inmediatamente antes del punto y coma en el DN.

Tenga en cuenta que el ámbito se aplica a toda la lista de DNS especificada para el parámetro correspondiente. Por ejemplo, si especifica una lista de tres DNS de usuario y subárbol diferentes para el ámbito de usuario, el usuario LDAP buscará en todo el subárbol para cada uno de los tres DNS especificados.

A partir de ONTAP 9.5, también puede especificar LDAP *referenciación persiguiendo*, lo que permite al cliente LDAP de ONTAP remitir solicitudes de búsqueda a otros servidores LDAP si el servidor LDAP principal no devuelve una respuesta de referencia LDAP. El cliente utiliza esos datos de referencia para recuperar el objeto de destino del servidor descrito en los datos de referencia. Para buscar objetos presentes en los servidores LDAP a los que se hace referencia, se puede agregar la base-dn de los objetos a los que se hace referencia a base-dn como parte de la configuración del cliente LDAP. Sin embargo, los objetos referidos sólo se consultan cuando la búsqueda de referencias está habilitada (mediante `-referral-enabled true` la opción) durante la creación o modificación del cliente LDAP.

Filtros de búsqueda LDAP personalizados

Puede utilizar el parámetro de opción de configuración LDAP para crear un filtro de búsqueda personalizado. `-group-membership-filter`El parámetro especifica el filtro de búsqueda que se utilizará al buscar la pertenencia a un grupo desde un servidor LDAP.

Un ejemplo de filtros válidos son:

```
(cn=*99), (cn=1*), (|(cn=*22)(cn=*33))
```

Más información sobre "Cómo configurar LDAP en ONTAP".

Mejorar el rendimiento de las búsquedas de grupos de redes por host del directorio LDAP para SVM NFS de ONTAP

Si el entorno LDAP está configurado para permitir búsquedas de netgroup-by-host, puede configurar ONTAP para aprovechar esta característica y realizar búsquedas de netgroup-by-host. Esto puede acelerar significativamente las búsquedas de netgroup y reducir posibles problemas de acceso de clientes NFS debido a la latencia durante las búsquedas de netgroup.

Antes de empezar

El directorio LDAP debe contener un `netgroup.byhost` mapa.

Los servidores DNS deben contener registros de búsqueda de reenvío (A) e inverso (PTR) para clientes NFS.

Al especificar direcciones IPv6 en grupos de red, siempre debe acortar y comprimir cada dirección como se especifica en RFC 5952.

Acerca de esta tarea

Los servidores NIS almacenan información de grupo de red en tres mapas separados denominados `netgroup`, `netgroup.byuser` y `netgroup.byhost`. El objetivo de `netgroup.byuser` `netgroup.byhost` los mapas y es acelerar las búsquedas de grupos de red. ONTAP puede realizar búsquedas de netgroup-by-host en servidores NIS para mejorar los tiempos de respuesta de montaje.

De forma predeterminada, los directorios LDAP no tienen un `netgroup.byhost` mapa como los servidores NIS. Sin embargo, es posible, con la ayuda de herramientas de terceros, importar un `netgroup.byhost` mapa NIS en directorios LDAP para permitir búsquedas rápidas de netgroup por host. Si ha configurado su entorno LDAP para permitir búsquedas netgroup por host, puede configurar el cliente LDAP de ONTAP con `netgroup.byhost` el nombre de la asignación, DN y ámbito de búsqueda para realizar búsquedas netgroup por host más rápidas.

Al recibir los resultados de las búsquedas de netgroup-by-host con mayor rapidez, ONTAP procesa las reglas de exportación con mayor rapidez cuando los clientes NFS solicitan acceso a las exportaciones. Esto reduce la posibilidad de retrasos en el acceso debido a problemas de latencia de búsqueda en netgroup.

Pasos

1. Obtenga el nombre completo completo exacto de la `netgroup.byhost` asignación NIS que importó en su directorio LDAP.

   El DN de mapa puede variar en función de la herramienta de terceros que haya utilizado para la importación. Para obtener el mejor rendimiento, debe especificar el DN exacto del mapa.

2. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
3. Habilite las búsquedas netgroup por host en la configuración de cliente LDAP de la máquina virtual de almacenamiento (SVM): `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost-dn netgroup-by-host_map_distinguished_name -netgroup-byhost -scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled` {`true` `false`} Permite o desactiva la búsqueda netgroup-by-host para directorios LDAP. El valor predeterminado es `false`.

   `-netgroup-byhost-dn` `netgroup-by-host_map_distinguished_name` Especifica el nombre distintivo del `netgroup.byhost` mapa en el directorio LDAP. Reemplaza el DN base para las búsquedas de netgroup-by-host. Si no se especifica este parámetro, ONTAP utiliza el DN base.

   `-netgroup-byhost-scope` {`base`|`onelevel` `subtree`} especifica el ámbito de búsqueda para las búsquedas netgroup-by-host. Si no especifica este parámetro, el valor por defecto es `subtree`.

   Si la configuración del cliente LDAP aún no existe, puede habilitar las búsquedas netgroup-by-host especificando estos parámetros al crear una nueva configuración de cliente LDAP con `vserver services name-service ldap client create` el comando.

   El `-ldap-servers` El campo reemplaza el `-servers` campo. Puedes utilizar el `-ldap-servers` campo para especificar un nombre de host o una dirección IP para el servidor LDAP.

4. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Ejemplo

El siguiente comando modifica la configuración de cliente LDAP existente denominada «`ldap_corp » para permitir las búsquedas netgroup-by-host utilizando el `netgroup.byhost` mapa denominado «nisMapName=«netgroup.byhost»,dc=corp,dc=example,dc=com» y el ámbito de búsqueda predeterminado `subtree` :

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

Después de terminar

Los `netgroup.byhost` `netgroup` mapas y del directorio se deben mantener sincronizados en todo momento para evitar problemas de acceso de los clientes.

Información relacionada

"RFC de IETF 5952: Recomendación para la representación de texto de direcciones IPv6"

Utilice el enlace rápido LDAP para la autenticación nsswitch para SVM NFS de ONTAP

A partir de ONTAP 9.11.1, puede aprovechar la funcionalidad LDAP *fast bind* (también conocida como *concurrente bind*) para obtener solicitudes de autenticación de clientes más rápidas y sencillas. Para utilizar esta funcionalidad, el servidor LDAP debe admitir la funcionalidad de enlace rápido.

Acerca de esta tarea

Sin enlace rápido, ONTAP utiliza la vinculación simple de LDAP para autenticar usuarios administradores con el servidor LDAP. Con este método de autenticación, ONTAP envía un nombre de usuario o de grupo al servidor LDAP, recibe la contraseña hash almacenada y compara el código hash del servidor con la contraseña hash generada localmente desde la contraseña de usuario. Si son idénticas, ONTAP otorga permiso de inicio de sesión.

Con la funcionalidad de enlace rápido, ONTAP sólo envía credenciales de usuario (nombre de usuario y contraseña) al servidor LDAP a través de una conexión segura. A continuación, el servidor LDAP valida estas credenciales y le indica a ONTAP que conceda permisos de inicio de sesión.

Una ventaja de enlace rápido es que no es necesario que ONTAP admita todos los nuevos algoritmos de hash compatibles con los servidores LDAP, ya que el servidor LDAP realiza hash de contraseñas.

"Aprenda sobre el uso de FAST BIND."

Puede utilizar las configuraciones de cliente LDAP existentes para enlace rápido LDAP. Sin embargo, se recomienda encarecidamente que el cliente LDAP esté configurado para TLS o LDAPS; de lo contrario, la contraseña se envía por el cable en texto sin formato.

Para habilitar el enlace rápido de LDAP en un entorno ONTAP, debe cumplir con estos requisitos:

- Los usuarios del administrador de ONTAP deben estar configurados en un servidor LDAP que admita el enlace rápido.

- La SVM de ONTAP debe configurarse para LDAP en la base de datos de switches de servicios de nombres (nsswitch).
- Las cuentas de usuario y de grupo admin de ONTAP deben configurarse para la autenticación nsswitch mediante fast bind.

Pasos

1. Confirme con el administrador LDAP que el enlace rápido LDAP es compatible con el servidor LDAP.
2. Asegúrese de que las credenciales de usuario administrador de ONTAP estén configuradas en el servidor LDAP.
3. Confirmar que el administrador o la SVM de datos están configurados correctamente para el enlace LDAP rápido.

   a. Para confirmar que el servidor de enlace rápido LDAP aparece en la configuración de cliente LDAP, introduzca:

      `vserver services name-service ldap client show`

      "Obtenga información acerca de la configuración del cliente LDAP."

   b. Para confirmar que `ldap` es uno de los orígenes configurados para la `passwd` base de datos nsswitch, introduzca:

      `vserver services name-service ns-switch show`

   "Más información sobre la configuración de nsswitch."

4. Asegúrese de que los usuarios de administrador se autenticen con nsswitch y de que la autenticación de enlace rápido LDAP esté habilitada en sus cuentas.

   - Para los usuarios existentes, introduzca `security login modify` y verifique los siguientes valores de parámetros:

     `-authentication-method nsswitch`

     `-is-ldap-fastbind true`

   Obtenga más información sobre `security login modify` en el "Referencia de comandos del ONTAP".

   - Para nuevos usuarios administradores, consulte "Active el acceso a la cuenta de ONTAP LDAP o NIS".

Mostrar estadísticas LDAP para SVM NFS de ONTAP

Puede mostrar estadísticas LDAP para máquinas virtuales de almacenamiento (SVM) en un sistema de almacenamiento para monitorear el rendimiento y diagnosticar problemas.

Antes de empezar

- Debe haber configurado un cliente LDAP en la SVM.
- Debe haber identificado los objetos LDAP desde los cuales se pueden ver datos.

Paso

1. Vea los datos de rendimiento para los objetos de contador:

   ```
   statistics show
   ```

Ejemplos

El siguiente ejemplo muestra estadísticas para la muestra denominada **smpl_1** para los contadores: avg_PROCESSOR_OCUPY y cpu_OCUPY

```
cluster1::*> statistics start -object system -counter
avg_processor_busy|cpu_busy -sample-id smpl_1
Statistics collection is being started for Sample-id: smpl_1

cluster1::*> statistics stop -sample-id smpl_1
Statistics collection is being stopped for Sample-id: smpl_1

cluster1::*> statistics show -sample-id smpl_1
Object: system
Instance: cluster
Start-time: 8/2/2012 18:27:53
End-time: 8/2/2012 18:27:56
Cluster: cluster1
   Counter                                                     Value
   -------------------------------- --------------------------------
   avg_processor_busy                                             6%
   cpu_busy
```

Información relacionada

- "Las estadísticas muestran"
- "Las estadísticas comienzan"
- "las estadísticas se detienen"

Configurar las asignaciones de nombres

Obtenga información sobre la configuración de asignación de nombres para SVM de ONTAP NAS

ONTAP utiliza la asignación de nombres para asignar identidades SMB a identidades UNIX, identidades Kerberos a identidades UNIX e identidades UNIX a identidades SMB. Necesita esta información para obtener credenciales de usuario y proporcionar un acceso adecuado a los archivos independientemente de si se están conectando desde un cliente NFS o un cliente SMB.

Existen dos excepciones en las que no es necesario utilizar la asignación de nombres:

- Configura un entorno UNIX puro y no planea usar el acceso SMB o el estilo de seguridad NTFS en los volúmenes.
- En su lugar, puede configurar el usuario predeterminado que se utilizará.

En este escenario, no es necesario asignar nombres porque en lugar de asignar cada credencial de cliente individual todas las credenciales de cliente se asignan al mismo usuario predeterminado.

Tenga en cuenta que sólo puede utilizar la asignación de nombres para usuarios, no para grupos.

Sin embargo, puede asignar un grupo de usuarios individuales a un usuario específico. Por ejemplo, puede asignar todos los usuarios de AD que comiencen o terminen con la palabra SALES a un usuario UNIX específico y al UID del usuario.

Obtenga información sobre las asignaciones de nombres para SVM de ONTAP NAS

Cuando ONTAP tiene que asignar credenciales para un usuario, primero comprueba la base de datos de asignación de nombres local y el servidor LDAP para buscar una asignación existente. Si comprueba uno o ambos y en qué orden se determina mediante la configuración del servicio de nombres de la SVM.

- Para la asignación de Windows a UNIX

  Si no se encuentra ninguna asignación, ONTAP comprueba si el nombre de usuario de Windows en minúsculas es un nombre de usuario válido en el dominio UNIX. Si esto no funciona, utiliza el usuario UNIX predeterminado siempre que esté configurado. Si el usuario UNIX predeterminado no está configurado y ONTAP no puede obtener una asignación de esta manera, se produce un error en la asignación y se devuelve un error.

- De asignación de UNIX a Windows

  Si no se encuentra ninguna asignación, ONTAP intenta encontrar una cuenta de Windows que coincida con el nombre UNIX en el dominio SMB. Si esto no funciona, utiliza el usuario SMB predeterminado, siempre que esté configurado. Si el usuario SMB predeterminado no está configurado y ONTAP no puede obtener una asignación de esta manera, se produce un error en la asignación y se devuelve un error.

Las cuentas de equipo se asignan al usuario UNIX predeterminado especificado de forma predeterminada. Si no se especifica ningún usuario UNIX predeterminado, las asignaciones de cuentas de equipo fallan.

- A partir de ONTAP 9.5, puede asignar cuentas de equipo a usuarios distintos del usuario UNIX predeterminado.
- En ONTAP 9.4 y versiones anteriores, no es posible asignar cuentas de equipo a otros usuarios.

  Incluso si se definen las asignaciones de nombre para las cuentas de equipo, las asignaciones se omiten.

Búsquedas multidominio para asignaciones de nombres de usuario de UNIX a Windows en SVM NAS de ONTAP

ONTAP admite las búsquedas multidominio al asignar usuarios de UNIX a usuarios de Windows. Se buscan todos los dominios de confianza detectados para que coincidan con el patrón de reemplazo hasta que se devuelva un resultado coincidente. También puede configurar una lista de dominios de confianza preferidos, que se utiliza en lugar de la lista de dominios de confianza detectados y se busca en orden hasta que se devuelve un resultado coincidente.

Cómo afectan las confianzas de dominio a las búsquedas de asignación de nombres de usuario de UNIX a Windows

Para comprender cómo funciona la asignación de nombres de usuario multidominio, debe comprender cómo funcionan las relaciones de confianza de dominios con ONTAP. Las relaciones de confianza de Active Directory con el dominio raíz del servidor SMB pueden ser una confianza bidireccional o pueden ser uno de los dos tipos de confianzas unidireccionales, ya sea una confianza entrante o una confianza saliente. El dominio inicial es el dominio al que pertenece el servidor SMB en la SVM.

- *Confianza bidireccional*

  Con confianzas bidireccionales, ambos dominios confían entre sí. Si el dominio principal del servidor SMB tiene una confianza bidireccional con otro dominio, el dominio principal puede autenticar y autorizar a un usuario que pertenece al dominio de confianza y viceversa.

  Las búsquedas de asignación de nombres de usuario de UNIX a usuario de Windows sólo se pueden realizar en dominios con relaciones de confianza bidireccionales entre el dominio principal y el otro dominio.

- *Confianza saliente*

  Con una confianza saliente, el dominio principal confía en el otro dominio. En este caso, el dominio principal puede autenticar y autorizar a un usuario que pertenezca al dominio de confianza saliente.

  Se realiza una búsqueda en un dominio con una confianza saliente con el dominio principal al realizar búsquedas de asignación de nombres de usuario de UNIX a usuario de Windows.

- *Confianza entrante*

  Con una confianza entrante, el otro dominio confía en el dominio raíz del servidor SMB. En este caso, el dominio principal no puede autenticar ni autorizar a un usuario que pertenezca al dominio de confianza entrante.

  Se busca un dominio con una confianza entrante con el dominio principal cuando se realizan búsquedas de asignación de nombres de usuario de UNIX a nombre de usuario de Windows.

Cómo se utilizan los comodines (*) para configurar las búsquedas multidominio para la asignación de nombres

Las búsquedas de asignación de nombres multidominio se facilitan mediante el uso de caracteres comodín en la sección de dominio del nombre de usuario de Windows. En la siguiente tabla se muestra cómo utilizar comodines en la parte de dominio de una entrada de asignación de nombres para habilitar las búsquedas multidominio:

Patrón	Sustitución	Resultado
raíz	{asterisco}{barra diagonal inversa}{barra invertida}administrador	El usuario UNIX «'root'» está asignado al usuario denominado «'Administrator'». Todos los dominios de confianza se buscan en orden hasta que se encuentre el primer usuario coincidente denominado «'Administrator'».

Patrón	Sustitución	Resultado
*	{asterisco}{barra diagonal inversa}{barra diagonal inversa}{asterisco}	Los usuarios UNIX válidos se asignan a los usuarios de Windows correspondientes. Todos los dominios de confianza se buscan en orden hasta que se encuentre el primer usuario que coincida con ese nombre. El patrón {asterisco}{barra diagonal inversa}{barra diagonal inversa}{asterisco} sólo es válido para la asignación de nombres de UNIX a Windows, no al revés.

Cómo se realizan las búsquedas de nombres multidominio

Puede elegir uno de los dos métodos para determinar la lista de dominios de confianza utilizados para las búsquedas de nombres multidominio:

- Utilice la lista de confianza bidireccional detectada automáticamente compilada por ONTAP
- Utilice la lista de dominios de confianza preferida que compila

Si un usuario de UNIX se asigna a un usuario de Windows con un comodín utilizado para la sección de dominio del nombre de usuario, se busca al usuario de Windows en todos los dominios de confianza de la siguiente manera:

- Si se configura una lista de dominio de confianza preferido, el usuario de Windows asignado se busca sólo en esta lista de búsqueda, en orden.
- Si no se configura una lista preferida de dominios de confianza, se busca al usuario de Windows en todos los dominios de confianza bidireccionales del dominio principal.
- Si no hay dominios de confianza bidireccional para el dominio principal, se busca al usuario en el dominio principal.

Si un usuario de UNIX está asignado a un usuario de Windows sin una sección de dominio en el nombre de usuario, se busca al usuario de Windows en el dominio principal.

Reglas de conversión de asignación de nombres para SVM de ONTAP NAS

Un sistema ONTAP mantiene un conjunto de reglas de conversión para cada SVM. Cada regla consta de dos piezas: Un *pattern* y un *substitut*. Las conversiones comienzan al principio de la lista apropiada y realizan una sustitución basada en la primera regla de coincidencia. El patrón es una expresión regular de estilo UNIX. El reemplazo es una cadena que contiene secuencias de escape que representan subexpresiones del patrón,

como en el `sed` programa UNIX.

Crear asignaciones de nombres para SVM de ONTAP NAS

Puede utilizar `vserver name-mapping create` el comando para crear una asignación de nombres. Se usan asignaciones de nombres para habilitar a los usuarios de Windows a fin de acceder a los volúmenes de estilo de seguridad de UNIX y al revés.

Acerca de esta tarea

Con cada SVM, ONTAP admite hasta 12,500 asignaciones de nombres para cada dirección.

Paso

1. Crear una asignación de nombres:

```
vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-
unix|unix-win} -position integer -pattern text -replacement text
```

> Las `-pattern` `-replacement` declaraciones y se pueden formular como expresiones regulares. También puede utilizar `-replacement` la sentencia para denegar explícitamente una asignación al usuario mediante la cadena de sustitución nula `" "` (el carácter de espacio). Obtenga más información sobre `vserver name-mapping create` en el "Referencia de comandos del ONTAP".

Cuando se crean las asignaciones de Windows a UNIX, todos los clientes de SMB que tengan conexiones abiertas al sistema ONTAP en el momento en el que se creen las nuevas asignaciones deben cerrar e iniciar sesión para ver las nuevas asignaciones.

Ejemplos

El siguiente comando crea un mapa de nombre en la SVM llamada vs1. La asignación es una asignación de UNIX a Windows en la posición 1 de la lista de prioridades. La asignación asigna el usuario UNIX johnd al usuario de Windows ENG\JohnDoe.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

El siguiente comando crea otra asignación de nombre en la SVM llamada vs1. La asignación es una asignación de Windows a UNIX en la posición 1 de la lista de prioridades. Aquí el patrón y reemplazo incluyen expresiones regulares. La asignación asigna cada usuario CIFS del dominio ENG a los usuarios del dominio LDAP asociado con la SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

El siguiente comando crea otra asignación de nombre en la SVM llamada vs1. Aquí el patrón incluye "'$" como elemento del nombre de usuario de Windows que debe escaparse. La asignación asigna al usuario de

Windows ENG\ john$OPS al usuario UNIX john_OPS.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

Configurar el usuario predeterminado para las SVM de ONTAP NAS

Puede configurar un usuario predeterminado para que lo utilice si todos los demás intentos de asignación fallan para un usuario o si no desea asignar usuarios individuales entre UNIX y Windows. Si desea que la autenticación de usuarios no asignados falle, no debe configurar un usuario predeterminado.

Acerca de esta tarea

Para la autenticación CIFS, si no desea asignar cada usuario de Windows a un usuario individual de UNIX, puede especificar un usuario predeterminado de UNIX.

Para la autenticación NFS, si no desea asignar cada usuario UNIX a un usuario individual de Windows, puede especificar un usuario predeterminado de Windows.

Paso

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el siguiente comando…
Configure el usuario UNIX predeterminado	`vserver cifs options modify -default-unix-user user_name`
Configure el usuario predeterminado de Windows	`vserver nfs modify -default-win-user user_name`

Comandos ONTAP para administrar asignaciones de nombres NFS

Hay comandos de la ONTAP específicos para gestionar las asignaciones de nombres.

Si desea…	Se usa este comando…
Cree una asignación de nombres	`vserver name-mapping create`
Inserte una asignación de nombres en una posición específica	`vserver name-mapping insert`
Mostrar asignaciones de nombres	`vserver name-mapping show`

Intercambiar la posición de dos asignaciones DE nombre NOTA: No se permite un intercambio cuando se configura la asignación de nombres con una entrada de calificador ip.	`vserver name-mapping swap`
Modificar una asignación de nombres	`vserver name-mapping modify`
Eliminar una asignación de nombres	`vserver name-mapping delete`
Validar la asignación de nombre correcta	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

Obtenga más información sobre `vserver name-mapping` en el "Referencia de comandos del ONTAP".

Habilitar el acceso de clientes NFS de Windows para SVM de ONTAP

ONTAP admite el acceso a archivos desde clientes de Windows NFSv3. Esto significa que los clientes que ejecutan sistemas operativos Windows con compatibilidad NFSv3 pueden acceder a archivos de las exportaciones NFSv3 del clúster. Para utilizar correctamente esta funcionalidad, debe configurar correctamente la máquina virtual de almacenamiento (SVM) y tener en cuenta ciertos requisitos y limitaciones.

Acerca de esta tarea

De manera predeterminada, la compatibilidad con el cliente de Windows NFSv3 está deshabilitada.

Antes de empezar

Debe estar habilitado NFSv3 en la SVM.

Pasos

1. Habilitar la compatibilidad con clientes de Windows NFSv3:

   `vserver nfs modify -vserver` *`svm_name`* `-v3-ms-dos-client enabled -mount-rootonly disabled`

2. En todas las SVM compatibles con clientes Windows NFSv3, deshabilite `-enable-ejukebox` `-v3-connection-drop` los parámetros y:

   ```
   vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection-drop disabled
   ```

   Los clientes de Windows NFSv3 ahora pueden montar las exportaciones en el sistema de almacenamiento.

3. Asegúrese de que cada cliente Windows NFSv3 utilice montajes duros especificando `-o mtype=hard` la opción.

Esto es necesario para garantizar montajes fiables.

```
mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
```

Habilitar la visualización de exportaciones en clientes NFS para SVM de ONTAP

Los clientes NFS pueden utilizar el `showmount -e` comando para ver una lista de exportaciones disponibles desde un servidor NFS de ONTAP. Esto puede ayudar a los usuarios a identificar el sistema de archivos que desean montar.

ONTAP permite que los clientes NFS vean la lista de exportaciones de forma predeterminada. En versiones anteriores, la `showmount` opción `vserver nfs modify` del comando debe habilitarse de forma explícita. Para ver la lista de exportación, debe habilitarse NFSv3 en la SVM.

Ejemplo

El siguiente comando muestra la función showmount en la SVM denominada vs1:

```
clusterl : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
------- ---------
vs1    enabled
```

El siguiente comando ejecutado en un cliente NFS muestra la lista de exportaciones en un servidor NFS con la dirección IP 10.63.21.9:

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix         (everyone)
/unix/unixl   (everyone)
/unix/unix2   (everyone)
/             (everyone)
```

Gestione el acceso a archivos mediante NFS

Habilitar o deshabilitar NFSv3 para SVM de ONTAP

Puede activar o desactivar NFSv3 modificando la `-v3` opción. De este modo, los clientes pueden acceder a los archivos que utilizan el protocolo NFSv3. De forma predeterminada, NFSv3 está habilitado.

Paso

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el comando…

Habilitar NFSv3	`vserver nfs modify -vserver vserver_name -v3 enabled`
Desactivar NFSv3	`vserver nfs modify -vserver vserver_name -v3 disabled`

Habilitar o deshabilitar NFSv4.0 para SVM de ONTAP

Puede activar o desactivar NFSv4,0 modificando la `-v4.0` opción. De este modo, los clientes pueden acceder a los archivos que utilizan el protocolo NFSv4,0. En ONTAP 9.9.1, NFSv4.0 está habilitado de forma predeterminada; en las versiones anteriores, está deshabilitado de forma predeterminada.

Paso

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el siguiente comando…
Habilitar NFSv4,0	`vserver nfs modify -vserver vserver_name -v4.0 enabled`
Desactivar NFSv4,0	`vserver nfs modify -vserver vserver_name -v4.0 disabled`

Habilitar o deshabilitar NFSv4.1 para SVM de ONTAP

Puede activar o desactivar NFSv4,1 modificando la `-v4.1` opción. De este modo, los clientes pueden acceder a los archivos que utilizan el protocolo NFSv4,1. En ONTAP 9.9.1, NFSv4.1 está habilitado de forma predeterminada; en las versiones anteriores, está deshabilitado de forma predeterminada.

Paso

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el siguiente comando…
Habilitar NFSv4,1	`vserver nfs modify -vserver vserver_name -v4.1 enabled`
Desactivar NFSv4,1	`vserver nfs modify -vserver vserver_name -v4.1 disabled`

Administrar los límites del grupo de almacenamiento de ONTAP NFSv4

A partir de ONTAP 9,13, los administradores pueden permitir que sus servidores NFSv4 denieguen recursos a NFSv4 clientes cuando hayan alcanzado los límites de recursos

por cada pool de clientes. Cuando los clientes consumen demasiados recursos de la agrupación de almacenamiento NFSv4, esto puede provocar que otros clientes NFSv4 se bloqueen debido a la falta de disponibilidad de los recursos de la agrupación de almacenamiento NFSv4.

La activación de esta función también permite a los clientes ver el consumo de recursos del grupo de almacenamiento activo por cada cliente. Esto facilita la identificación de clientes que agotan los recursos del sistema y permite imponer límites de recursos por cliente.

Ver los recursos del almacén consumidos

El `vserver nfs storepool show` comando muestra el número de recursos de la agrupación almacenada consumidos. Una tienda es un conjunto de recursos utilizados por los clientes de NFSv4.

Paso

1. Como administrador, ejecute el `vserver nfs storepool show` comando para mostrar la información de la agrupación de almacenes de los clientes NFSv4.

Ejemplo

Este ejemplo muestra la información de la agrupación de almacenamiento de clientes NFSv4.

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-Ip: 10.0.1.1

Client-Ip Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount

-------------- --------- --------- ---------- ---------- ----------
---------

10.0.2.1          nfs4.1     true    2 1 0 4

10.0.2.2          nfs4.2     true    2 1 0 4

2 entries were displayed.
```

Activar o desactivar los controles de límite de grupo de almacenamiento

Los administradores pueden utilizar los siguientes comandos para activar o desactivar los controles de límite de storepool.

Paso

1. Como administrador, realice una de las siguientes acciones:

Si desea…	Introduzca el siguiente comando…
Active los controles de límite de grupo de almacenamiento	`vserver nfs storepool config modify -limit-enforce enabled`
Desactive los controles de límite de la agrupación de almacenamiento	`vserver nfs storepool config modify -limit-enforce disabled`

Ver una lista de clientes bloqueados

Si el límite de grupo de almacenamiento está activado, los administradores pueden ver qué clientes se han bloqueado al alcanzar el umbral de recursos por cliente. Los administradores pueden usar el siguiente comando para ver qué clientes se han marcado como clientes bloqueados.

Pasos

1. Utilice el `vserver nfs storepool blocked-client show` comando para mostrar la lista de clientes bloqueados NFSv4.

Eliminar un cliente de la lista de clientes bloqueados

Los clientes que alcancen su umbral por cliente se desconectarán y añadirán a la caché del cliente de bloques. Los administradores pueden usar el siguiente comando para eliminar el cliente de la caché del cliente de bloques. Esto permitirá que el cliente se conecte al servidor ONTAP NFSv4.

Pasos

1. Utilice `vserver nfs storepool blocked-client flush -client-ip <ip address>` el comando para vaciar la caché de cliente bloqueada de storepool.
2. Utilice `vserver nfs storepool blocked-client show` el comando para verificar que el cliente se ha eliminado de la caché del cliente de bloques.

Ejemplo

En este ejemplo, se muestra un cliente bloqueado con la dirección IP «10,2.1,1» vaciada en todos los nodos.

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
----------
10.1.1.1

1 entries were displayed.
```

Habilitar o deshabilitar pNFS para SVM de ONTAP

PNFs mejora el rendimiento al permitir que los clientes NFS realicen operaciones de lectura/escritura en dispositivos de almacenamiento directamente y en paralelo, evitando así el servidor NFS como un posible cuello de botella. Para habilitar o deshabilitar pNFS (NFS paralelo), puede modificar `-v4.1-pnfs` la opción.

Si la versión de ONTAP es…	El valor predeterminado de pNFS es…
9,8 o posterior	deshabilitado
9,7 o anterior	activado

Antes de empezar

Se requiere compatibilidad con NFSv4.1 para poder utilizar pNFS.

Si desea habilitar pNFS, primero debe deshabilitar las referencias NFS. No se pueden habilitar ambos a la vez.

Si utiliza pNFS con Kerberos en SVM, debe habilitar Kerberos en cada LIF de la SVM.

Paso

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el comando…
Habilite pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled`
Deshabilite pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled`

Información relacionada

- Descripción general de trunking NFS

Controlar el acceso NFS a través de TCP y UDP para SVM de ONTAP

Puede habilitar o deshabilitar el acceso de NFS a las máquinas virtuales de almacenamiento (SVM) a través de TCP y UDP modificando `-tcp -udp` los parámetros y, respectivamente. De este modo, puede controlar si los clientes NFS pueden acceder a los datos a través de TCP o UDP de su entorno.

Acerca de esta tarea

Estos parámetros solo se aplican a NFS. No afectan a los protocolos auxiliares. Por ejemplo, si NFS over TCP está deshabilitado, las operaciones de montaje mediante TCP siguen teniendo éxito. Para bloquear completamente el tráfico TCP o UDP, puede utilizar reglas de política de exportación.

Debe desactivar SnapDiff RPC Server antes de deshabilitar TCP para NFS para evitar un error de comando. Puede desactivar TCP mediante el comando `vserver snapdiff-rpc-server off -vserver vserver name`.

Paso

1. Ejecute una de las siguientes acciones:

Si desea que el acceso NFS sea…	Introduzca el comando…
Activado a través de TCP	`vserver nfs modify -vserver vserver_name -tcp enabled`
Desactivado en TCP	`vserver nfs modify -vserver vserver_name -tcp disabled`
Activado a través de UDP	`vserver nfs modify -vserver vserver_name -udp enabled`
Desactivado en UDP	`vserver nfs modify -vserver vserver_name -udp disabled`

Controlar solicitudes NFS desde puertos no reservados para SVM de ONTAP

Puede rechazar las solicitudes de montaje NFS desde puertos no reservados si habilita `-mount-rootonly` la opción. Para rechazar todas las solicitudes NFS de puertos no reservados, puede habilitar `-nfs-rootonly` la opción.

Acerca de esta tarea

Por defecto, la opción `-mount-rootonly` es `enabled`.

Por defecto, la opción `-nfs-rootonly` es `disabled`.

Estas opciones no se aplican al procedimiento NULL.

Paso

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el comando…
Permita las solicitudes de montaje NFS de puertos no reservados	`vserver nfs modify -vserver vserver_name -mount -rootonly disabled`
Rechace las solicitudes de montaje NFS de puertos no reservados	`vserver nfs modify -vserver vserver_name -mount -rootonly enabled`
Permita todas las solicitudes NFS de puertos no reservados	`vserver nfs modify -vserver vserver_name -nfs -rootonly disabled`

Rechace todas las solicitudes NFS de puertos no reservados	`vserver nfs modify -vserver vserver_name -nfs -rootonly enabled`

Manejar el acceso NFS a volúmenes NTFS de ONTAP o qtrees para usuarios desconocidos de UNIX

Si ONTAP no puede identificar a los usuarios de UNIX que intentan conectarse a volúmenes o qtrees con un estilo de seguridad NTFS, no puede asignar explícitamente el usuario a un usuario de Windows. Puede configurar ONTAP para denegar el acceso a dichos usuarios para una seguridad más estricta o para asignarlos a un usuario de Windows predeterminado para garantizar un nivel mínimo de acceso a todos los usuarios.

Antes de empezar

Si desea habilitar esta opción, se debe configurar un usuario de Windows predeterminado.

Acerca de esta tarea

Si un usuario de UNIX intenta acceder a volúmenes o qtrees con estilo de seguridad NTFS, el usuario de UNIX primero debe asignarse a un usuario de Windows para que ONTAP pueda evaluar correctamente los permisos NTFS. Sin embargo, si ONTAP no puede buscar el nombre del usuario UNIX en los orígenes del servicio de nombres de información de usuario configurados, no puede asignar explícitamente el usuario UNIX a un usuario específico de Windows. Puede decidir cómo manejar estos usuarios de UNIX desconocidos de las siguientes formas:

- Denegar el acceso a usuarios UNIX desconocidos.

  Esto aplica una seguridad más estricta al requerir una asignación explícita para que todos los usuarios de UNIX obtengan acceso a volúmenes o qtrees NTFS.

- Asignar usuarios UNIX desconocidos a un usuario predeterminado de Windows.

  Esto proporciona menos seguridad pero más comodidad al garantizar que todos los usuarios obtienen un nivel mínimo de acceso a volúmenes o qtrees NTFS a través de un usuario de Windows predeterminado.

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Ejecute una de las siguientes acciones:

Si desea el usuario predeterminado de Windows para usuarios UNIX desconocidos…	Introduzca el comando…
Activado	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled`

Deshabilitado	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled`

3. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Consideraciones para los clientes que montan exportaciones NFS de ONTAP en puertos no reservados

`-mount-rootonly`La opción debe estar deshabilitada en un sistema de almacenamiento que deba admitir clientes que montan exportaciones NFS con un puerto no reservado incluso cuando el usuario haya iniciado sesión como raíz. Entre estos clientes se encuentran los clientes Hummingbird y los clientes Solaris NFS/IPv6.

Si la `-mount-rootonly` opción está habilitada, ONTAP no permite que los clientes NFS que utilicen puertos no reservados, es decir, que los puertos con números superiores a 1.023, monten las exportaciones NFS.

Realice una comprobación de acceso más estricta para los grupos de redes verificando los dominios para las SVM NFS de ONTAP

De forma predeterminada, ONTAP realiza una verificación adicional al evaluar el acceso de cliente para un grupo de red. La comprobación adicional garantiza que el dominio del cliente coincida con la configuración de dominio de la máquina virtual de almacenamiento (SVM). De lo contrario, ONTAP niega el acceso del cliente.

Acerca de esta tarea

Cuando ONTAP evalúa las reglas de política de exportación para el acceso de cliente y una regla de política de exportación contiene un grupo de red, ONTAP debe determinar si la dirección IP de un cliente pertenece al grupo de redes. Con este fin, ONTAP convierte la dirección IP del cliente en un nombre de host mediante DNS y obtiene un nombre de dominio completo (FQDN).

Si el archivo netgroup sólo enumera un nombre corto para el host y el nombre corto para el host existe en varios dominios, es posible que un cliente de un dominio diferente obtenga acceso sin esta comprobación.

Para evitar esto, ONTAP compara el dominio que ha devuelto el DNS del host con la lista de nombres de dominio DNS configurados para la SVM. Si coincide, se permite el acceso. Si no coincide, se deniega el acceso.

Esta verificación está habilitada de forma predeterminada. Puede gestionarla modificando `-netgroup-dns -domain-search` el parámetro, que está disponible en el nivel de privilegios avanzado.

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Realice la acción deseada:

Si desea que la verificación del dominio para los grupos de red sea…	Introduzca…
Activado	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled`
Deshabilitado	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled`

3. Configure el nivel de privilegio en admin:

```
set -privilege admin
```

Modificar los puertos utilizados para los servicios NFSv3 para las SVM de ONTAP

El servidor NFS del sistema de almacenamiento usa servicios como el demonio de montaje y Network Lock Manager para comunicarse con los clientes NFS a través de puertos de red predeterminados específicos. En la mayoría de los entornos NFS, los puertos predeterminados funcionan correctamente y no requieren modificación, pero si desea utilizar puertos de red NFS diferentes en su entorno NFSv3, puede hacerlo.

Antes de empezar

Cambiar los puertos NFS del sistema de almacenamiento requiere que todos los clientes NFS se vuelvan a conectar al sistema, por lo que debe comunicar esta información a los usuarios antes de realizar el cambio.

Acerca de esta tarea

Puede establecer los puertos utilizados por los servicios de daemon de montaje NFS, Network Lock Manager, Network Status Monitor y NFS quota para cada máquina virtual de almacenamiento (SVM). El cambio de número de puerto afecta a los clientes NFS que acceden a los datos a través de TCP y UDP.

Los puertos de NFSv4 y NFSv4.1 no se pueden cambiar.

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Desactivar el acceso a NFS:

```
vserver nfs modify -vserver vserver_name -access false
```

3. Establezca el puerto NFS para el servicio NFS específico:

```
vserver nfs modify -vserver vserver_namenfs_port_parameterport_number
```

Parámetro de puerto NFS	Descripción	Puerto predeterminado
`-mountd-port`	Daemon de montaje NFS	635
`-nlm-port`	Administrador de bloqueo de red	4045
`-nsm-port`	Monitor de estado de red	4046
`-rquotad-port`	Daemon de cuota NFS	4049

Además del puerto predeterminado, el intervalo permitido de números de puerto es de 1024 a 65535. Cada servicio NFS debe utilizar un puerto único.

4. Habilitar el acceso a NFS:

   ```
   vserver nfs modify -vserver vserver_name -access true
   ```

5. Utilice `network connections listening show` el comando para verificar los cambios en el número de puerto.

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

6. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Ejemplo

Los siguientes comandos establecen el puerto del daemon de montaje NFS en 1113 en la SVM llamada vs1:

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: cluster1-01
Cluster          cluster1-01_clus_1:7700          TCP/ctlopcp
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:1113                       TCP/mount
vs1              data1:1113                       UDP/mount
...
vs1::*> set -privilege admin
```

Comandos de ONTAP para gestionar servidores NFS

Hay comandos ONTAP específicos para gestionar los servidores NFS.

Si desea…	Se usa este comando…
Cree un servidor NFS	`vserver nfs create`
Muestre los servidores NFS	`vserver nfs show`
Modificar un servidor NFS	`vserver nfs modify`
Suprimir un servidor NFS	`vserver nfs delete`

Oculte la `.snapshot` lista de directorios en NFSv3 puntos de montaje `.snapshot`Se permitirá el acceso explícito al directorio incluso si la opción está activada.	`vserver nfs` comandos con `-v3-hide-snapshot` la opción habilitada

Obtenga más información sobre `vserver nfs` en el "Referencia de comandos del ONTAP".

Solucionar problemas de servicio de nombres para SVM NAS de ONTAP

Cuando los clientes experimentan fallos de acceso debido a problemas de servicio de nombres, puede utilizar la `vserver services name-service getxxbyyy` familia de comandos para realizar manualmente varias consultas de servicio de nombres y examinar los detalles y resultados de la búsqueda para ayudar con la solución de problemas.

Acerca de esta tarea

- Para cada comando, puede especificar lo siguiente:
  - Nombre del nodo o de la máquina virtual de almacenamiento (SVM) en la que se realiza la búsqueda.

    Esto le permite probar las búsquedas del servicio de nombres para un nodo o SVM específicos a fin de limitar la búsqueda de un posible problema de configuración del servicio de nombres.
  - Si se muestra el origen utilizado para la búsqueda.

    Esto le permite comprobar si se ha utilizado la fuente correcta.
- ONTAP selecciona el servicio para realizar la búsqueda de acuerdo con el orden del switch de servicio de nombres configurado.
- Estos comandos están disponibles en el nivel de privilegio avanzado.

Pasos

1. Ejecute una de las siguientes acciones:

Para recuperar…	Usar el comando…

Dirección IP de un nombre de host	`vserver services name-service getxxbyyy getaddrinfo` `vserver services name-service getxxbyyy gethostbyname` (Solo direcciones IPv4)
Miembros de un grupo por ID de grupo	`vserver services name-service getxxbyyy getgrbygid`
Miembros de un grupo por nombre de grupo	`vserver services name-service getxxbyyy getgrbyname`
Lista de grupos a los que pertenece un usuario	`vserver services name-service getxxbyyy getgrlist`
Nombre de host de una dirección IP	`vserver services name-service getxxbyyy getnameinfo` `vserver services name-service getxxbyyy gethostbyaddr` (Solo direcciones IPv4)
Información de usuario por nombre de usuario	`vserver services name-service getxxbyyy getpwbyname` Puede probar la resolución de nombres de los usuarios de RBAC especificando el `-use-rbac` parámetro como `true`.
Información de usuario por ID de usuario	`vserver services name-service getxxbyyy getpwbyuid` Puede probar la resolución de nombres de los usuarios de RBAC especificando el `-use -rbac` parámetro como `true`.
Pertenencia a netgroup de un cliente	`vserver services name-service getxxbyyy netgrp`
Pertenencia a netgroup de un cliente mediante la búsqueda netgroup-by-host	`vserver services name-service getxxbyyy netgrpbyhost`

En el siguiente ejemplo, se muestra una prueba de búsqueda DNS para la SVM vs1 intentando obtener la dirección IP del host acast1.eng.example.com:

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

En el siguiente ejemplo, se muestra una prueba de búsqueda de NIS para el SVM vs1 intentando recuperar la información de usuario de un usuario con el UID 501768:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvc2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

En el siguiente ejemplo, se muestra una prueba de búsqueda LDAP para la SVM vs1 intentando recuperar la información de usuario de un usuario con el nombre ldap1:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

En el siguiente ejemplo se muestra una prueba de búsqueda de netgroup para la SVM vs1 intentando averiguar si el cliente dnshost0 es miembro del netgroup lnetgroup136:

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. Analice los resultados de la prueba realizada y tome las medidas necesarias.

Si…	Compruebe…
Error en la búsqueda del nombre de host o de la dirección IP o se obtuvieron resultados incorrectos	Configuración de DNS

Si…	Compruebe…
La búsqueda se ha consultado con un origen incorrecto	Asigne un nombre a la configuración del switch de servicio
Error de búsqueda de usuarios o grupos o resultados incorrectos	• Asigne un nombre a la configuración del switch de servicio • Configuración de origen (archivos locales, dominio NIS, cliente LDAP) • Configuración de red (por ejemplo, LIF y rutas)
Se ha producido un error en la búsqueda del nombre de host o se ha agotado el tiempo de espera y el servidor DNS no resuelve los nombres cortos de DNS (por ejemplo, host1)	Configuración de DNS para consultas de dominio de nivel superior (TLD). Puede desactivar las consultas TLD con la `-is-tld-query-enabled false` opción del `vserver services name-service dns modify` comando.

Información relacionada

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

Verificar las conexiones del servicio de nombres para las SVM de ONTAP NAS

Puede verificar los servidores de nombres DNS y del Protocolo ligero de acceso a directorios (LDAP) para verificar que estén conectados a ONTAP. Estos comandos están disponibles en el nivel de privilegios de administrador.

Acerca de esta tarea

Puede comprobar que la configuración del servicio de nombres DNS o LDAP sea válida según sea necesario mediante el comprobador de configuración del servicio de nombres. Esta comprobación de validación puede iniciarse en la línea de comandos o en System Manager.

Para las configuraciones DNS, todos los servidores se han probado y deben funcionar para que la configuración se considere válida. Para las configuraciones LDAP, siempre que un servidor esté activo, la configuración es válida. Los comandos del servicio de nombres aplican el comprobador de configuración a menos que el `skip-config-validation` campo sea verdadero (el valor por defecto es falso).

Paso

1. Utilice el comando apropiado para comprobar la configuración de un servicio de nombres. La interfaz de usuario muestra el estado de los servidores configurados.

Para comprobar…	Se usa este comando…
Estado de configuración de DNS	`vserver services name-service dns check`
Estado de configuración de LDAP	`vserver services name-service ldap check`

```
cluster1::> vserver services name-service dns check -vserver vs0

Vserver         Name Server     Status  Status Details
--------------  --------------- ------- -------------------------
 vs0            10.11.12.13     up      Response time (msec): 55
 vs0            10.11.12.14     up      Response time (msec): 70
 vs0            10.11.12.15     down    Connection refused.
+---------------------------------------------------------------+
```

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                 |
| Client Configuration Name: c1                                |
| LDAP Status: up                                              |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                 |
```

La validación de la configuración se realiza correctamente si se puede acceder al menos uno de los servidores configurados (servidores/servidores ldap) y se proporciona el servicio. Se muestra una advertencia si algunos de los servidores no son accesibles.

Comandos ONTAP para administrar entradas de conmutación del servicio de nombres NAS

Puede administrar las entradas del conmutador de servicios de nombres creando, visualizando, modificando y eliminando.

Si desea…	Se usa este comando…
Crear una entrada de conmutador de servicio de nombres	`vserver services name-service ns-switch create`
Mostrar las entradas del conmutador de servicio de nombres	`vserver services name-service ns-switch show`
Modificar una entrada de cambio de servicio de nombres	`vserver services name-service ns-switch modify`
Eliminar una entrada de cambio de servicio de nombres	`vserver services name-service ns-switch delete`

Obtenga más información sobre `vserver services name-service ns-switch` en el "Referencia de comandos del ONTAP".

Información relacionada

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

Comandos ONTAP para administrar la caché del servicio de nombres NAS

Puede gestionar la caché del servicio de nombres modificando el valor de tiempo de vida (TTL). El valor TTL determina el tiempo que la información del servicio de nombre es persistente en la caché.

Si desea modificar el valor TTL para…	Se usa este comando…
Usuarios de UNIX	`vserver services name-service cache unix-user settings`
Grupos UNIX	`vserver services name-service cache unix-group settings`
Grupos de redes UNIX	`vserver services name-service cache netgroups settings`
Hosts	`vserver services name-service cache hosts settings`
Pertenencia a grupos	`vserver services name-service cache group-membership settings`

Información relacionada

"Referencia de comandos del ONTAP"

Comandos ONTAP para administrar asignaciones de nombres NFS

Hay comandos de la ONTAP específicos para gestionar las asignaciones de nombres.

Si desea…	Se usa este comando…
Cree una asignación de nombres	`vserver name-mapping create`
Inserte una asignación de nombres en una posición específica	`vserver name-mapping insert`
Mostrar asignaciones de nombres	`vserver name-mapping show`
Intercambiar la posición de dos asignaciones DE nombre NOTA: No se permite un intercambio cuando se configura la asignación de nombres con una entrada de calificador ip.	`vserver name-mapping swap`

Modificar una asignación de nombres	`vserver name-mapping modify`
Eliminar una asignación de nombres	`vserver name-mapping delete`
Validar la asignación de nombre correcta	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

Obtenga más información sobre `vserver name-mapping` en el "Referencia de comandos del ONTAP".

Comandos ONTAP para administrar usuarios locales de UNIX en NAS

Hay comandos específicos de la ONTAP para administrar los usuarios locales de UNIX.

Si desea…	Se usa este comando…
Cree un usuario UNIX local	`vserver services name-service unix-user create`
Cargar usuarios UNIX locales desde un URI	`vserver services name-service unix-user load-from-uri`
Mostrar usuarios UNIX locales	`vserver services name-service unix-user show`
Modificar un usuario UNIX local	`vserver services name-service unix-user modify`
Elimine un usuario UNIX local	`vserver services name-service unix-user delete`

Obtenga más información sobre `vserver services name-service unix-user` en el "Referencia de comandos del ONTAP".

Comandos ONTAP para administrar grupos locales de UNIX NAS

Hay comandos específicos de la ONTAP para administrar los grupos UNIX locales.

Si desea…	Se usa este comando…
Cree un grupo UNIX local	`vserver services name-service unix-group create`
Agregar un usuario a un grupo UNIX local	`vserver services name-service unix-group adduser`
Cargar grupos UNIX locales desde un URI	`vserver services name-service unix-group load-from-uri`

Mostrar grupos UNIX locales	`vserver services name-service unix-group show`
Modificar un grupo UNIX local	`vserver services name-service unix-group modify`
Eliminar un usuario de un grupo UNIX local	`vserver services name-service unix-group deluser`
Elimine un grupo UNIX local	`vserver services name-service unix-group delete`

Obtenga más información sobre `vserver services name-service unix-group` en el "Referencia de comandos del ONTAP".

Límites para usuarios, grupos y miembros de grupos locales de UNIX para SVM NFS de ONTAP

ONTAP ha introducido límites para el número máximo de usuarios y grupos de UNIX en el clúster, así como comandos para gestionar estos límites. Estos límites pueden ayudar a evitar problemas de rendimiento, ya que impiden que los administradores creen demasiados usuarios y grupos locales de UNIX en el clúster.

Hay un límite para el número combinado de grupos de usuarios UNIX locales y miembros de grupo. Hay un límite independiente para los usuarios locales de UNIX. Los límites se limitan a todo el clúster. Cada uno de estos nuevos límites se establece en un valor predeterminado que se puede modificar hasta un límite rígido preasignado.

Base de datos	Límite predeterminado	Limitación estricta
Usuarios UNIX locales	32.768	65.536
Grupos UNIX locales y miembros del grupo	32.768	65.536

Administrar límites para usuarios y grupos locales de UNIX para SVM NFS de ONTAP

Hay comandos específicos de ONTAP para administrar límites para usuarios y grupos de UNIX locales. Los administradores de clústeres pueden utilizar estos comandos para solucionar problemas de rendimiento en el clúster que se creen que están relacionados con un número excesivo de usuarios y grupos UNIX locales.

Acerca de esta tarea

Estos comandos están disponibles para el administrador del clúster en el nivel de privilegio avanzado.

Paso

1. Ejecute una de las siguientes acciones:

Si desea…	Usar el comando…
Mostrar información acerca de los límites de usuario local de UNIX	`vserver services unix-user max-limit show`
Muestra información acerca de los límites de grupos UNIX locales	`vserver services unix-group max-limit show`
Modificar los límites de usuarios UNIX locales	`vserver services unix-user max-limit modify`
Modificar los límites de grupos UNIX locales	`vserver services unix-group max-limit modify`

Obtenga más información sobre `vserver services unix` en el "Referencia de comandos del ONTAP".

Comandos ONTAP para administrar grupos de redes locales NFS

Puede administrar los grupos de red locales cargándolos desde un URI, verificando su estado entre los nodos, mostrándolos y borrándolos.

Si desea…	Usar el comando…
Cargar grupos de red desde un URI	`vserver services name-service netgroup load`
Compruebe el estado de los grupos de red en los nodos	`vserver services name-service netgroup status` Disponible a nivel de privilegio avanzado y superior.
Mostrar grupos de redes locales	`vserver services name-service netgroup file show`
Elimine un netgroup local	`vserver services name-service netgroup file delete`

Obtenga más información sobre `vserver services name-service netgroup file` en el "Referencia de comandos del ONTAP".

Comandos ONTAP para administrar configuraciones de dominios NIS NFS

Hay comandos específicos de ONTAP para administrar configuraciones de dominio NIS.

Si desea…	Se usa este comando…
Cree una configuración de dominio NIS	`vserver services name-service nis-domain create`

Mostrar configuraciones de dominio NIS	`vserver services name-service nis-domain show`
Mostrar el estado de enlace de una configuración de dominio NIS	`vserver services name-service nis-domain show-bound`
Mostrar estadísticas NIS	`vserver services name-service nis-domain show-statistics` Disponible en el nivel de privilegio avanzado y superior.
Borrar estadísticas de NIS	`vserver services name-service nis-domain clear-statistics` Disponible en el nivel de privilegio avanzado y superior.
Modifique una configuración de dominio NIS	`vserver services name-service nis-domain modify`
Elimine una configuración de dominio NIS	`vserver services name-service nis-domain delete`
Habilite el almacenamiento en caché para búsquedas de netgroup-by-host	`vserver services name-service nis-domain netgroup-database config modify` Disponible en el nivel de privilegio avanzado y superior.

Obtenga más información sobre `vserver services name-service nis-domain` en el "Referencia de comandos del ONTAP".

Comandos ONTAP para administrar configuraciones de cliente LDAP NFS

Hay comandos ONTAP específicos para gestionar las configuraciones de cliente LDAP.

> Los administradores de SVM no pueden modificar ni eliminar las configuraciones de cliente LDAP que crearon los administradores del clúster.

Si desea…	Se usa este comando…
Cree una configuración de cliente LDAP	`vserver services name-service ldap client create`
Mostrar las configuraciones del cliente LDAP	`vserver services name-service ldap client show`
Modifique una configuración de cliente LDAP	`vserver services name-service ldap client modify`
Cambie la contraseña de ENLACE de cliente LDAP	`vserver services name-service ldap client modify-bind-password`

Eliminar una configuración de cliente LDAP	`vserver services name-service ldap client delete`

Obtenga más información sobre `vserver services name-service ldap client` en el "Referencia de comandos del ONTAP".

Comandos ONTAP para administrar configuraciones LDAP de NFS

Hay comandos de la ONTAP específicos para gestionar las configuraciones LDAP.

Si desea…	Se usa este comando…
Cree una configuración LDAP	`vserver services name-service ldap create`
Mostrar configuraciones LDAP	`vserver services name-service ldap show`
Modificar una configuración LDAP	`vserver services name-service ldap modify`
Eliminar una configuración de LDAP	`vserver services name-service ldap delete`

Obtenga más información sobre `vserver services name-service ldap` en el "Referencia de comandos del ONTAP".

Comandos ONTAP para administrar plantillas de esquema de cliente LDAP NFS

Hay comandos ONTAP específicos para administrar plantillas de esquema de cliente LDAP.

> Los administradores de SVM no pueden modificar ni eliminar esquemas de cliente LDAP que crearon los administradores de clúster.

Si desea…	Se usa este comando…
Copie una plantilla de esquema LDAP existente	`vserver services name-service ldap client schema copy` Disponible en el nivel de privilegio avanzado y superior.
Mostrar plantillas de esquema LDAP	`vserver services name-service ldap client schema show`
Modificar una plantilla de esquema LDAP	`vserver services name-service ldap client schema modify` Disponible en el nivel de privilegio avanzado y superior.
Eliminar una plantilla de esquema LDAP	`vserver services name-service ldap client schema delete` Disponible en el nivel de privilegio avanzado y superior.

Obtenga más información sobre `vserver services name-service ldap client schema` en el

"Referencia de comandos del ONTAP".

Comandos ONTAP para administrar configuraciones de interfaz Kerberos de NFS

Hay comandos de ONTAP específicos para gestionar las configuraciones de la interfaz de Kerberos de NFS.

Si desea…	Se usa este comando…
Habilite NFS Kerberos en una LIF	`vserver nfs kerberos interface enable`
Mostrar las configuraciones de la interfaz Kerberos para NFS	`vserver nfs kerberos interface show`
Modifique la configuración de una interfaz NFS Kerberos	`vserver nfs kerberos interface modify`
Desactive NFS Kerberos en una LIF	`vserver nfs kerberos interface disable`

Obtenga más información sobre `vserver nfs kerberos interface` en el "Referencia de comandos del ONTAP".

Comandos ONTAP para administrar configuraciones de dominio Kerberos de NFS

Hay comandos específicos de ONTAP para gestionar configuraciones de dominio de Kerberos de NFS.

Si desea…	**Se usa este comando…**
Cree una configuración de dominio de Kerberos para NFS	`vserver nfs kerberos realm create`
Mostrar configuraciones de dominio de Kerberos para NFS	`vserver nfs kerberos realm show`
Modificar una configuración de dominio de Kerberos para NFS	`vserver nfs kerberos realm modify`
Elimine una configuración de dominio de Kerberos para NFS	`vserver nfs kerberos realm delete`

Obtenga más información sobre `vserver nfs kerberos realm` en el "Referencia de comandos del ONTAP".

Comandos de ONTAP para gestionar políticas de exportación

Hay comandos de ONTAP específicos para gestionar las políticas de exportación.

Si desea…	Se usa este comando…
Mostrar información acerca de las políticas de exportación	`vserver export-policy show`
Cambiar el nombre de una política de exportación	`vserver export-policy rename`
Copiar una política de exportación	`vserver export-policy copy`
Eliminar una política de exportación	`vserver export-policy delete`

Obtenga más información sobre `vserver export-policy` en el "Referencia de comandos del ONTAP".

Comandos de ONTAP para administrar reglas de exportación

Hay comandos ONTAP específicos para gestionar las reglas de exportación.

Si desea…	Se usa este comando…
Cree una regla de exportación	`vserver export-policy rule create`
Muestra información acerca de las reglas de exportación	`vserver export-policy rule show`
Modificar una regla de exportación	`vserver export-policy rule modify`
Eliminar una regla de exportación	`vserver export-policy rule delete`

Si ha configurado varias reglas de exportación idénticas que coinciden con distintos clientes, asegúrese de mantenerlas sincronizadas al gestionar las reglas de exportación.

Obtenga más información sobre `vserver export-policy` en el "Referencia de comandos del ONTAP".

Configure la caché de credenciales NFS

Razones para modificar el tiempo de vida de la caché de credenciales NFS para las SVM de ONTAP

ONTAP utiliza la memoria caché de credenciales para almacenar la información necesaria para la autenticación de usuarios para acceder a la exportación de NFS con el fin de proporcionar un acceso más rápido y mejorar el rendimiento. Puede configurar el tiempo que se almacena la información en la caché de credenciales para personalizarla en su entorno.

Hay varios escenarios cuando se modifica el tiempo de vida de la caché de credenciales de NFS (TTL) puede ayudar a resolver los problemas. Usted debe entender cuáles son estos escenarios así como las consecuencias de hacer estas modificaciones.

Razones

Considere cambiar el TTL predeterminado en las siguientes circunstancias:

Problema	Acción correctiva
Los servidores de nombres de su entorno están experimentando una degradación del rendimiento debido a una gran carga de solicitudes de ONTAP.	Aumente el TTL para las credenciales positivas y negativas en la caché para reducir el número de solicitudes de ONTAP a los servidores de nombres.
El administrador del servidor de nombres realizó cambios para permitir el acceso a usuarios NFS que se denegaron anteriormente.	Disminuya el TTL para las credenciales negativas en la caché a fin de reducir el tiempo que los usuarios NFS tienen que esperar a que ONTAP solicite credenciales nuevas de los servidores de nombres externos para que puedan acceder.
El administrador del servidor de nombres realizó cambios para denegar el acceso a usuarios NFS que se habían permitido previamente.	Reduzca el TTL para las credenciales positivas en caché para reducir el tiempo antes de que ONTAP solicite credenciales nuevas de los servidores de nombres externos, de modo que los usuarios de NFS no tengan acceso.

Consecuencias

Puede modificar el período de tiempo individualmente para almacenar en caché las credenciales positivas y negativas. Sin embargo, usted debe ser consciente de las ventajas y desventajas de hacerlo.

Si…	La ventaja es…	La desventaja es…
Aumente el tiempo positivo de la caché de credenciales	ONTAP envía solicitudes de credenciales a servidores de nombres con menos frecuencia, lo que reduce la carga en los servidores de nombres.	La denegación del acceso a los usuarios de NFS tarda más tiempo, pero ya no es así.
Reduzca el tiempo positivo de la caché de credenciales	Tarda menos tiempo en denegar el acceso a los usuarios de NFS a los que antes no se había permitido, pero ya no lo están.	ONTAP envía solicitudes de credenciales a los servidores de nombres con mayor frecuencia, lo que aumenta la carga en los servidores de nombres.
Aumente el tiempo de la caché de credenciales negativas	ONTAP envía solicitudes de credenciales a servidores de nombres con menos frecuencia, lo que reduce la carga en los servidores de nombres.	Lleva más tiempo conceder acceso a los usuarios de NFS que antes no estaban permitidos pero que ahora lo son.

Si…	La ventaja es…	La desventaja es…
Reduzca el tiempo de la caché de credenciales negativas	Tarda menos tiempo en conceder acceso a los usuarios de NFS que antes no estaban permitidos pero que ahora lo son.	ONTAP envía solicitudes de credenciales a los servidores de nombres con mayor frecuencia, lo que aumenta la carga en los servidores de nombres.

Configurar el tiempo de vida de las credenciales de usuario NFS almacenadas en caché para las SVM de ONTAP

Puede configurar el lapso en que ONTAP almacena credenciales para los usuarios NFS en su caché interna (tiempo de actividad o TTL) mediante la modificación del servidor NFS de la máquina virtual de almacenamiento (SVM). De este modo, puede solucionar algunos problemas relacionados con la alta carga de los servidores de nombres o con los cambios de las credenciales que afectan al acceso del usuario NFS.

Acerca de esta tarea

Estos parámetros están disponibles en el nivel de privilegios avanzado.

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Realice la acción deseada:

Si desea modificar el TTL para el almacenamiento en caché…	Usar el comando…
Credenciales positivas	`vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live` El TTL se mide en milisegundos. A partir de ONTAP 9.10.1 y versiones posteriores, el valor predeterminado es 1 hora (3.600.000 milisegundos). En ONTAP 9.9.1 y las versiones anteriores, el valor predeterminado es de 24 horas (86.400.000 milisegundos). El intervalo permitido para este valor es de 1 minuto (60000 milisegundos) a 7 días (604,800,000 milisegundos).
Credenciales negativas	`vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live` El TTL se mide en milisegundos. El valor predeterminado es 2 horas (7.200.000 milisegundos). El intervalo permitido para este valor es de 1 minuto (60000 milisegundos) a 7 días (604,800,000 milisegundos).

3. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Gestione las cachés de la política de exportación

Vaciar cachés de políticas de exportación para SVM de ONTAP NAS

ONTAP usa varios cachés de políticas de exportación para almacenar información relacionada con las políticas de exportación para agilizar el acceso. Vaciar las cachés de política de exportación manualmente (`vserver export-policy cache flush`) Elimina la información potencialmente obsoleta y obliga a ONTAP a recuperar la información actual de los recursos externos correspondientes. Esto puede ayudar a resolver diversos problemas relacionados con el acceso de clientes a exportaciones NFS.

Acerca de esta tarea

La información de la caché de la directiva de exportación puede quedar obsoleta por los siguientes motivos:

- Un cambio reciente en las reglas de política de exportación
- Un cambio reciente en los registros de nombres de host en servidores de nombres
- Un cambio reciente en las entradas de netgroup en los servidores de nombres
- Recuperación de una interrupción de la red que impidió que los grupos de red se cargaran por completo

Pasos

1. Si no se cuenta con la caché de servicio de nombres habilitada, realice una de las siguientes acciones en el modo de privilegio avanzado:

Si quieres tirar la cadena…	Introduzca el comando…
Todas las cachés de directivas de exportación (excepto showmount)	`vserver export-policy cache flush -vserver vserver_name`
La política de exportación rige la caché de acceso	`vserver export-policy cache flush -vserver vserver_name -cache access` Puede incluir el parámetro opcional `-node` para especificar el nodo en el que desea vaciar la caché de acceso.
La caché de nombres del host	`vserver export-policy cache flush -vserver vserver_name -cache host`
La caché de netgroup	`vserver export-policy cache flush -vserver vserver_name -cache netgroup` El procesamiento de netgroups requiere muchos recursos. Solo debe vaciar la caché de netgroup si intenta resolver un problema de acceso de cliente causado por un grupo de red obsoleto.

Si quieres tirar la cadena…	Introduzca el comando…
La caché showmount	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

2. Si la caché del servicio de nombres está habilitada, realice una de las siguientes acciones:

Si quieres tirar la cadena…	Introduzca el comando…
La política de exportación rige la caché de acceso	`vserver export-policy cache flush -vserver vserver_name -cache access` Puede incluir el parámetro opcional `-node` para especificar el nodo en el que desea vaciar la caché de acceso.
La caché de nombres del host	`vserver services name-service cache hosts forward-lookup delete-all`
La caché de netgroup	`vserver services name-service cache netgroups ip-to-netgroup delete-all` `vserver services name-service cache netgroups members delete-all` El procesamiento de netgroups requiere muchos recursos. Solo debe vaciar la caché de netgroup si intenta resolver un problema de acceso de cliente causado por un grupo de red obsoleto.
La caché showmount	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

Mostrar la cola y el caché del grupo de redes de políticas de exportación para SVM NFS de ONTAP

ONTAP utiliza la cola de netgroup al importar y resolver grupos de red y utiliza la caché de netgroup para almacenar la información resultante. Al solucionar problemas relacionados con el grupo de red de la política de exportación, puede utilizar los `vserver export-policy netgroup queue show` `vserver export-policy netgroup cache show` comandos y para mostrar el estado de la cola de grupo de red y el contenido de la caché de grupo de red.

Paso

1. Ejecute una de las siguientes acciones:

Para mostrar el grupo de red de la directiva de exportación…	Introduzca el comando…

Cola	`vserver export-policy netgroup queue show`
Almacenamiento en caché	`vserver export-policy netgroup cache show -vserver vserver_name`

Obtenga más información sobre `vserver export-policy netgroup` en el "Referencia de comandos del ONTAP".

Comprobar si una dirección IP de cliente es miembro de un grupo de red NFS de ONTAP

Al solucionar problemas de acceso de cliente NFS relacionados con netgroups, puede utilizar el `vserver export-policy netgroup check-membership` comando para determinar si una IP de cliente es miembro de un determinado grupo de red.

Acerca de esta tarea

Al comprobar la pertenencia a un grupo de red, puede determinar si ONTAP sabe que un cliente es o no miembro de un grupo de red. También le permite saber si la caché del netgroup de ONTAP está en un estado transitorio mientras actualiza la información del netgroup. Esta información puede ayudarle a entender por qué se puede conceder o denegar el acceso a un cliente de forma inesperada.

Paso

1. Compruebe la pertenencia a netgroup de una dirección IP de cliente: `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

   El comando puede mostrar los siguientes resultados:

   - El cliente es un miembro del netgroup.

     Esto se ha confirmado mediante una búsqueda inversa o una búsqueda de netgroup-by-host.

   - El cliente es un miembro del netgroup.

     Se encontró en la caché de netgroup de ONTAP.

   - El cliente no es miembro del netgroup.
   - La pertenencia al cliente aún no se puede determinar porque ONTAP está actualizando la caché de netgroup.

     Hasta que esto se haga, la membresía no puede ser explícitamente dentro o fuera. Utilice el `vserver export-policy netgroup queue show` comando para supervisar la carga del grupo de red y vuelva a intentar la comprobación una vez que haya terminado.

Ejemplo

En el siguiente ejemplo, se comprueba si un cliente con la dirección IP 172.17.16.72 es miembro del netgroup Mercury en la SVM vs1:

```
 cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
```

Optimice el rendimiento de la caché de acceso para las SVM NFS de ONTAP

Puede configurar varios parámetros para optimizar la caché de acceso y encontrar el equilibrio perfecto entre el rendimiento y la corriente de la información almacenada en la caché de acceso.

Acerca de esta tarea

Cuando configure los periodos de actualización de la caché de acceso, tenga en cuenta lo siguiente:

- Valores más altos significa que las entradas permanecen más tiempo en la caché de acceso.

  La ventaja es que ofrece un mejor rendimiento, ya que ONTAP gasta menos recursos en actualizar las entradas de la caché de acceso. La desventaja es que si las reglas de la política de exportación cambian y las entradas de la caché de acceso se quedan obsoletas como resultado, se necesita más tiempo para actualizarlas. Como resultado, los clientes que deberían obtener acceso podrían ser denegados, y los clientes que deberían ser denegados podrían obtener acceso.

- Los valores más bajos significan ONTAP que las entradas de la caché de acceso se actualizan con más frecuencia.

  La ventaja es que las entradas son más actuales y es más probable que los clientes se les conceda o deniegue el acceso correctamente. La desventaja es una reducción del rendimiento, ya que ONTAP gasta más recursos en actualizar las entradas de la caché de acceso.

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Realice la acción deseada:

Para modificar…	Introduzca…
Período de actualización para entradas positivas	`vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value`
Actualizar período para entradas negativas	`vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value`
Tiempo de espera para entradas antiguas	`vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value`

3. Compruebe la nueva configuración de parámetros:

   ```
   vserver export-policy access-cache config show-all-vservers
   ```

4. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Administrar bloqueos de archivos

Obtenga información sobre el bloqueo de archivos entre protocolos para SVM NFS de ONTAP

El bloqueo de archivos es un método que utilizan las aplicaciones cliente para evitar que un usuario acceda a un archivo abierto previamente por otro usuario. La forma en que ONTAP bloquea los archivos depende del protocolo del cliente.

Si el cliente es NFS, los bloqueos son consultivos; si el cliente es un cliente SMB, los bloqueos son obligatorios.

Debido a las diferencias entre los bloqueos de archivos NFS y SMB, es posible que un cliente NFS no pueda acceder a un archivo que abrió previamente una aplicación SMB.

Lo siguiente se produce cuando un cliente NFS intenta acceder a un archivo bloqueado por una aplicación SMB:

- En volúmenes mixtos o NTFS, las operaciones de manipulación de archivos `rm` como , , `rmdir` y `mv` pueden provocar el fallo de la aplicación NFS.
- Las operaciones de lectura y escritura de NFS se deniegan en los modos abiertos Deny-Read y Deny-write de SMB, respectivamente.
- Error en las operaciones de escritura de NFS cuando el rango escrito del archivo está bloqueado por un bytelock exclusivo de SMB.

En los volúmenes de estilo de seguridad de UNIX, las operaciones de desenlace y cambio de nombre de NFS ignoran el estado de bloqueo de SMB y permiten el acceso al archivo. Todas las demás operaciones de NFS en volúmenes de estilo de seguridad de UNIX honran el estado de bloqueo de SMB.

Obtenga información sobre los bits de solo lectura para SVM NFS de ONTAP

El bit de sólo lectura se establece en base a archivo para reflejar si un archivo es grabable (deshabilitado) o de sólo lectura (habilitado).

Los clientes SMB que usan Windows pueden establecer un bit de solo lectura por archivo. Los clientes NFS no establecen un bit de solo lectura por archivo, ya que los clientes NFS no tienen ninguna operación de protocolo que utilice un bit de solo lectura por archivo.

ONTAP puede establecer un bit de solo lectura en un archivo cuando un cliente SMB que utiliza Windows crea ese archivo. ONTAP también puede establecer un bit de solo lectura cuando se comparte un archivo entre los clientes NFS y los clientes SMB. Parte del software, cuando lo utilizan los clientes NFS y clientes SMB, requiere que se habilite el bit de solo lectura.

Para que ONTAP mantenga los permisos de lectura y escritura adecuados en un archivo compartido entre clientes NFS y clientes SMB, trata el bit de solo lectura de acuerdo con las siguientes reglas:

- NFS trata cualquier archivo con el bit de solo lectura habilitado como si no tiene bits de permiso de escritura habilitados.
- Si un cliente NFS deshabilita todos los bits de permiso de escritura y al menos uno de esos bits se había habilitado anteriormente, ONTAP habilita el bit de solo lectura para ese archivo.
- Si un cliente NFS habilita algún bit de permiso de escritura, ONTAP deshabilita el bit de solo lectura para ese archivo.
- Si se habilita el bit de solo lectura de un archivo y un cliente NFS intenta detectar permisos para el archivo, los bits de permiso del archivo no se envían al cliente NFS; en su lugar, ONTAP envía los bits de permiso al cliente NFS con los bits de permiso de escritura enmascarados.
- Si se habilita el bit de solo lectura de un archivo y un cliente SMB deshabilita el bit de solo lectura, ONTAP habilita el bit de permiso de escritura del propietario para el archivo.
- Los archivos con el bit de sólo lectura activado sólo son grabables por raíz.

El bit de solo lectura interactúa con los bits de modo ACL y Unix de las siguientes maneras:

Cuando el bit de solo lectura está configurado en un archivo:

- No se realizan cambios en la ACL de ese archivo. Los clientes NFS verán la misma ACL que antes de configurar el bit de solo lectura.
- Se ignoran todos los bits del modo Unix que permiten acceso de escritura al archivo.
- Tanto los clientes NFS como SMB pueden leer el archivo, pero no pueden modificarlo.
- Las ACL y los bits de modo UNIX se ignoran en favor del bit de solo lectura. Esto significa que, incluso si la ACL permite el acceso de escritura, el bit de solo lectura impide las modificaciones.

Cuando el bit de solo lectura no está configurado en un archivo:

- ONTAP determina el acceso según los bits de modo ACL y UNIX.
  - Si los bits del modo ACL o UNIX niegan el acceso de escritura, los clientes NFS y SMB no pueden modificar el archivo.
  - Si ni los bits del modo ACL ni los del modo UNIX niegan el acceso de escritura, los clientes NFS y SMB pueden modificar el archivo.

> Los cambios en los permisos de archivo se aplican inmediatamente en los clientes SMB, pero es posible que no se apliquen de inmediato en los clientes NFS si el cliente NFS habilita el almacenamiento de atributos en caché.

Descubra cómo ONTAP NFS y Windows difieren en el manejo de bloqueos en componentes de rutas compartidas

A diferencia de Windows, ONTAP no bloquea cada componente de la ruta de acceso a un archivo abierto mientras el archivo está abierto. Este comportamiento también afecta a las rutas de recursos compartidos de SMB.

Como ONTAP no bloquea cada componente de la ruta, es posible cambiar el nombre de un componente de ruta por encima del archivo o el recurso compartido abierto, lo que puede provocar problemas en determinadas aplicaciones o hacer que la ruta del recurso compartido en la configuración del SMB no sea válida. Esto puede hacer que el recurso compartido sea inaccesible.

Para evitar problemas causados por el cambio de nombre de los componentes de la ruta de acceso, puede

aplicar la configuración de seguridad Lista de control de acceso (ACL) de Windows que impide que los usuarios o aplicaciones cambien el nombre de los directorios críticos.

Más información sobre "Cómo evitar que se cambie el nombre de los directorios mientras los clientes acceden a ellos".

Mostrar información sobre bloqueos para SVM NFS de ONTAP

Puede mostrar información acerca de los bloqueos de archivos actuales, incluidos los tipos de bloqueos que se conservan y el estado de bloqueo, detalles sobre bloqueos de rango de bytes, modos sharelock, bloqueos de delegación y bloqueos oportunistas, y si se abren bloqueos con identificadores duraderos o persistentes.

Acerca de esta tarea

No se puede mostrar la dirección IP del cliente para los bloqueos establecidos a través de NFSv4 o NFSv4.1.

De forma predeterminada, el comando muestra información sobre todos los bloqueos. Puede usar los parámetros del comando para mostrar información sobre los bloqueos de una máquina virtual de almacenamiento (SVM) específica o para filtrar el resultado del comando según otros criterios.

El `vserver locks show` comando muestra información sobre cuatro tipos de bloqueos:

- Bloqueos de rango de bytes, que bloquean sólo una parte de un archivo.
- Bloqueos de uso compartido, que bloquean los archivos abiertos.
- Bloqueos oportunistas, que controlan el almacenamiento en caché en el cliente a través de SMB.
- Delegaciones, que controlan el almacenamiento en caché en el cliente a través de NFSv4.x.

Al especificar parámetros opcionales, puede determinar información importante sobre cada tipo de bloqueo. Obtenga más información sobre `vserver locks show` en el "Referencia de comandos del ONTAP".

Paso

1. Muestra información sobre los bloqueos mediante `vserver locks show` el comando.

Ejemplos

El siguiente ejemplo muestra información de resumen para un bloqueo NFSv4 en un archivo con la ruta `/vol1/file1`. El modo de acceso sharelock es write-deny_none, y el bloqueo se concedió mediante la delegación de escritura:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                         delegation  -
               Delegation Type: write
```

El siguiente ejemplo muestra información detallada sobre el bloqueo operativo y el bloqueo compartido sobre el bloqueo SMB en un archivo con la ruta de acceso `/data2/data2_2/intro.pptx`. Se concede un identificador duradero en el archivo con un modo de acceso de bloqueo compartido de Write-Deny_none a un cliente con una dirección IP de 10.3.1.3. Un plock de arrendamiento se concede con un nivel de plock por lotes:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
              Lock Protocol: cifs
                  Lock Type: share-level
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/test.pptx
                  Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
```

```
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Romper bloqueos de archivos para SVMs NFS de ONTAP

Cuando los bloqueos de archivos impiden que los clientes accedan a los archivos, puede mostrar información sobre los bloqueos retenidos actualmente y romperán bloqueos específicos. Entre los ejemplos de escenarios en los que es posible que necesite romper los bloqueos se incluyen las aplicaciones de depuración.

Acerca de esta tarea

`vserver locks break`El comando solo está disponible en el nivel de privilegios avanzado y superior. Obtenga más información sobre `vserver locks break` en el link:https://docs.netapp.com/us-en/ontap-cli/vserver-locks-break.html["Referencia de comandos del ONTAP"^].

Pasos

1. Para encontrar la información que necesita para romper un bloqueo, utilice el `vserver locks show` comando.

   Obtenga más información sobre `vserver locks show` en el "Referencia de comandos del ONTAP".

2. Configure el nivel de privilegio en Advanced:

   `set -privilege advanced`

3. Ejecute una de las siguientes acciones:

Si desea romper un bloqueo especificando…	Introduzca el comando…
El nombre de SVM, el nombre del volumen, el nombre de LIF y la ruta de archivo	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`

El ID del bloqueo	`vserver locks break -lockid UUID`

4. Vuelva al nivel de privilegio de administrador:

   `set -privilege admin`

Descubra cómo funcionan los filtros de primera lectura y primera escritura de ONTAP FPolicy con NFS

Los clientes NFS experimentan un tiempo de respuesta elevado durante el tráfico elevado de solicitudes de lectura/escritura cuando se habilita FPolicy mediante un servidor FPolicy externo con operaciones de lectura/escritura como eventos supervisados. Para los clientes NFS, el uso de filtros de primera lectura y primera escritura en FPolicy reduce el número de notificaciones de FPolicy y mejora el rendimiento.

En NFS, el cliente realiza operaciones de I/o en un archivo mediante la recuperación de su gestor. Este identificador puede seguir siendo válido durante todos los reinicios del servidor y el cliente. Por lo tanto, el cliente puede almacenar en caché el identificador y enviar solicitudes al mismo sin recuperar los controladores de nuevo. En una sesión normal, se envían muchas solicitudes de lectura/escritura al servidor de archivos. Si se generan notificaciones para todas estas solicitudes, se podrían producir los siguientes problemas:

- Mayor carga gracias al procesamiento de notificaciones adicional y al mayor tiempo de respuesta.
- Un gran número de notificaciones que se envían al servidor de FPolicy aunque el servidor no se vea afectado por todas las notificaciones.

Después de recibir la primera solicitud de lectura/escritura de un cliente para un archivo concreto, se crea una entrada de caché y se aumenta el número de lectura/escritura. Esta solicitud se Marca como la primera operación de lectura/escritura y se genera un evento FPolicy. Antes de planificar y crear los filtros FPolicy para un cliente NFS, debe comprender los conceptos básicos de cómo funcionan los filtros FPolicy.

- Primera lectura: Filtra las solicitudes de lectura del cliente para la primera lectura.

  Cuando se utiliza este filtro para eventos NFS, la `-file-session-io-grouping-count` `-file -session-io-grouping-duration` configuración y determinan la solicitud de primera lectura para la que se procesa FPolicy.

- Primera escritura: Filtra las solicitudes de escritura del cliente para la primera escritura.

  Cuando se utiliza este filtro para eventos NFS, la `-file-session-io-grouping-count` `-file -session-io-grouping-duration` configuración determina la solicitud de escritura para la que se procesó FPolicy.

Las siguientes opciones se agregan a la base de datos de servidores NFS.

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

Modificar el ID de implementación del servidor NFSv4.1 para las SVM de ONTAP

El protocolo NFSv4.1 incluye un ID de implementación del servidor que documenta el dominio, el nombre y la fecha del servidor. Puede modificar los valores predeterminados del ID de implementación del servidor. Cambiar los valores predeterminados puede ser útil, por ejemplo, al recopilar estadísticas de uso o solucionar problemas de interoperabilidad. Para obtener más información, consulte RFC 5661.

Acerca de esta tarea

Los valores predeterminados de las tres opciones son los siguientes:

Opción	Nombre de la opción	Valor predeterminado
Dominio de ID de implementación de NFSv4.1	`-v4.1-implementation -domain`	netapp.com
Nombre de ID de implementación de NFSv4.1	`-v4.1-implementation-name`	Nombre de la versión del clúster
Fecha del ID de implementación de NFSv4.1	`-v4.1-implementation-date`	Fecha de versión del clúster

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Ejecute una de las siguientes acciones:

Si desea modificar el ID de implementación de NFSv4.1…	Introduzca el comando…
Dominio	`vserver nfs modify -v4.1 -implementation-domain domain`
Nombre	`vserver nfs modify -v4.1 -implementation-name name`

Si desea modificar el ID de implementación de NFSv4.1…	Introduzca el comando…
Fecha	`vserver nfs modify -v4.1 -implementation-date date`

3. Vuelva al nivel de privilegio de administrador:

   `set -privilege admin`

Gestione las ACL de NFSv4

Conozca los beneficios de habilitar las ACL de NFSv4 para las SVM de ONTAP

Existen muchas ventajas a la hora de habilitar las ACL de NFSv4.

Entre las ventajas de habilitar las ACL de NFSv4 se incluyen las siguientes:

- Control más detallado del acceso de los usuarios a archivos y directorios
- Mejor seguridad NFS
- Interoperabilidad mejorada con CIFS
- Eliminación de la limitación de NFS de 16 grupos por usuario

Obtenga información sobre las ACL de NFSv4 para SVM de ONTAP

Un cliente que utilice las ACL de NFSv4 puede establecer y ver las ACL en archivos y directorios del sistema. Cuando se crea un nuevo archivo o subdirectorio en un directorio que tiene una ACL, el nuevo archivo o subdirectorio hereda todas las entradas de control de acceso (ACE) en la ACL que se han etiquetado con los indicadores de herencia adecuados.

Cuando se crea un archivo o un directorio como resultado de una solicitud de NFSv4, la ACL del archivo o directorio resultante depende de si la solicitud de creación de archivos incluye una ACL o solo permisos de acceso estándar a archivos UNIX y si el directorio principal tiene una ACL:

- Si la solicitud incluye una ACL, se utiliza esa ACL.
- Si la solicitud incluye sólo permisos de acceso estándar a archivos UNIX pero el directorio principal tiene una ACL, el archivo o directorio nuevos heredan los ACE de la ACL del directorio principal siempre que se hayan etiquetado los ACE con los indicadores de herencia correspondientes.

  Una ACL principal se hereda incluso si `-v4.0-acl` se establece en `off`.

- Si la solicitud incluye sólo permisos de acceso estándar a archivos UNIX y el directorio principal no tiene una ACL, el modo de archivo de cliente se utiliza para establecer permisos de acceso estándar a archivos UNIX.
- Si la solicitud incluye sólo permisos de acceso estándar a archivos UNIX y el directorio primario tiene una ACL no heredable, el nuevo objeto se crea sólo con bits de modo.

Si el `-chown-mode` parámetro se ha establecido en `restricted` con comandos en `vserver nfs` `vserver export-policy rule` las familias o, la propiedad del archivo solo puede ser cambiada por el superusuario, incluso si los permisos en disco establecidos con NFSv4 ACL permiten a un usuario que no sea root cambiar la propiedad del archivo. Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

Habilitar o deshabilitar la modificación de ACL de NFSv4 para SVM de ONTAP

Cuando ONTAP recibe un `chmod` comando para un archivo o directorio con una ACL, de forma predeterminada, la ACL se conserva y se modifica para reflejar el cambio de bits de modo. Puede desactivar el `-v4-acl-preserve` parámetro para cambiar el comportamiento si desea que se borre la ACL en su lugar.

Acerca de esta tarea

Cuando se utiliza un estilo de seguridad unificado, este parámetro también especifica si los permisos de archivo NTFS se conservan o se borran cuando un cliente envía un comando chmod, chgroup o chown para un archivo o directorio.

El valor predeterminado de este parámetro es Enabled.

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el siguiente comando…
Habilitación de la retención y modificación de las ACL de NFSv4 existentes (predeterminado)	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
Deshabilite la retención y borre las ACL de NFSv4 cuando cambie los bits de modo	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

3. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Descubra cómo ONTAP utiliza las ACL de NFSv4 para determinar si puede eliminar archivos

Para determinar si puede eliminar un archivo, ONTAP utiliza una combinación del bit DE ELIMINACIÓN del archivo y el bit DELETE_CHILD del directorio que lo contiene. Para obtener más información, consulte NFS 4.1 RFC 5661.

Habilitar o deshabilitar las ACL de NFSv4 para las SVM de ONTAP

Para activar o desactivar las ACL de NFSv4, puede modificar las `-v4.0-acl` `-v4.1-acl` opciones y. Estas opciones están desactivadas de forma predeterminada.

Acerca de esta tarea

`-v4.0-acl` `-v4.1-acl`La opción o controla la configuración y visualización de las ACL de NFSv4; no controla la aplicación de estas ACL para la comprobación de acceso.

Paso

1. Ejecute una de las siguientes acciones:

Si desea…	Realice lo siguiente…
Habilite las ACL de NFSv4.0	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
Deshabilitar las ACL de NFSv4.0	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
Habilite las ACL de NFSv4.1	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`
Deshabilitar las ACL de NFSv4.1	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

Modificar el límite máximo de ACE para las ACL de NFSv4 para las SVM de ONTAP

Puede modificar el Núm. Máximo de ACE permitidos para cada ACL NFSv4 modificando el parámetro `-v4-acl-max-aces`. De forma predeterminada, el límite se establece en 400 ACE para cada ACL. El aumento de este límite puede ayudar a garantizar una correcta migración de datos con ACL que contengan más de 400 ACE en sistemas de almacenamiento que ejecuten ONTAP.

Acerca de esta tarea

Si aumenta este límite, el rendimiento de los clientes que acceden a archivos con ACL de NFSv4.

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Modifique el límite máximo de ACE para ACL de NFSv4:

   ```
   vserver nfs modify -v4-acl-max-aces max_ace_limit
   ```

   El rango válido de

   `max_ace_limit` es a. `192` `1024.`

3. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Gestione las delegaciones de archivos NFSv4

Habilitar o deshabilitar las delegaciones de archivos de lectura NFSv4 para SVM de ONTAP

Para habilitar o deshabilitar las delegaciones de archivos de lectura de NFSv4, puede modificar `-v4.0-read-delegation`la opción o. Al activar las delegaciones de archivos de lectura, puede eliminar gran parte de la sobrecarga de mensajes asociada con la apertura y el cierre de archivos.

Acerca de esta tarea

De forma predeterminada, las delegaciones de archivos de lectura están deshabilitadas.

La desventaja de habilitar las delegaciones de archivos de lectura es que el servidor y sus clientes deben recuperar las delegaciones una vez que se reinicia o reinicia el servidor, se reinicia o reinicia un cliente o se produce una partición de red.

Paso

1. Ejecute una de las siguientes acciones:

Si desea…	Realice lo siguiente…
Habilitar las delegaciones de archivos de lectura de NFSv4	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled`
Habilitar las delegaciones de archivos de lectura de NFSv4.1	Introduzca el siguiente comando: + `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled`

Deshabilitar las delegaciones de archivos de lectura de NFSv4	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled`
Deshabilitar las delegaciones de archivos de lectura de NFSv4.1	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled`

Resultado

Las opciones de delegación de archivos surten efecto tan pronto como se cambien. No es necesario reiniciar o reiniciar NFS.

Habilitar o deshabilitar las delegaciones de archivos de escritura NFSv4 para SVM de ONTAP

Para habilitar o deshabilitar las delegaciones de archivos de escritura, puede modificar `-v4.0-write-delegation`la opción o. Al habilitar las delegaciones de archivos de escritura, puede eliminar gran parte de la sobrecarga de mensajes asociada con el bloqueo de archivos y registros, además de abrir y cerrar archivos.

Acerca de esta tarea

De forma predeterminada, las delegaciones de archivos de escritura están deshabilitadas.

La desventaja de habilitar las delegaciones de archivos de escritura es que el servidor y sus clientes deben realizar tareas adicionales para recuperar delegaciones una vez que se reinicia o reinicia el servidor, un cliente se reinicia o reinicia, o se produce una partición de red.

Paso

1. Ejecute una de las siguientes acciones:

Si desea…	Realice lo siguiente…
Habilite las delegaciones de archivos de escritura de NFSv4	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled`
Habilite las delegaciones de archivos de escritura de NFSv4,1	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled`
Deshabilitar las delegaciones de archivos de escritura de NFSv4	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled`

Si desea…	Realice lo siguiente…
Deshabilitar las delegaciones de archivos de escritura de NFSv4.1	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled`

Resultado

Las opciones de delegación de archivos surten efecto tan pronto como se cambien. No es necesario reiniciar o reiniciar NFS.

Configure el bloqueo de archivos y registros de NFSv4

Obtenga información sobre el bloqueo de archivos y registros NFSv4 para SVM de ONTAP

En el caso de los clientes NFSv4, ONTAP admite el mecanismo de bloqueo de archivos NFSv4 y mantiene el estado de todos los bloqueos de archivos bajo un modelo basado en arrendamiento.

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

Especifique el período de concesión de bloqueo de NFSv4 para las SVM de ONTAP

Para especificar el periodo de concesión de bloqueo NFSv4 (es decir, el período en el que ONTAP otorga un bloqueo de forma irrevocable a un cliente), puede modificar `-v4 -lease-seconds` la opción. Los periodos de concesión más breves aceleran la recuperación del servidor, a la vez que los periodos de concesión más largos son beneficiosos para los servidores que gestionan una gran cantidad de clientes.

Acerca de esta tarea

De forma predeterminada, esta opción se establece en `30`. El valor mínimo para esta opción es `10`. El valor máximo de esta opción es el período de gracia de bloqueo, que se puede definir con la `locking.lease_seconds` opción.

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Introduzca el siguiente comando:

   ```
   vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
   ```

3. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Especifique el período de gracia de bloqueo de NFSv4 para las SVM de ONTAP

Para especificar el período de gracia de bloqueo NFSv4 (es decir, el período de tiempo en el que los clientes intentan reclamar su estado de bloqueo de ONTAP durante la recuperación del servidor), puede modificar la `-v4-grace-seconds` opción.

Acerca de esta tarea

De forma predeterminada, esta opción se establece en `45`.

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Introduzca el siguiente comando:

   ```
   vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
   ```

3. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Obtenga información sobre las referencias de NFSv4 para SVM de ONTAP

Al activar las referencias de NFSv4, ONTAP proporciona referencias «'intra-SVM» a los clientes de NFSv4. La referencia dentro de SVM se produce cuando un nodo de clúster que recibe la solicitud NFSv4 hace referencia al cliente NFSv4 a otra interfaz lógica (LIF) de la máquina virtual de almacenamiento (SVM).

El cliente NFSv4 debe acceder a la ruta que ha recibido la referencia en la LIF de destino desde ese punto. El nodo de clúster original proporciona una referencia de este tipo cuando determina que hay una LIF en la SVM que reside en el nodo de clúster en el que reside el volumen de datos, lo cual permite que los clientes accedan más rápido a los datos y eviten una comunicación adicional del clúster.

Habilitar o deshabilitar referencias NFSv4 para SVM de ONTAP

Puede habilitar las referencias NFSv4 en las máquinas virtuales de almacenamiento (SVM) mediante la habilitación de las opciones `-v4-fsid-change` y `-v4.0 -referralso`. La habilitación de las referencias A NFSV4 puede resultar en un acceso más rápido a los datos para los clientes de NFSv4 que admiten esta función.

Antes de empezar

Si desea habilitar las referencias NFS, primero debe deshabilitar NFS paralelo. No puede habilitar ambos a la vez.

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el comando…
Activar NFSv4 referencias	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled`
Deshabilitar las referencias de NFSv4	`vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled`
Activar NFSv4,1 referencias	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled`
Deshabilitar las referencias de NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled`

3. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Mostrar estadísticas para SVM de ONTAP NFS

Puede mostrar estadísticas de NFS para las máquinas virtuales de almacenamiento (SVM) en el sistema de almacenamiento para supervisar el rendimiento y diagnosticar problemas.

Pasos

1. Utilice `statistics catalog object show` el comando para identificar los objetos NFS desde los que puede ver los datos.

   ```
   statistics catalog object show -object nfs*
   ```

2. Utilice `statistics start` `statistics stop` los comandos opcionales y para recopilar una muestra de datos de uno o más objetos.
3. Utilice `statistics show` el comando para ver los datos de ejemplo.

Ejemplo: Supervisión del rendimiento de NFSv3

El siguiente ejemplo muestra datos de rendimiento para el protocolo NFSv3.

El siguiente comando inicia la recogida de datos de una nueva muestra:

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

El siguiente comando muestra datos de la muestra especificando contadores que muestran el número de solicitudes de lectura y escritura correctas, en comparación con el número total de solicitudes de lectura y

escritura:

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                     Value
    -------------------------- ----------------------------
    read_success                                40042
    read_total                                  40042
    write_success                             1492052
    write_total                               1492052
```

Información relacionada

- "Configuración de supervisión del rendimiento"
- "Catálogo de estadísticas de objetos mostrados"
- "Las estadísticas muestran"
- "Las estadísticas comienzan"
- "las estadísticas se detienen"

Mostrar estadísticas de DNS para SVM NFS de ONTAP

Puede mostrar estadísticas de DNS para las máquinas virtuales de almacenamiento (SVM) en el sistema de almacenamiento para supervisar el rendimiento y diagnosticar problemas.

Pasos

1. Utilice `statistics catalog object show` el comando para identificar los objetos DNS desde los que puede ver datos.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Use `statistics start` `statistics stop` los comandos y para recopilar una muestra de datos de uno o más objetos.
3. Utilice `statistics show` el comando para ver los datos de ejemplo.

Supervisar las estadísticas de DNS

Los siguientes ejemplos muestran datos de rendimiento para las consultas DNS. Los siguientes comandos inician la recopilación de datos de una nueva muestra:

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

El siguiente comando muestra datos de la muestra especificando contadores que muestran el número de consultas DNS enviadas en comparación con el número de consultas DNS recibidas, con errores o con tiempo de espera agotado:

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            0
    num_requests_sent                                               1
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

El siguiente comando muestra los datos de la muestra especificando contadores que muestran el número de veces que se recibió un error específico para una consulta DNS en el servidor concreto:

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                             NXDOMAIN
    server_ip_address                                   10.72.219.109
3 entries were displayed.
```

Información relacionada

- "Configuración de supervisión del rendimiento"
- "Catálogo de estadísticas de objetos mostrados"
- "Las estadísticas muestran"
- "Las estadísticas comienzan"
- "las estadísticas se detienen"

Mostrar estadísticas NIS para SVM NFS de ONTAP

Puede mostrar estadísticas de NIS para las máquinas virtuales de almacenamiento (SVM) en el sistema de almacenamiento para supervisar el rendimiento y diagnosticar problemas.

Pasos

1. Utilice el `statistics catalog object show` comando para identificar los objetos NIS desde los que puede ver los datos.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Use `statistics start` `statistics stop` los comandos y para recopilar una muestra de datos de uno o más objetos.
3. Utilice `statistics show` el comando para ver los datos de ejemplo.

Supervisar las estadísticas de NIS

Los siguientes ejemplos muestran datos de rendimiento para consultas NIS. Los siguientes comandos inician la recopilación de datos de una nueva muestra:

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

El siguiente comando muestra los datos de la muestra especificando contadores que muestran el número de consultas NIS enviadas en comparación con el número de consultas NIS recibidas, fallidas o con el tiempo de espera agotado:

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                        0
    num_request_failures                                           1
    num_requests_sent                                              2
    num_responses_received                                         1
    num_successful_responses                                       1
    num_timeouts                                                   0
6 entries were displayed.
```

El siguiente comando muestra los datos de la muestra especificando contadores que muestran el número de veces que se recibió un error específico para una consulta NIS en el servidor concreto:

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                            YP_NOTFOUND
    server_ip_address                                     10.227.13.221
3 entries were displayed.
```

Información relacionada

- "Configuración de supervisión del rendimiento"
- "Catálogo de estadísticas de objetos mostrados"
- "Las estadísticas muestran"
- "Las estadísticas comienzan"
- "las estadísticas se detienen"

Obtenga información sobre la compatibilidad con VMware vStorage sobre ONTAP NFS

ONTAP admite ciertas funciones de VMware vStorage APIs for Array Integration (VAAI) en un entorno NFS.

Funciones admitidas

Se admiten las siguientes funciones:

- Descarga de copias

  Permite que un host ESXi copie máquinas virtuales o discos de máquinas virtuales (VMDK) directamente entre la ubicación de almacén de datos de origen y destino sin implicar al host. Esto ahorra ciclos de CPU del host ESXi y ancho de banda de red. La descarga de copia preserva la eficiencia del espacio si el volumen de origen es escaso.

- Reserva de espacio

  Garantiza espacio de almacenamiento para un archivo VMDK reservando espacio para él.

Limitaciones

VMware vStorage over NFS tiene las siguientes limitaciones:

- Las operaciones de descarga de copia pueden fallar en las siguientes situaciones:
  - Mientras se ejecuta waiflron en el volumen de origen o de destino porque desconecta temporalmente el volumen
  - Al mover el volumen de origen o el de destino
  - Al mover las LIF de origen o de destino
  - Al realizar operaciones de toma de control o devolución del retorno al nodo primario
  - Al mismo tiempo que realiza operaciones de conmutación de sitios o conmutación de estado
- La copia del servidor puede fallar debido a diferencias de formato de gestión de archivos en el siguiente escenario:

  Se intentan copiar datos de las SVM que tienen actualmente o habían exportado qtrees anteriormente a las SVM que nunca han exportado qtrees. Para solucionar esta limitación, puede exportar al menos un qtree en la SVM de destino.

Información relacionada

"¿Qué operaciones de VAAI descargados son compatibles con Data ONTAP?"

Habilitar o deshabilitar VMware vStorage sobre ONTAP NFS

Puede habilitar o deshabilitar la compatibilidad con VMware vStorage over NFS en máquinas virtuales de almacenamiento (SVM) mediante `vserver nfs modify` el comando.

Acerca de esta tarea

De forma predeterminada, la compatibilidad con VMware vStorage over NFS está deshabilitada.

Pasos

1. Mostrar el estado actual de soporte de vStorage para las SVM:

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

2. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el siguiente comando…
Activar la compatibilidad con VMware vStorage	`vserver nfs modify -vserver vserver_name -vstorage enabled`
Desactivar la compatibilidad con VMware vStorage	`vserver nfs modify -vserver vserver_name -vstorage disabled`

Después de terminar

Para poder utilizar esta funcionalidad, es necesario instalar el plugin de NFS para VMware VAAI. Para obtener más información, consulte *Installing the NetApp NFS Plug-in for VMware VAAI*.

Información relacionada

"Documentación de NetApp: Plugin de NetApp NFS para VMware VAAI"

Habilitar o deshabilitar la compatibilidad con rquota en SVM NFS de ONTAP

El protocolo de cuota remota (rquota) permite a los clientes NFS obtener información de cuotas para los usuarios de un equipo remoto. La compatibilidad con las versiones rquota varía según la versión de ONTAP.

- Rquota v1 es compatible con ONTAP 9 y versiones posteriores.
- Rquota v2 es compatible con ONTAP 9.12.1 y versiones posteriores.

  Si actualiza de rquota v1 a rquota v2, es posible que observe un cambio inesperado en el límite de cuota de usuario. Este cambio se debe a la diferencia en la forma en que se calcula la cuota entre rquota v1 y rquota v2. Para obtener más información, consulte la"Base de conocimientos de NetApp : ¿Por qué el límite de cuota de usuario cambió inesperadamente?" .

Acerca de esta tarea

De forma predeterminada, rquota está desactivado.

Paso

1. Habilitar o deshabilitar rquota:

Si desea…	Introduzca el siguiente comando…
Habilite la compatibilidad de rquota para SVM	`vserver nfs modify -vserver vserver_name -rquota enable`
Deshabilite el soporte rquota para SVM	`vserver nfs modify -vserver vserver_name -rquota disable`

Para obtener más información sobre las cuotas, consulte "Gestión de almacenamiento lógico".

Obtenga información sobre las mejoras de rendimiento de NFSv3 y NFSv4 y el tamaño de transferencia TCP para SVM de ONTAP

Puede mejorar el rendimiento de los clientes NFSv3 y NFSv4 que se conectan a los sistemas de almacenamiento a través de una red de alta latencia al modificar el tamaño máximo de transferencia de TCP.

Cuando los clientes acceden a los sistemas de almacenamiento a través de una red de alta latencia, como una red de área extensa (WAN) o una red de área metropolitana (MAN) con una latencia superior a 10 milisegundos, es posible que pueda mejorar el rendimiento de la conexión modificando el tamaño máximo de transferencia de TCP. Los clientes que acceden a sistemas de almacenamiento en una red de baja latencia, como una red de área local (LAN), pueden esperar muy poco o ningún beneficio de la modificación de estos

parámetros. Si la mejora del rendimiento no supera el impacto en la latencia, no debe usar estos parámetros.

Para determinar si su entorno de almacenamiento se beneficiaría de la modificación de estos parámetros, primero debe realizar una evaluación completa del rendimiento de un cliente NFS de bajo rendimiento. Revise si el bajo rendimiento se debe a una latencia excesiva de ida y vuelta y una solicitud pequeña en el cliente. En estas condiciones, el cliente y el servidor no pueden utilizar por completo el ancho de banda disponible porque gastan la mayoría de sus ciclos de servicio esperando a que pequeñas solicitudes y respuestas se transmitan a través de la conexión.

Al aumentar el tamaño de las solicitudes de NFSv3 y NFSv4, el cliente y el servidor pueden utilizar el ancho de banda disponible de forma más eficaz para mover más datos por unidad y, de este modo, aumentar la eficiencia general de la conexión.

Tenga en cuenta que la configuración entre el sistema de almacenamiento y el cliente puede variar. El sistema de almacenamiento y el cliente admiten un tamaño máximo de 1 MB para las operaciones de transferencia. Sin embargo, si configura el sistema de almacenamiento para que admita un tamaño de transferencia máximo de 1 MB pero el cliente solo admita 64 KB, el tamaño de transferencia de montaje estará limitado a 64 KB o menos.

Antes de modificar estos parámetros, debe tener en cuenta que genera un consumo adicional de memoria en el sistema de almacenamiento durante el período de tiempo necesario para ensamblar y transmitir una gran respuesta. Cuanto más conexiones de alta latencia tenga con el sistema de almacenamiento, mayor será el consumo de memoria adicional. Los sistemas de almacenamiento con una gran capacidad de memoria pueden experimentar un efecto muy reducido a partir de este cambio. Los sistemas de almacenamiento con baja capacidad de memoria pueden experimentar una degradación considerable del rendimiento.

El uso correcto de este parámetro depende de la capacidad de recuperar datos de varios nodos de un clúster. La latencia inherente de la red de clúster podría aumentar la latencia general de la respuesta. La latencia general tiende a aumentar cuando se usa estos parámetros. Como resultado, las cargas de trabajo sensibles a la latencia pueden mostrar un impacto negativo.

Modificar el tamaño máximo de transferencia TCP de NFSv3 y NFSv4 para SVM de ONTAP

Puede modificar `-tcp-max-xfer-size` la opción de configurar tamaños de transferencia máximos para todas las conexiones TCP mediante los protocolos NFSv3 y NFSv4.x.

Acerca de esta tarea

Puede modificar estas opciones de forma individual para cada máquina virtual de almacenamiento (SVM).

A partir de ONTAP 9, las `v3-tcp-max-read-size` `v3-tcp-max-write-size` opciones y están obsoletas. `-tcp-max-xfer-size`En su lugar, debe usar la opción.

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el comando…
Modifique el tamaño de transferencia máximo de TCP de NFSv3 o NFSv4	`vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size`

Opción	Rango	Predeterminado
`-tcp-max-xfer-size`	de 8192 a 1048576 bytes	65536 bytes

El tamaño de transferencia máximo introducido debe ser un múltiplo de 4 KB (4096 bytes). Las solicitudes que no están alineadas correctamente afectan negativamente al rendimiento.

3. Utilice `vserver nfs show -fields tcp-max-xfer-size` el comando para verificar los cambios.
4. Si alguno de los clientes utiliza montajes estáticos, desmonte y vuelva a montar para que el nuevo tamaño de parámetro entre en vigor.

Ejemplo

El siguiente comando establece el tamaño de transferencia máximo de TCP de NFSv3 y NFSv4.x en 1048576 bytes de la SVM llamada vs1:

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

Configurar la cantidad de ID de grupo permitidos para usuarios de NFS para SVM de ONTAP

De forma predeterminada, ONTAP admite hasta 32 identificadores de grupo al gestionar credenciales de usuario de NFS mediante la autenticación Kerberos (RPCSEC_GSS). Cuando se utiliza la autenticación AUTH_SYS, el número máximo predeterminado de ID de grupo es 16, tal como se define en RFC 5531. Puede aumentar el máximo hasta 1,024 si tiene usuarios que son miembros de más del número predeterminado de grupos.

Acerca de esta tarea

Si un usuario tiene más de la cantidad predeterminada de identificadores de grupo en sus credenciales, los ID de grupo restantes se truncarán y el usuario podría recibir errores al intentar acceder a los archivos desde el sistema de almacenamiento. Debe establecer el número máximo de grupos, por SVM, en un número que represente los grupos máximos en su entorno.

Para comprender los requisitos previos de autenticación AUTH_SYS para habilitar grupos extendidos(`-auth-sys-extended-groups`) que utilizan identificadores de grupo más allá del máximo predeterminado de 16, consulte la"Base de conocimientos de NetApp : ¿Cuáles son los requisitos previos para habilitar auth-sys-extended-groups?"

La siguiente tabla muestra los dos parámetros del `vserver nfs modify` comando que determinan el número máximo de ID de grupo en tres configuraciones de ejemplo:

Parámetros	Configuración	Límite de ID de grupo resultante

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`32`
	
	`disabled`
	
	Esta es la configuración predeterminada.
		RPCSEC_GSS: 32
		
		AUTH_SYS: 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`256`
	
	`disabled`
		RPCSEC_GSS: 256
		
		AUTH_SYS: 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`512`
	
	`enabled`
		RPCSEC_GSS: 512
		
		AUTH_SYS: 512

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Realice la acción deseada:

Si desea establecer el número máximo de grupos auxiliares permitidos…	Introduzca el comando…
Sólo para RPCSEC_GSS y deje AUTH_SYS establecido en el valor predeterminado de 16	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled`
Para RPCSEC_GSS y AUTH_SYS	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled`

3. Verifique el `-extended-groups-limit` valor y verifique si AUTH_SYS está utilizando grupos extendidos: `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`
4. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Ejemplo

En el ejemplo siguiente se habilitan grupos extendidos para la autenticación AUTH_SYS y se establece el número máximo de grupos extendidos en 512 para la autenticación AUTH_SYS y RPCSEC_GSS. Estos cambios se realizan solo para los clientes que acceden al SVM denominado vs1:

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
------- ------------------------ --------------------
vs1     enabled                  512

vs1::*> set -privilege admin
```

Información relacionada

- "Base de conocimientos de NetApp : Cambios en los grupos extendidos AUTH_SYS para la autenticación NFS para ONTAP 9"

Controlar el acceso del usuario root a los datos de estilo de seguridad NTFS para SVM de ONTAP

Puede configurar ONTAP para permitir que los clientes NFS accedan a datos de estilo de seguridad NTFS y a clientes NTFS para acceder a los datos de estilo de seguridad NFS. Cuando se utiliza un estilo de seguridad NTFS en un almacén de datos NFS, se debe decidir cómo tratar el acceso por parte del usuario raíz y configurar la máquina virtual de almacenamiento (SVM) según corresponda.

Acerca de esta tarea

Cuando un usuario raíz accede a datos de estilo de seguridad NTFS, tiene dos opciones:

- Asignar el usuario raíz a un usuario de Windows como cualquier otro usuario NFS y gestionar el acceso según ACL de NTFS.
- Ignorar las ACL de NTFS y proporcionar acceso completo a la raíz.

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Realice la acción deseada:

Si desea que el usuario raíz…	Introduzca el comando…

Estar asignado a un usuario de Windows	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled`
Omitir la comprobación de ACL de NT	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled`

De manera predeterminada, este parámetro está deshabilitado.

Si este parámetro está habilitado pero no hay ninguna asignación de nombres para el usuario raíz, ONTAP utiliza una credencial de administrador de SMB predeterminada para la auditoría.

3. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Admiten versiones y clientes NFS

Obtenga información sobre las versiones y los clientes NFS de ONTAP compatibles

Antes de poder utilizar NFS en la red, debe saber qué versiones de NFS y clientes admite ONTAP.

Esta tabla indica si las versiones de protocolo NFS principales y secundarias son compatibles de forma predeterminada con ONTAP. La compatibilidad de forma predeterminada no indica que esta es la versión más antigua de ONTAP compatible con ese protocolo NFS.

Versión	Compatible	Introducido
NFSv3	Sí	Todos los lanzamientos de ONTAP
NFSv4.0	Sí	ONTAP 8
NFSv4.1	Sí	ONTAP 8,1
NFSv4.2	Sí	ONTAP 9,8
PNFs	Sí	ONTAP 8,1

Para obtener la información más reciente sobre la compatibilidad con ONTAP para clientes NFS, consulte la matriz de interoperabilidad.

"Herramienta de matriz de interoperabilidad de NetApp"

Obtenga información sobre la compatibilidad de ONTAP con la funcionalidad NFSv4.0

ONTAP admite todas las funciones obligatorias de NFSv4.0 excepto los mecanismos de seguridad SPKM3 y LIPKEY.

Se admiten las siguientes funciones DE NFSV4:

- **COMPUESTO**

  Permite a un cliente solicitar varias operaciones de archivo en una única solicitud de llamada a procedimiento remoto (RPC).

- **Delegación de archivos**

  Permite al servidor delegar el control de archivos en algunos tipos de clientes para el acceso de lectura y escritura.

- **Pseudofs**

  Los servidores NFSv4 los utilizan para determinar los puntos de montaje del sistema de almacenamiento. No existe ningún protocolo de montaje en NFSv4.

- **Bloqueo**

  Basado en arrendamiento. No hay protocolos NLM (Network Lock Manager) o NSM (Network Status Monitor) separados en NFSv4.

Para obtener más información acerca del protocolo NFSv4.0, consulte RFC 3530.

Conozca las limitaciones de compatibilidad de ONTAP para NFSv4

Debe conocer varias limitaciones del soporte de ONTAP para NFSv4.

- La función de delegación no es compatible con todos los tipos de cliente.
- En ONTAP 9.4 y versiones anteriores, el sistema de almacenamiento rechaza los nombres con caracteres no ASCII en volúmenes distintos a UTF8.

  En ONTAP 9.5 y versiones posteriores, los volúmenes creados con la configuración de idioma utf8mb4 y montados con NFS v4 ya no están sujetos a esta restricción.

- Todos los identificadores de archivos son persistentes; el servidor no proporciona identificadores de archivos volátiles.
- No se admiten la migración ni la replicación.
- Los clientes NFSv4 no son compatibles con los reflejos de uso compartido de carga de solo lectura.

  ONTAP enruta los clientes NFSv4 al origen de la duplicación de uso compartido de la carga para obtener acceso directo de lectura y escritura.

- No se admiten los atributos con nombre.
- Se admiten todos los atributos recomendados, excepto los siguientes:

- archive
- hidden
- homogeneous
- mimetype
- quota_avail_hard
- quota_avail_soft
- quota_used
- system
- time_backup

> Aunque no admite los `quota*` atributos, ONTAP admite cuotas de usuarios y grupos a través del protocolo de banda lateral RQUOTA.

Obtenga más información sobre la compatibilidad de ONTAP con NFSv4.1

A partir de ONTAP 9.8, la funcionalidad nconnect está disponible de forma predeterminada con NFSv4.1 habilitado.

En las implementaciones anteriores de clientes NFS solo se utiliza una única conexión TCP con un montaje. En ONTAP, una única conexión TCP puede convertirse en un cuello de botella que aumenta las IOPS.

nconnect mejora el rendimiento del cliente NFS al permitir múltiples conexiones TCP (hasta 16) para un solo montaje, lo que ayuda a superar el cuello de botella de rendimiento que puede ocurrir con una sola conexión TCP a medida que aumentan las IOPS.

NFSv4.1 está habilitado de forma predeterminada en ONTAP 9.9.1 y posteriores. En versiones anteriores, puede habilitarla especificando `-v4.1` la opción y configurándola en `enabled` al crear un servidor NFS en la máquina virtual de almacenamiento (SVM).

ONTAP no es compatible con las delegaciones a nivel de archivo y directorio de NFSv4.1.

Información relacionada

"Obtenga información sobre nconnect para el rendimiento de NFS".

Obtenga más información sobre la compatibilidad de ONTAP con NFSv4.2

A partir de ONTAP 9,8, ONTAP admite el protocolo NFSv4,2 para permitir acceso a clientes habilitados para NFSv4,2.

NFSv4.2 está habilitado de forma predeterminada en ONTAP 9.9.1 y versiones posteriores. En ONTAP 9.8, es necesario habilitar manualmente la versión 4.2 especificando el `-v4.2` opción y configurarla en `enabled` al crear un servidor NFS en la máquina virtual de almacenamiento (SVM). Habilitar NFSv4.1 también permite a los clientes usar las características de NFSv4.1 mientras están montados como v4.2.

Las versiones sucesivas de ONTAP amplían la compatibilidad de NFSv4,2 funciones opcionales.

Empezando por…	NFSv4,2 características opcionales incluyen…
ONTAP 9.12.1	• Atributos NFS extendidos • Archivos dispersos • Reservas de espacio
ONTAP 9.9.1	El control de acceso obligatorio (MAC) tiene la etiqueta NFS

Etiquetas de seguridad de NFS v4,2

A partir de ONTAP 9.9.1, se pueden habilitar las etiquetas de seguridad NFS. Están desactivadas de forma predeterminada.

Con etiquetas de seguridad NFS v4.2, los servidores NFS de ONTAP tienen en cuenta el control de acceso obligatorio (MAC), al almacenar y recuperar atributos sec_label enviados por los clientes.

Para obtener más información, consulte "RFC 7240".

A partir de ONTAP 9.12.1, las etiquetas de seguridad v4.2 de NFS son compatibles con las operaciones de volcado NDMP. Si las etiquetas de seguridad se encuentran en archivos o directorios en versiones anteriores, el volcado falla.

Pasos

1. Cambie la configuración del privilegio a avanzado:

```
set -privilege advanced
```

2. Habilitar etiquetas de seguridad:

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel enabled
```

Atributos NFS extendidos

A partir de ONTAP 9.12.1, los atributos extendidos de NFS (xattrs) están habilitados de forma predeterminada.

Los atributos ampliados son atributos estándar de NFS definidos "RFC 8276" y activados en los clientes NFS modernos. Se pueden utilizar para adjuntar metadatos definidos por el usuario a objetos del sistema de archivos, y son de interés en implementaciones de seguridad avanzadas.

Los atributos extendidos de NFS no se admiten actualmente para las operaciones de volcado de NDMP. Si se encuentran atributos extendidos en archivos o directorios, el volcado se realiza pero no realiza una copia de seguridad de los atributos extendidos en esos archivos o directorios.

Si necesita deshabilitar los atributos ampliados, utilice `vserver nfs modify -v4.2-xattrs disabled` el comando.

Obtenga información sobre nconnect para el rendimiento de NFS

A partir de ONTAP 9.8, la funcionalidad nconnect está disponible de forma predeterminada cuando NFSv4.1 está habilitado. nconnect mejora el rendimiento del cliente NFS al permitir múltiples conexiones TCP para un único montaje.

Cómo funciona nconnect

En las implementaciones anteriores de clientes NFS solo se utiliza una única conexión TCP con un montaje. En ONTAP, una única conexión TCP puede convertirse en un cuello de botella que aumenta las IOPS.

Un cliente compatible con nconnect puede tener múltiples conexiones TCP (hasta 16) asociadas a un único montaje NFS. nconnect utiliza una sola dirección IP y establece múltiples conexiones TCP a través de esa única IP para montar la exportación NFS. El cliente NFS distribuye las operaciones de archivos en múltiples conexiones TCP de forma rotativa, obteniendo un mayor rendimiento del ancho de banda de red disponible.

Versiones de NFS compatibles

- Se recomienda usar nconnect para montajes NFSv3, NFSv4.2 y NFSv4.1.
- No se recomienda usar nconnect para montajes NFSv4.0.

> Para un rendimiento óptimo, NetApp recomienda usar NFSv4.1 con nconnect en lugar de NFSv4.0. Si bien NFSv4.0 admite múltiples conexiones, NFSv4.1 con nconnect proporciona una mejor distribución de la carga y un rendimiento mejorado.

Soporte al cliente

Consulte su documentación de cliente NFS para confirmar si nconnect es compatible con su versión de cliente.

Información relacionada

- "Obtenga más información sobre la compatibilidad de ONTAP con NFSv4.1"
- "Obtenga más información sobre la compatibilidad de ONTAP con NFSv4.2"

Obtenga información sobre la compatibilidad de ONTAP con NFS paralelo

ONTAP es compatible con NFS paralelo (pNFS). El protocolo pNFS ofrece mejoras en el rendimiento al proporcionar a los clientes acceso directo a los datos de un conjunto de archivos distribuidos por varios nodos de un clúster. Ayuda a los clientes a localizar la ruta óptima para un volumen.

Obtenga más información sobre los montajes duros de NFS de ONTAP

Al solucionar los problemas de montaje, debe asegurarse de utilizar el tipo de montaje correcto. NFS admite dos tipos de montaje: Montajes soft y montajes hard. Solo debe utilizar montajes hard por motivos de fiabilidad.

No debería utilizar montajes soft, especialmente cuando hay una posibilidad de tiempos de espera de NFS frecuentes. Las condiciones de carrera pueden producirse como resultado de estos tiempos de espera, que

pueden provocar daños en los datos.

NFS paralelo

Introducción

Obtenga más información sobre NFS paralelo (pNFS) en ONTAP

NFS paralelo se introdujo como estándar RFC en enero de 2010 bajo RFC-5661 para permitir que los clientes accedan directamente a los datos de archivos en servidores NFSv4.1 separando las rutas de metadatos y datos. Ese acceso directo ofrece beneficios de rendimiento en términos de localización de datos, eficiencia de la CPU y paralelización de operaciones. En 2018 se redactó un RFC posterior que cubre los tipos de diseño pNFS (RFC-8434) y define estándares para diseños de archivos, bloques y objetos. ONTAP aprovecha el tipo de diseño de archivo para operaciones pNFS.

A partir de julio de 2024, el contenido de los informes técnicos publicados anteriormente en formato PDF se integrará con la documentación del producto ONTAP . La documentación de administración de almacenamiento NFS de ONTAP ahora incluye contenido de *TR-4063: Sistema de archivos de red paralelos (pNFS) en NetApp ONTAP*.

Durante años, NFSv3 fue la versión estándar del protocolo NFS que se utilizó para casi todos los casos de uso. Sin embargo, el protocolo tenía limitaciones, como la falta de estado, un modelo de permisos rudimentario y capacidades de bloqueo básicas. NFSv4.0 (RFC 7530) introdujo una serie de mejoras respecto de NFSv3 y se mejoró aún más con las versiones posteriores NFSv4.1 (RFC 5661) y NFSv4.2 (RFC 7862), que agregaron características como NFS paralelo (pNFS).

Beneficios de NFSv4.x

NFSv4.x ofrece los siguientes beneficios sobre NFSv3:

- Compatible con firewall porque NFSv4 usa solo un puerto (2049) para sus operaciones
- Gestión de caché avanzada y agresiva, como las delegaciones en NFSv4.x
- Opciones de seguridad RPC sólidas que emplean criptografía
- Internacionalización de personajes
- Operaciones compuestas
- Funciona sólo con TCP
- Protocolo con estado (no sin estado como NFSv3)
- Integración completa de Kerberos para mecanismos de autenticación eficientes
- Referencias de NFS
- Soporte de control de acceso compatible con UNIX y Windows
- Identificadores de usuarios y grupos basados en cadenas
- pNFS (NFSv4.1)
- Atributos extendidos (NFSv4.2)
- Etiquetas de seguridad (NFSv4.2)

- Operaciones de archivos dispersos (FALLOCATE) (NFSv4.2)

Para obtener más información sobre NFSv4.x general, incluidas las mejores prácticas y detalles sobre las características, consulte "Informe técnico de NetApp 4067: Guía de prácticas recomendadas e implementación de NFS".

Información relacionada

- "Información general de la configuración DE NFS"
- "Descripción general de la gestión de NFS"
- "Gestión de volúmenes de FlexGroup"
- "Descripción general de trunking NFS"
- https://www.netapp.com/pdf.html?item=/media/19370-tr-4523.pdf
- "Informe técnico de NetApp 4616: Kerberos de NFS en ONTAP con Microsoft Active Directory"

Aprenda sobre la arquitectura pNFS en ONTAP

La arquitectura pNFS se compone de tres componentes principales: un cliente NFS que admite pNFS, un servidor de metadatos que proporciona una ruta dedicada para operaciones de metadatos y un servidor de datos que proporciona rutas localizadas a los archivos.

El acceso del cliente a pNFS necesita conectividad de red a las rutas de datos y metadatos disponibles en el servidor NFS. Si el servidor NFS contiene interfaces de red a las que los clientes no pueden acceder, es posible que el servidor anuncie al cliente rutas de datos que no son accesibles, lo que puede provocar interrupciones.

Servidor de metadatos

El servidor de metadatos en pNFS se establece cuando un cliente inicia un montaje utilizando NFSv4.1 o posterior cuando pNFS está habilitado en el servidor NFS. Una vez hecho esto, todo el tráfico de metadatos se envía a través de esta conexión y permanece en ella mientras dura el montaje, incluso si la interfaz se migra a otro nodo.

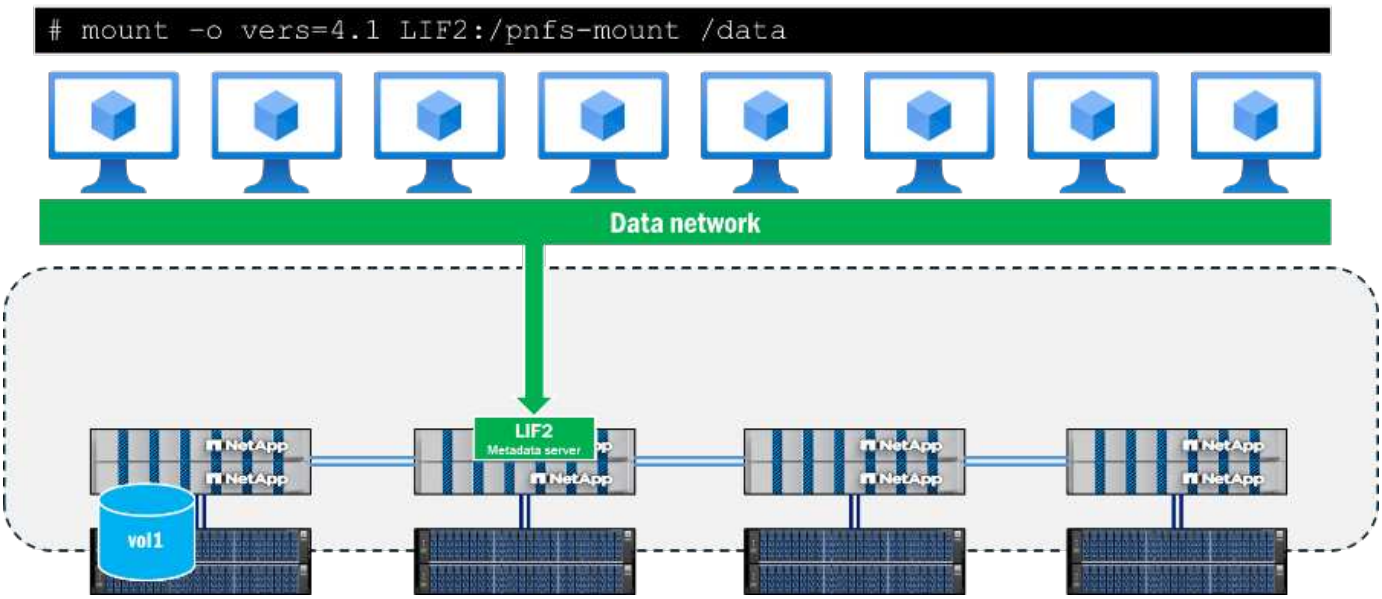


Figura 1. Establecer el servidor de metadatos en pNFS en ONTAP

La compatibilidad de pNFS se determina durante la llamada de montaje, específicamente en las llamadas EXCHANGE_ID. Esto se puede ver en una captura de paquetes debajo de las operaciones NFS como una bandera. Cuando las banderas pNFS `EXCHGID4_FLAG_USE_PNFS_DS` y `EXCHGID4_FLAG_USE_PNFS_MDS` se establecen en 1, entonces la interfaz es elegible para operaciones de datos y metadatos en pNFS.

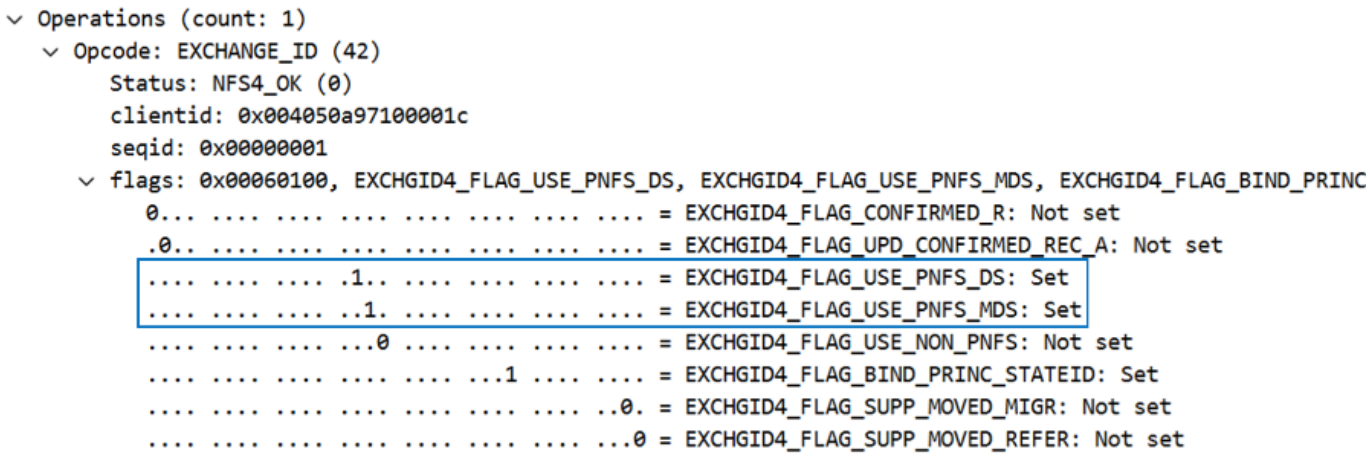


Figura 2. Captura de paquetes para montaje pNFS

Los metadatos en NFS generalmente consisten en atributos de archivos y carpetas, como identificadores de archivos, permisos, tiempos de acceso y modificación e información de propiedad. Los metadatos también pueden incluir crear y eliminar llamadas, vincular y desvincular llamadas y cambiar nombres.

En pNFS, también hay un subconjunto de llamadas de metadatos específicas para la función pNFS y se tratan con más detalle en "RFC 5661". Estas llamadas se utilizan para ayudar a determinar dispositivos elegibles para pNFS, asignaciones de dispositivos a conjuntos de datos y otra información requerida. La siguiente tabla muestra una lista de estas operaciones de metadatos específicas de pNFS.

Funcionamiento	Descripción
DISEÑO	Obtiene el mapa del servidor de datos del servidor de metadatos.
COMPROMISO DE DISEÑO	Los servidores confirman el diseño y actualizan los mapas de metadatos.
DISEÑO RETORNO	Devuelve el diseño o el nuevo diseño si se modifican los datos.
OBTENER INFORMACIÓN DEL DISPOSITIVO	El cliente obtiene información actualizada sobre un servidor de datos en el clúster de almacenamiento.
OBTENERLISTADEDISPOSITIVOS	El cliente solicita la lista de todos los servidores de datos que participan en el clúster de almacenamiento.
CB_RECUPERACIÓN DE DISEÑO	El servidor recupera el diseño de datos de un cliente si se detectan conflictos.
CB_RECALL_ANY	Devuelve cualquier diseño al servidor de metadatos.
CB_NOTIFY_ID_DE DISPOSITIVO	Notifica cualquier cambio de ID del dispositivo.

Información de la ruta de datos

Una vez establecido el servidor de metadatos y comienzan las operaciones de datos, ONTAP comienza a rastrear los ID de dispositivos elegibles para operaciones de lectura y escritura de pNFS, así como las asignaciones de dispositivos, que asocian los volúmenes en el clúster con las interfaces de red local. Este proceso ocurre cuando se realiza una operación de lectura o escritura en el montaje. Llamadas de metadatos,

como `GETATTR`. no activará estas asignaciones de dispositivos. Como tal, ejecutar una `ls` El comando dentro del punto de montaje no actualizará las asignaciones.

Los dispositivos y las asignaciones se pueden ver usando la CLI de ONTAP con privilegios avanzados, como se muestra a continuación.

```
::*> pnfs devices show -vserver DEMO
  (vserver nfs pnfs devices show)
Vserver Name     Mapping ID      Volume MSID     Mapping Status
Generation
---------------  --------------- --------------- ---------------
-------------
DEMO             16              2157024470      available       1

::*> pnfs devices mappings show -vserver SVM
  (vserver nfs pnfs devices mappings show)
Vserver Name    Mapping ID      Dsid            LIF IP
--------------  --------------- --------------- --------------------
DEMO            16              2488            10.193.67.211
```

En estos comandos, los nombres de los volúmenes no están presentes. En su lugar, se utilizan los identificadores numéricos asociados a esos volúmenes: el identificador del conjunto maestro (MSID) y el identificador del conjunto de datos (DSID). Para encontrar los volúmenes asociados a las asignaciones, puede utilizar `volume show -dsid [dsid_numeric]` o `volume show -msid [msid_numeric]` en privilegio avanzado de la CLI de ONTAP .

Cuando un cliente intenta leer o escribir en un archivo ubicado en un nodo remoto a la conexión del servidor de metadatos, pNFS negociará las rutas de acceso apropiadas para garantizar la localidad de los datos para esas operaciones y el cliente lo redireccionará al dispositivo pNFS anunciado en lugar de intentar atravesar la red del clúster para acceder al archivo. Esto ayuda a reducir la sobrecarga de la CPU y la latencia de la red.

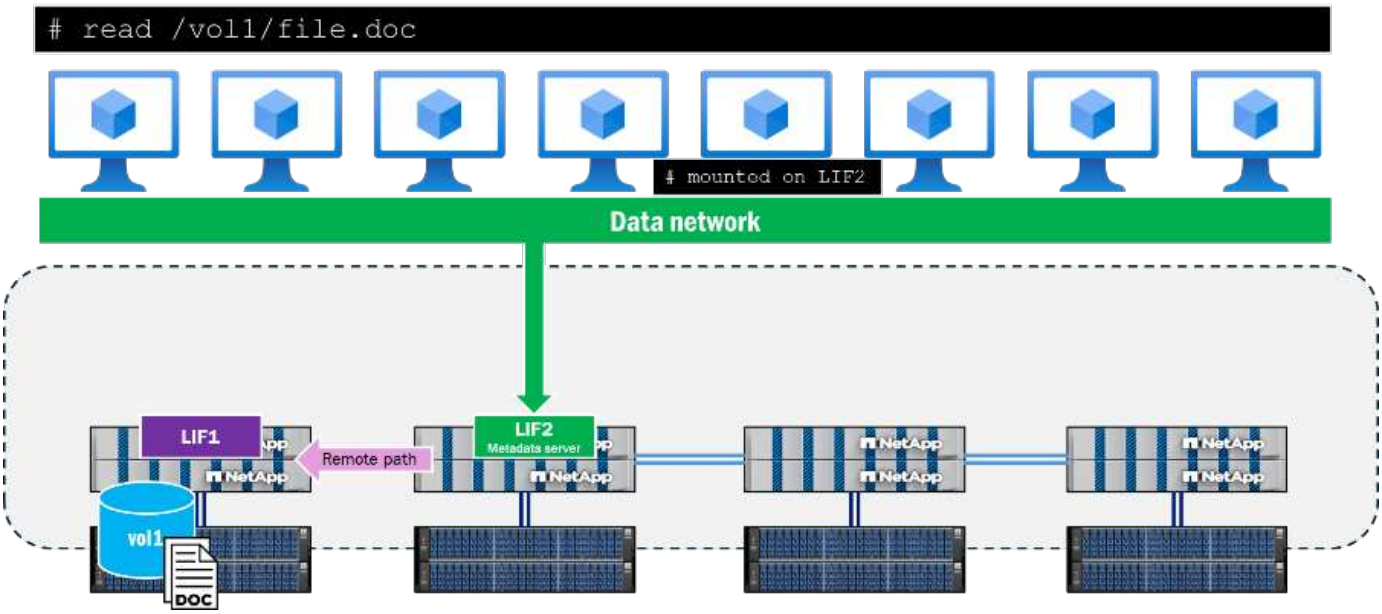


Figura 3. Ruta de lectura remota usando NFSv4.1 sin pNFS

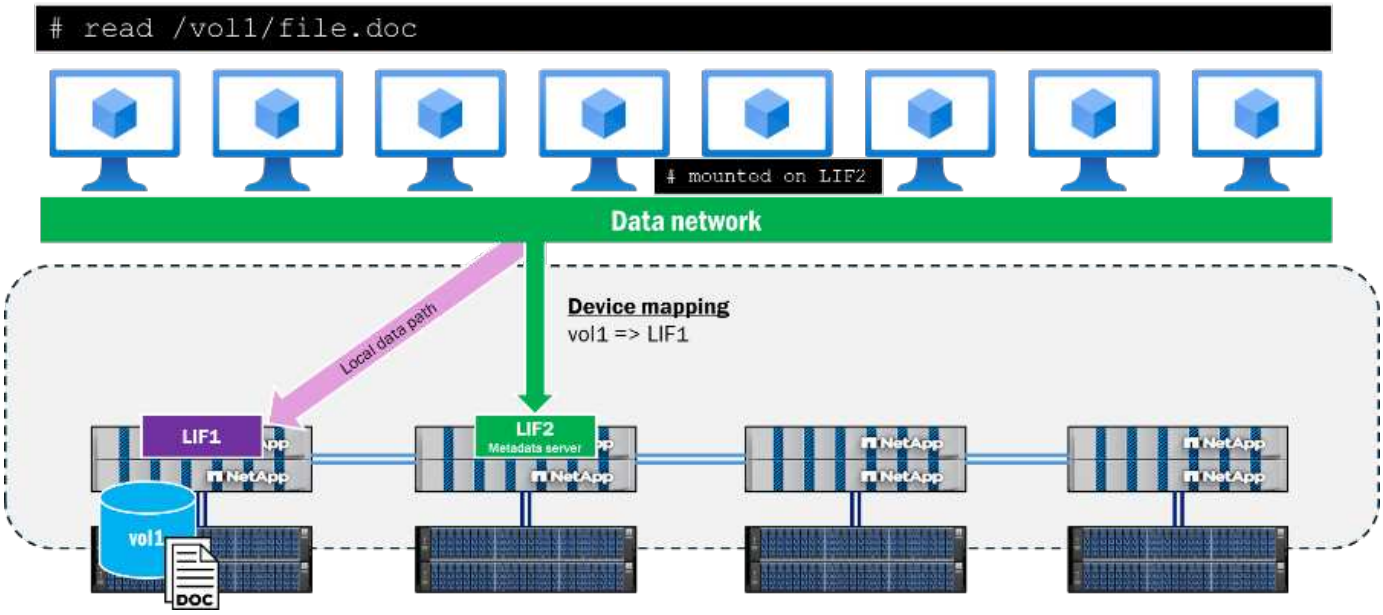


Figura 4. Ruta de lectura localizada mediante pNFS

Ruta de control pNFS

Además de los metadatos y las partes de datos de pNFS, también hay una ruta de control de pNFS. El servidor NFS utiliza la ruta de control para sincronizar la información del sistema de archivos. En un clúster ONTAP , la red del clúster backend se replica periódicamente para garantizar que todos los dispositivos pNFS y las asignaciones de dispositivos estén sincronizados.

Flujo de trabajo de población de dispositivos pNFS

A continuación se describe cómo se completa un dispositivo pNFS en ONTAP después de que un cliente realiza una solicitud para leer o escribir un archivo en un volumen.

1. El cliente solicita lectura o escritura; se realiza una operación OPEN y se recupera el identificador del archivo.
2. Una vez que se realiza la operación OPEN, el cliente envía el identificador de archivo al almacenamiento en una llamada LAYOUTGET a través de la conexión del servidor de metadatos.
3. LAYOUTGET devuelve al cliente información sobre el diseño del archivo, como el ID de estado, el tamaño de la banda, el segmento de archivo y el ID del dispositivo.
4. Luego, el cliente toma el ID del dispositivo y envía una llamada GETDEVINFO al servidor para recuperar la dirección IP asociada con el dispositivo.
5. El almacenamiento envía una respuesta con la lista de direcciones IP asociadas para el acceso local al dispositivo.
6. El cliente continúa la conversación NFS a través de la dirección IP local enviada desde el almacenamiento.

Interacción de pNFS con volúmenes FlexGroup

Los volúmenes FlexGroup en ONTAP presentan el almacenamiento como componentes de FlexVol volume que abarcan múltiples nodos en un clúster, lo que permite que una carga de trabajo aproveche múltiples recursos de hardware mientras mantiene un único punto de montaje. Debido a que varios nodos con múltiples interfaces de red interactúan con la carga de trabajo, es un resultado natural ver tráfico remoto atravesar la red del clúster backend en ONTAP.

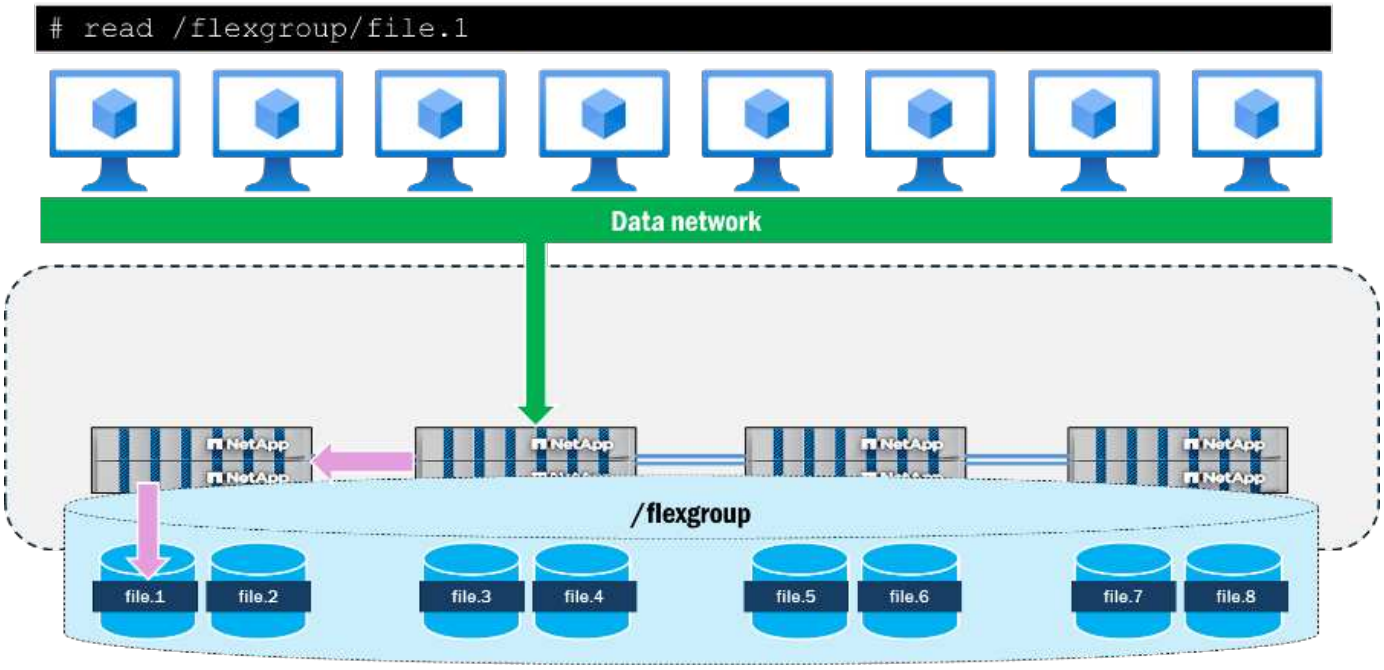


Figura 5. Acceso a un solo archivo en un volumen FlexGroup sin pNFS

Al utilizar pNFS, ONTAP realiza un seguimiento de los diseños de archivos y volúmenes del volumen FlexGroup y los asigna a las interfaces de datos locales en el clúster. Por ejemplo, si un volumen constituyente que contiene un archivo al que se accede reside en el nodo 1, entonces ONTAP notificará al cliente para redirigir el tráfico de datos a la interfaz de datos en el nodo 1.

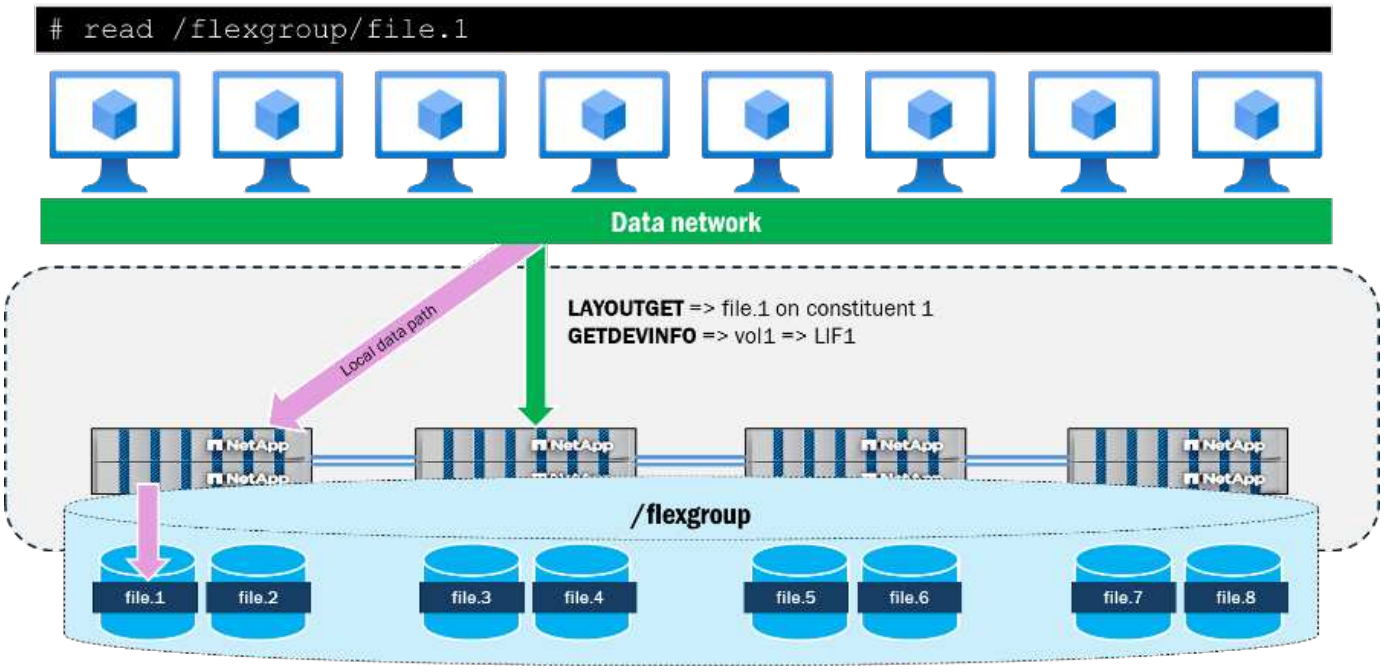


Figura 6. Acceso a un solo archivo en un volumen FlexGroup con pNFS

pNFS también permite la presentación de rutas de red paralelas a archivos desde un único cliente, algo que NFSv4.1 sin pNFS no proporciona. Por ejemplo, si un cliente desea acceder a cuatro archivos al mismo tiempo desde el mismo montaje usando NFSv4.1 sin pNFS, se utilizaría la misma ruta de red para todos los archivos y, en su lugar, el clúster ONTAP enviaría solicitudes remotas a esos archivos. La ruta de montaje puede convertirse en un cuello de botella para las operaciones, ya que todas siguen una única ruta y llegan a un único nodo y también atiende operaciones de metadatos junto con las operaciones de datos.

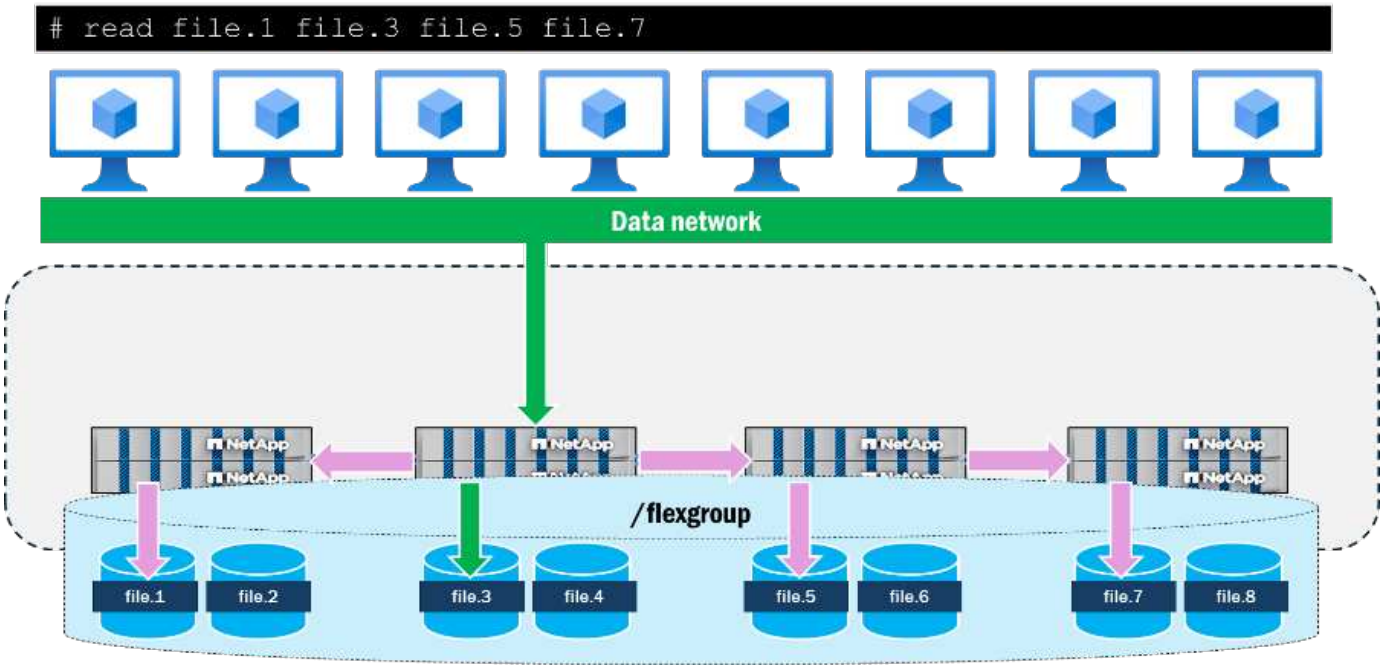


Figura 7. Acceso simultáneo a múltiples archivos en un volumen FlexGroup sin pNFS

Cuando se utiliza pNFS para acceder a los mismos cuatro archivos simultáneamente desde un solo cliente, el cliente y el servidor negocian rutas locales a cada nodo con los archivos y utilizan múltiples conexiones TCP para las operaciones de datos, mientras que la ruta de montaje actúa como la ubicación para todas las operaciones de metadatos. Esto proporciona beneficios de latencia al utilizar rutas locales a los archivos, pero también puede agregar beneficios de rendimiento mediante el uso de múltiples interfaces de red, siempre que los clientes puedan enviar suficientes datos para saturar la red.

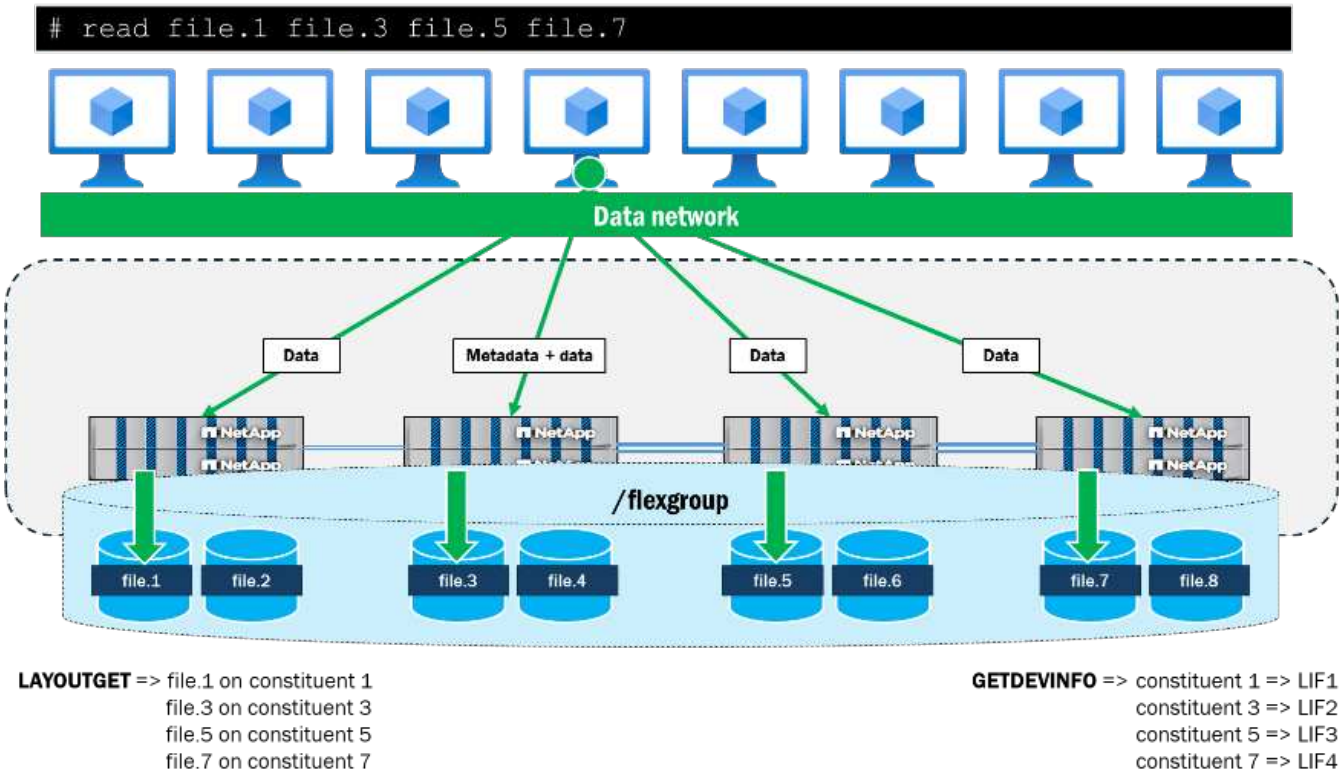


Figura 8. Acceso simultáneo a múltiples archivos en un volumen FlexGroup con pNFS

A continuación se muestran los resultados de una ejecución de prueba simple en un solo cliente RHEL 9.5

donde se leen en paralelo cuatro archivos de 10 GB (todos ellos residentes en diferentes volúmenes constituyentes en dos nodos del clúster ONTAP) mediante dd. Para cada archivo, se mejoró el rendimiento general y el tiempo de finalización al utilizar pNFS. Al usar NFSv4.1 sin pNFS, la diferencia de rendimiento entre los archivos que eran locales en el punto de montaje y los remotos era mayor que con pNFS.

Prueba	Rendimiento por archivo (MB/s)	Tiempo de finalización por archivo
NFSv4.1: sin pNFS	• Archivo.1–228 (local) • Archivo.2–227 (local) • Archivo.3–192 (remoto) • Archivo.4–192 (remoto)	• Archivo.1–46 (local) • Archivo.2–46.1 (local) • Archivo.3–54.5 (remoto) • Archivo.4–54.5 (remoto)
NFSv4.1: con pNFS	• Archivo.1–248 (local) • Archivo.2–246 (local) • Archivo .3–244 (local vía pNFS) • Archivo .4–244 (local vía pNFS)	• Archivo.1–42.3 (local) • Archivo.2–42.6 (local) • Archivo 3–43 (local vía pNFS) • Archivo 4–43 (local a través de pNFS)

Información relacionada

- "Gestión de volúmenes de FlexGroup"
- "Informe técnico 4571 de NetApp : Prácticas recomendadas de FlexGroup"

Casos de uso de pNFS en ONTAP

pNFS se puede utilizar con varias funciones de ONTAP para mejorar el rendimiento y proporcionar flexibilidad adicional para las cargas de trabajo NFS.

pNFS con nconnect

NFS introdujo una nueva opción de montaje con algunos clientes y servidores más recientes que proporciona una manera de entregar múltiples conexiones TCP mientras se monta una sola dirección IP. Esto proporciona un mecanismo para paralelizar mejor las operaciones, solucionar las limitaciones del servidor y del cliente NFS y, potencialmente, proporcionar un mayor rendimiento general para ciertas cargas de trabajo. nconnect es compatible con ONTAP 9.8 y versiones posteriores, siempre que el cliente admita nconnect.

Al usar nconnect con pNFS, las conexiones se paralelizarán usando la opción nconnect en cada dispositivo pNFS anunciado por el servidor NFS. Por ejemplo, si nconnect está configurado en cuatro y hay cuatro interfaces elegibles para pNFS, entonces la cantidad total de conexiones creadas será de hasta 16 por punto de montaje (4 nconnect x 4 direcciones IP).

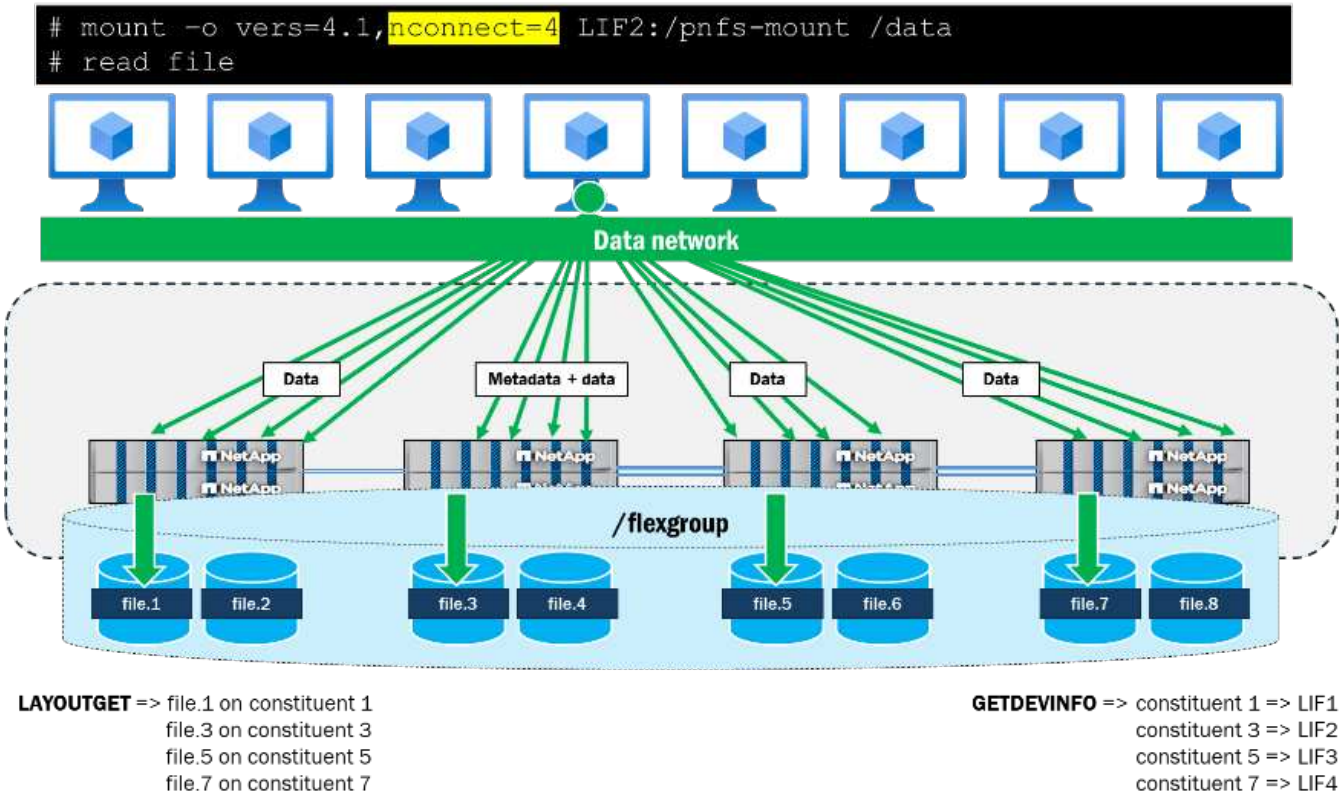


Figura 9. pNFS con nconnect establecido en 4

"Obtenga más información sobre la compatibilidad de ONTAP con NFSv4.1"

pNFS con enlace troncal de sesión NFSv4.1

Troncalización de sesión NFSv4.1 ("RFC 5661, sección 2.10.5") es el uso de múltiples conexiones TCP entre un cliente y un servidor para aumentar la velocidad de transferencia de datos. Se agregó soporte para troncalización de sesión NFSv4.1 a ONTAP 9.14.1 y debe usarse con clientes que también admitan troncalización de sesión.

En ONTAP, el enlace troncal de sesiones se puede utilizar en varios nodos de un clúster para proporcionar mayor rendimiento y redundancia en las conexiones.

La troncalización de sesiones se puede establecer de varias maneras:

- **Descubrir automáticamente a través de las opciones de montaje:** La troncalización de sesiones en la mayoría de los clientes NFS modernos se puede establecer a través de opciones de montaje (consulte la documentación del proveedor de su sistema operativo) que indican al servidor NFS que envíe información al cliente acerca de los troncales de sesión. Esta información aparece a través de un paquete NFS como un `fs_location4` llamar.

  La opción de montaje en uso depende de la versión del sistema operativo del cliente. Por ejemplo, las versiones de Ubuntu Linux generalmente usan `max_connect=n` para señalar que se debe utilizar un enlace troncal de sesión. En las distribuciones de Linux RHEL, el `trunkdiscovery` Se utiliza la opción de montaje.

  Ejemplo de Ubuntu

  ```
  mount -o vers=4.1,max_connect=8 10.10.10.10:/pNFS /mnt/pNFS
  ```

Ejemplo de RHEL

```
mount -o vers=4.1,trunkdiscovery 10.10.10.10:/pNFS /mnt/pNFS
```

Si intenta utilizar `max_connect` En las distribuciones RHEL, se tratará como nconnect y el enlace troncal de sesión no funcionará como se espera.

- **Establecer manualmente:** puede establecer la troncalización de sesiones manualmente montando cada dirección IP individual en la misma ruta de exportación y punto de montaje. Por ejemplo, si tiene dos direcciones IP en el mismo nodo (10.10.10.10 y 10.10.10.11) para una ruta de exportación de `/pNFS`, ejecuta el comando mount dos veces:

```
mount -o vers=4.1 10.10.10.10:/pNFS /mnt/pNFS
mount -o vers=4.1 10.10.10.11:/pNFS /mnt/pNFS
```

Repita este proceso en todas las interfaces que desee que participen en el enlace troncal.

Cada nodo obtiene su propio tronco de sesión. Los troncos no atraviesan los nodos.

Al utilizar pNFS, utilice únicamente el enlace troncal de sesión *o* nconnect. El uso de ambos generará un comportamiento no deseado, como por ejemplo que solo la conexión del servidor de metadatos obtenga los beneficios de nconnect mientras que los servidores de datos utilizan una única conexión.

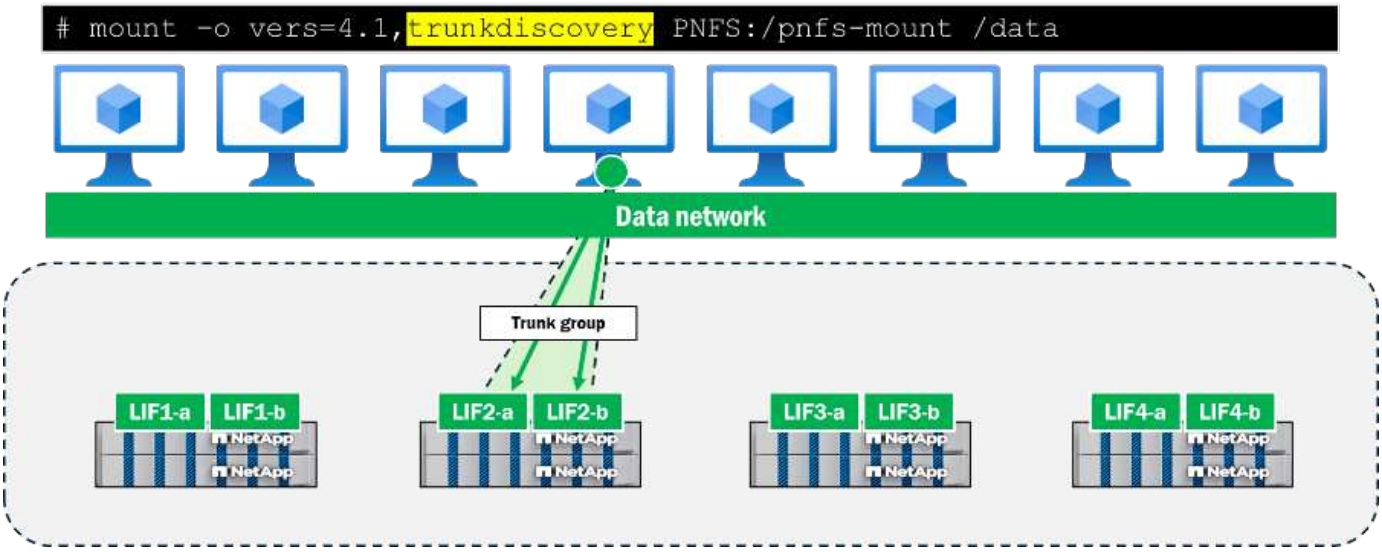
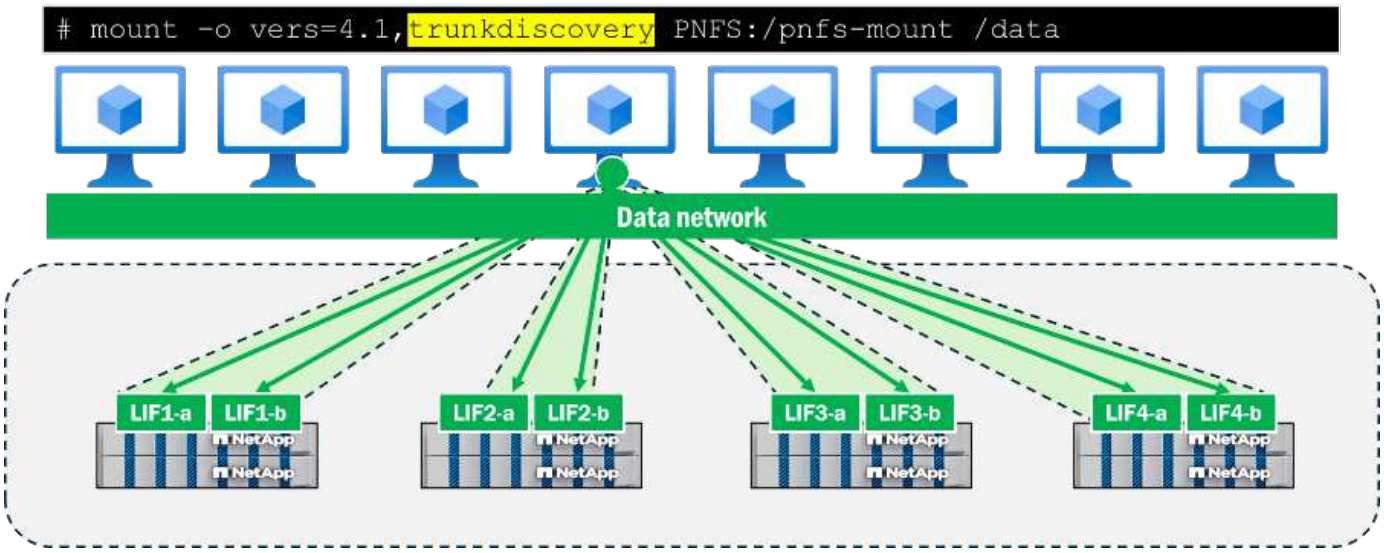


Figura 10. Troncalización de sesiones NFSv4.1 en ONTAP

pNFS puede proporcionar una ruta local a cada nodo participante en un clúster y, cuando se utiliza con troncalización de sesión, pNFS puede aprovechar un troncal de sesión por nodo para maximizar el rendimiento de todo el clúster.



Cuando `trunkdiscovery` se utiliza, se aprovecha una llamada GETATTR agregada (FS_Locations) para las interfaces troncales de sesión enumeradas en el nodo del servidor NFS donde se encuentra la interfaz de montaje. Una vez que se devuelven, se realizan montajes posteriores en las direcciones devueltas. Esto se puede ver en una captura de paquetes durante el montaje.

```
198 1.219372  [redacted]  [redacted]  NFS  246 V4 Call (Reply In 199) GETATTR FH: 0x787f5cf1
199 1.219579  [redacted]  [redacted]  NFS  238 V4 Reply (Call In 198) GETATTR

  Opcode: SEQUENCE (53)
      Status: NFS4_OK (0)
      sessionid: 7100001e004090a90000000000000409
      seqid: 0x00000009
      slot id: 0
      high slot id: 63
      target high slot id: 63
    > status flags: 0x00000000
  Opcode: PUTFH (22)
      Status: NFS4_OK (0)
  Opcode: GETATTR (9)
      Status: NFS4_OK (0)
    Attr mask: 0x01000100 (FSID, FS_Locations)
      reqd_attr: FSID (8)
        > fattr4_fsid
      reco_attr: FS_Locations (24)
        fattr4_fs_locations
            pathname components: 0
          fs_location4
              num: 1
            fs_location4
              servers
                  num: 1
                server: [redacted]
                    length: 14
                    contents: [redacted]
                    fill bytes: opaque data
                pathname components: 0
```

Figura 11. Detección de troncos de sesión NFS durante el montaje: captura de paquetes

"Obtenga más información sobre los enlaces troncales NFS"

Referencias de pNFS versus NFSv4.1

Las referencias NFSv4.1 proporcionan un modo de redirección de ruta de montaje inicial que dirige a un cliente a la ubicación de los volúmenes cuando se produce una solicitud de montaje. Las referencias de NFSv4.1 funcionan dentro de una única SVM. Esta función intenta localizar el montaje NFS en una interfaz de red que reside en el mismo nodo que el volumen de datos. Si esa interfaz o volumen se mueve a otro nodo mientras está montado en un cliente, la ruta de datos ya no estará localizada hasta que se establezca un nuevo montaje.

pNFS no intenta localizar una ruta de montaje. En su lugar, establece un servidor de metadatos utilizando una ruta de montaje y luego localiza la ruta de datos dinámicamente según sea necesario.

Las referencias NFSv4.1 se pueden usar con pNFS, pero la funcionalidad es innecesaria. Habilitar referencias con pNFS no mostrará resultados notables.

"Habilitar o deshabilitar referencias NFSv4"

Interacción de pNFS con equilibrio de capacidad avanzado

"Equilibrado de capacidad avanzado" en ONTAP escribe porciones de datos de archivos en los volúmenes constituyentes de un volumen FlexGroup (no compatible con volúmenes FlexVol individuales). A medida que un archivo crece, ONTAP decide comenzar a escribir datos en un nuevo inodo multiparte en un volumen constituyente diferente, que puede estar en el mismo nodo o en uno diferente. Las operaciones de escritura, lectura y metadatos en estos archivos multi-inodo son transparentes y no interrumpen a los clientes. El equilibrio de capacidad avanzado mejora la gestión del espacio entre los volúmenes constituyentes de FlexGroup , lo que proporciona un rendimiento más consistente.

pNFS puede redirigir la E/S de datos a una ruta de red localizada dependiendo de la información de diseño de archivo almacenada en el servidor NFS. Cuando se crea un solo archivo grande en partes en múltiples volúmenes constituyentes que potencialmente pueden abarcar varios nodos en el clúster, pNFS en ONTAP aún puede proporcionar tráfico localizado a cada parte del archivo porque ONTAP también mantiene la información de diseño del archivo para todas las partes del archivo. Cuando se lee un archivo, la localidad de la ruta de datos cambiará según sea necesario.

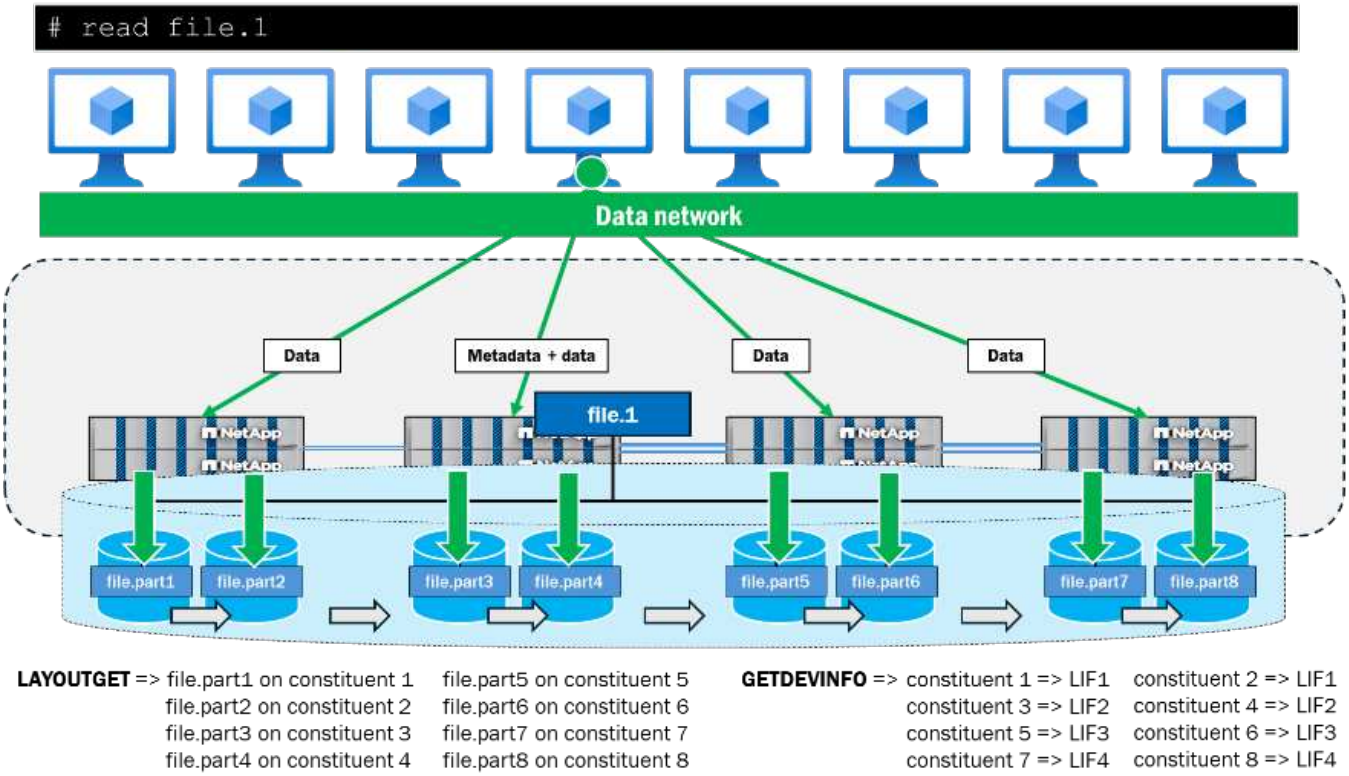


Figura 12. Equilibrio de capacidad avanzado con pNFS

Información relacionada

- "Configuración del volumen de FlexGroup"

Estrategia de implementación de pNFS en ONTAP

pNFS se introdujo para mejorar el NFS tradicional separando metadatos y rutas de datos, proporcionando localización de datos y permitiendo operaciones paralelas.

Desafíos del NFS tradicional y beneficios del pNFS

La siguiente tabla muestra los desafíos del NFS tradicional y explica cómo pNFS en ONTAP los aborda.

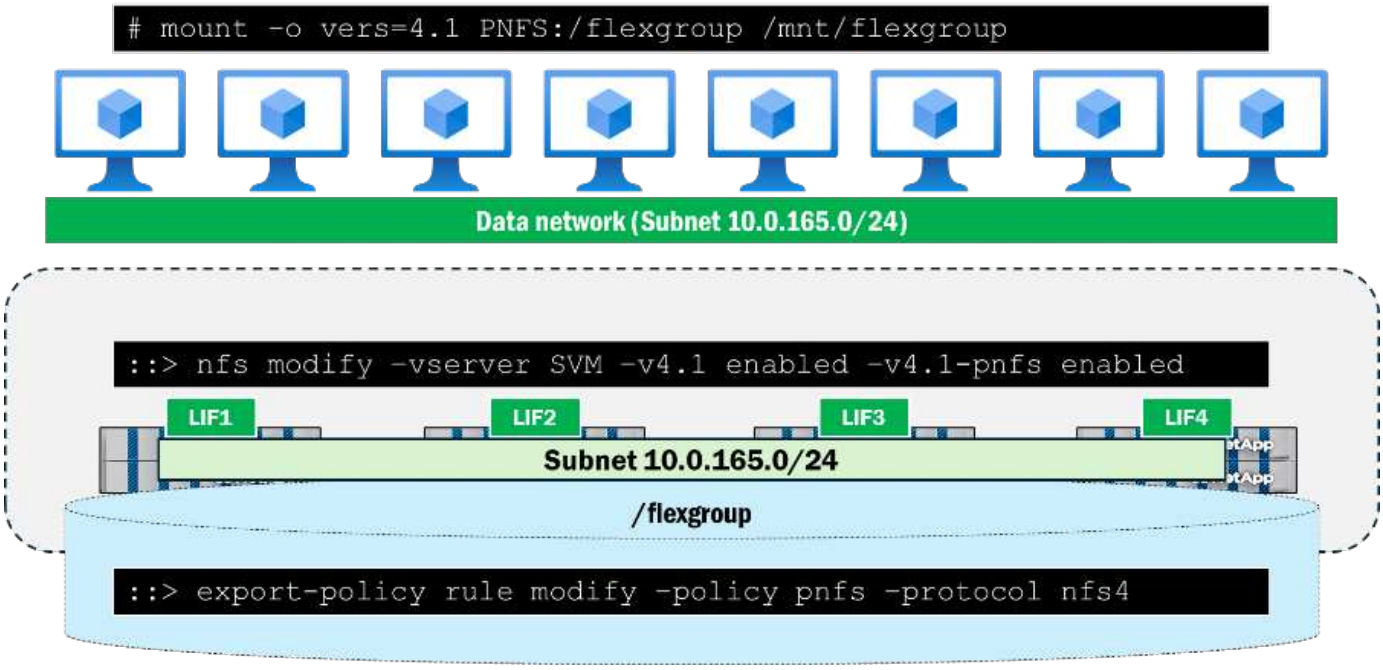
Desafío	beneficio de pNFS
La misma ruta para metadatos y datos En NFS tradicional, los metadatos y los datos recorren la misma ruta, lo que puede saturar tanto la red como la CPU, ya que una sola ruta se conectará a un solo nodo de hardware en el clúster. Esto se agrava cuando muchos usuarios intentan acceder a la misma exportación NFS.	**Las rutas de metadatos y datos están separadas, las rutas de datos están paralelizadas** Al separar las rutas de metadatos y datos para el tráfico NFS y proporcionar múltiples rutas de red para las rutas de datos, se maximizan los recursos de CPU y red en un clúster ONTAP , lo que proporciona una escala mejorada para las cargas de trabajo.

Desafío	beneficio de pNFS
Desafíos de la distribución de la carga de trabajo En un clúster NAS de ONTAP , puede tener hasta 24 nodos, cada uno de los cuales puede tener su propio conjunto de volúmenes de datos e interfaces de red. Cada volumen puede alojar su propia carga de trabajo, o un subconjunto de una carga de trabajo, y con un volumen FlexGroup esa carga de trabajo puede existir en múltiples nodos que acceden a un único espacio de nombres para mayor simplicidad. Cuando un cliente monta una exportación NFS, el tráfico de red se establecerá en un solo nodo. Cuando los datos a los que se accede residen en un nodo separado del clúster, se producirá tráfico remoto, lo que puede agregar latencia a la carga de trabajo y complejidad en la administración.	**Rutas locales y paralelas a las estructuras de datos** Debido a que pNFS separa las rutas de datos de los metadatos y proporciona múltiples rutas de datos paralelas según la localidad del volumen en el clúster, la latencia se puede reducir al reducir la distancia del tráfico de red en el clúster, además de aprovechar múltiples recursos de hardware en un clúster. Además, dado que pNFS en ONTAP redirige el tráfico de datos automáticamente, los administradores tienen menos necesidad de administrar múltiples rutas y ubicaciones de exportación.
Reubicación de puntos de montaje NFS Una vez establecido un punto de montaje, sería disruptivo desmontar y volver a montar el volumen. ONTAP ofrece la posibilidad de migrar interfaces de red entre nodos, pero eso agrega sobrecarga de administración y es perjudicial para las conexiones NFS con estado que utilizan NFSv4.x. Algunas de las razones para reubicar un punto de montaje están relacionadas con los desafíos de localidad de datos.	**Reubicación automática de rutas** Con pNFS, el servidor NFS mantiene una tabla de las ubicaciones de las interfaces y volúmenes de red. Cuando se solicita una estructura de datos a un cliente a través de la ruta de metadatos en pNFS, el servidor entregará una ruta de red optimizada al cliente, que luego utilizará esa ruta para operaciones de datos. Esto reduce drásticamente la sobrecarga de gestión de las cargas de trabajo y puede mejorar el rendimiento en algunos casos.

Requisitos de configuración

La configuración de pNFS en NetApp ONTAP requiere lo siguiente:

- Un cliente NFS que admita pNFS y esté montado con NFSv4.1 o posterior
- NFSv4.1 habilitado en el servidor NFS en ONTAP (`nfs modify -v4.1 enabled`; desactivado por defecto)
- pNFS habilitado en el servidor NFS en ONTAP (`nfs modify -v4.1-pnfs enabled`; deshabilitado por defecto)
- Al menos una interfaz de red por nodo, enrutable a los clientes NFS
- Volúmenes de datos en la SVM que tienen políticas y reglas de exportación que permiten NFSv4



Una vez cumplidos los requisitos de configuración anteriores, pNFS simplemente funcionará por sí solo.

Información relacionada

- "Configuración de NFS"
- "Compatibilidad de ONTAP con NFSv4.1"
- "Conectividad de interfaz de red para pNFS"

Planificación

Plan para la implementación de pNFS

Antes de implementar pNFS en su entorno, asegúrese de cumplir con los requisitos previos y comprender los requisitos de interoperabilidad y los límites de configuración.

Requisitos previos

Antes de habilitar y usar pNFS en ONTAP, asegúrese de que se cumplan los siguientes requisitos:

- NFSv4.1 o posterior está habilitado en el servidor NFS
- Al menos uno "Los datos LIF existen por nodo" en el clúster para el SVM que aloja el servidor NFS
- Todo "Los LIF de datos en el SVM son enrutables" a clientes NFS
- Los clientes NFS admiten pNFS (la mayoría de las distribuciones de Linux modernas a partir de 2014)
- La conectividad de red entre los clientes y todos los LIF de datos en la SVM es funcional
- La resolución de DNS (si se utilizan nombres de host) está configurada correctamente para todos los LIF de datos
- "Volúmenes de FlexGroup" están configurados (recomendado para obtener mejores resultados)
- "Coincidencia de dominios de identificación de NFSv4.x" entre clientes y ONTAP
- "NFS Kerberos" (si se utiliza) está habilitado en todos los LIF de datos en el SVM

Resumen de mejores prácticas

Al implementar pNFS en su entorno, siga estas prácticas recomendadas:

- Usar "Volúmenes de FlexGroup" Para un mejor rendimiento y escalamiento de capacidad
- Asegúrese de que todos "Las interfaces de red en el SVM son enrutables" a los clientes
- "Desactivar NFSv4,0" para garantizar que los clientes utilicen NFSv4.1 o posterior
- Distribuya los puntos de montaje en múltiples interfaces y nodos de red
- Utilice DNS round robin para "servidores de metadatos de equilibrio de carga"
- Verificar "Coincidencia de dominios de identificación de NFSv4.x" en clientes y servidores
- Conducta "migraciones de interfaz de red" y "conmutaciones por error de almacenamiento" durante las ventanas de mantenimiento
- Permitir "NFS Kerberos" en todos los LIF de datos si se utiliza seguridad Kerberos
- Evite usar "Referencias de NFSv4.1" al usar pNFS
- Prueba "Configuración de nconnect" con cuidado para evitar sobrepasar los límites de conexión TCP
- Considerar "troncalización de sesiones" como alternativa a "nconectar" (no utilice ambos juntos)
- Verificar "Soporte del proveedor del sistema operativo del cliente" para pNFS antes de la implementación

Interoperabilidad

pNFS en ONTAP está diseñado para funcionar con clientes NFS compatibles con RFC. Se aplican las siguientes consideraciones:

- El más moderno "Distribuciones de Linux de 2014 y posteriores" Admite pNFS (RHEL 6.4, Fedora 17 y posteriores)
- Verifique con el proveedor del sistema operativo de su cliente que pNFS sea compatible
- pNFS funciona tanto con FlexVol como con "Volúmenes de FlexGroup"
- pNFS es compatible con NFSv4.1 y "NFSv4.2"
- pNFS se puede utilizar con "NFS Kerberos" (krb5, krb5i, krb5p), pero el rendimiento podría verse afectado
- pNFS se puede utilizar junto con "nconectar" o "troncalización de sesiones" (pero no ambos simultáneamente)
- pNFS no funciona sobre "NFSv4.0"

Límites

Los siguientes límites se aplican a pNFS en ONTAP:

- "Límites de conexión TCP" por nodo varía según la plataforma (consulte NetApp Hardware Universe para conocer los límites específicos)
- Tamaño máximo de archivo: depende del tipo de volumen y la versión de ONTAP
- Cantidad máxima de archivos: hasta 200 mil millones de archivos con "Volúmenes de FlexGroup"
- Capacidad máxima: Hasta 60 PB con "Volúmenes de FlexGroup"
- "Recuento de interfaces de red":Se requiere al menos un LIF de datos por nodo; es posible que se necesiten más para equilibrar la carga

Al utilizar "Conéctese con pNFS"Tenga en cuenta que los recuentos de conexiones TCP se multiplican

rápidamente:

- Cada montaje de cliente con nconnect crea múltiples conexiones TCP por LIF de datos
- Con muchos clientes que utilizan valores altos de nconnect, "Límites de conexión TCP" puede superarse
- Exceder los límites de conexión TCP impide nuevas conexiones hasta que se liberen las conexiones existentes

Información relacionada

- "Conectividad de interfaz de red para pNFS"
- "Habilitar o deshabilitar NFSv4.1"
- "Compatibilidad de ONTAP con NFSv4.1"
- "Compatibilidad de ONTAP con NFSv4.2"
- "NetApp Hardware Universe"

Mejores prácticas de rendimiento y ajuste de pNFS

Al utilizar pNFS en ONTAP, tenga en cuenta estas consideraciones y prácticas recomendadas para obtener mejores resultados.

Recomendaciones de tipo de volumen

pNFS en ONTAP funciona con volúmenes FlexVol y FlexGroup , pero para obtener los mejores resultados generales, utilice volúmenes FlexGroup .

Los volúmenes FlexGroup proporcionan:

- Un único punto de montaje que puede abarcar múltiples recursos de hardware en un clúster y al mismo tiempo permitir que pNFS localice el tráfico de datos
- Posibilidades de capacidad masiva (hasta 60 PB) y gran cantidad de archivos (hasta 200 mil millones de archivos)
- Compatibilidad con archivos multiparte para equilibrar la capacidad y obtener posibles beneficios de rendimiento
- Acceso paralelo a volúmenes y hardware que admiten una única carga de trabajo

"Obtenga más información sobre la gestión de volúmenes de FlexGroup"

Recomendaciones de clientes

No todos los clientes NFS admiten pNFS, pero la mayoría de los clientes modernos sí. RHEL 6.4 y Fedora 17 fueron los primeros clientes pNFS compatibles (aproximadamente en 2014), por lo que es razonable suponer que las versiones de cliente lanzadas en los últimos años son totalmente compatibles con esta función. La postura de soporte de NFS de ONTAP es la siguiente: "si el cliente admite la función y cumple con RFC, y nosotros admitimos la función, entonces la combinación es compatible". Sin embargo, es una buena práctica asegurarse de que el proveedor del sistema operativo del cliente admita pNFS.

El volumen se mueve

ONTAP brinda la capacidad de mover volúmenes sin interrupciones entre nodos o agregados en el mismo clúster para brindar flexibilidad de equilibrio de capacidad y rendimiento. Cuando se realiza un movimiento de volumen en ONTAP, las asignaciones de dispositivos pNFS se actualizan automáticamente para informar a los

clientes que utilicen la nueva relación de volumen a interfaz si es necesario.

"Aprenda a mover un volumen"

Migración de la interfaz de red

ONTAP proporciona la capacidad de mover interfaces de red entre nodos del mismo clúster para brindar equilibrio de rendimiento y flexibilidad de mantenimiento. Al igual que los movimientos de volumen, cuando se realiza una migración de interfaz de red en ONTAP, las asignaciones de dispositivos pNFS se actualizan automáticamente para informar a los clientes que utilicen la nueva relación de volumen a interfaz si es necesario.

Sin embargo, debido a que NFSv4.1 es un protocolo con estado, una migración de interfaz de red puede ser perjudicial para los clientes que utilizan activamente el montaje NFS. Es una buena práctica realizar migraciones de interfaz de red en una ventana de mantenimiento y notificar a los clientes sobre posibles interrupciones de la red.

Conmutaciones por error/devoluciones de almacenamiento

pNFS sigue las mismas consideraciones de conmutación por error de almacenamiento que NFSv4.1. Estos temas se tratan en detalle en "Informe técnico de NetApp 4067: Guía de prácticas recomendadas e implementación de NFS"En general, cualquier conmutación por error o devolución de almacenamiento que involucre pNFS debe realizarse en una ventana de mantenimiento, con posibles interrupciones de almacenamiento esperadas debido al estado del protocolo.

Cargas de trabajo de metadatos

Las operaciones de metadatos son de tamaño pequeño y pueden ser grandes en número según la carga de trabajo (¿Está creando una gran cantidad de archivos? ¿Está ejecutando comandos "buscar"?) y el recuento total de archivos. Como resultado, las cargas de trabajo con muchas llamadas de metadatos pueden sobrecargar la CPU del servidor NFS y potencialmente pueden generar un cuello de botella en una sola conexión. pNFS (y NFSv4.x en general) no es adecuado para cargas de trabajo con muchas llamadas de metadatos que dependen del rendimiento, ya que el estado, los mecanismos de bloqueo y algunas de las características de seguridad de la versión del protocolo pueden afectar negativamente la utilización y la latencia de la CPU. Estos tipos de carga de trabajo (como GETATTR o SETATTR altos) generalmente funcionan mejor con NFSv3.

Servidor de metadatos

El servidor de metadatos en pNFS se establece en el montaje inicial de una exportación NFS. Cuando se establece el punto de montaje, permanece en su lugar hasta que se vuelve a montar o se mueve la interfaz de datos. Por este motivo, es una buena práctica garantizar que varios clientes que acceden al mismo volumen se monten en diferentes nodos e interfaces de datos en toda la SVM. Este enfoque permite equilibrar la carga de los servidores de metadatos entre los nodos y los recursos de la CPU, al tiempo que maximiza las interfaces de red en el clúster. Una forma de lograr esto es establecer una configuración de DNS round robin, que se describe en "Informe técnico 4523 de NetApp : Equilibrio de carga de DNS en ONTAP".

Dominios de identificación de NFSv4.x

NFSv4.x proporciona funcionalidad de seguridad de muchas maneras (que se explican en detalle en "Informe técnico de NetApp 4067: Guía de prácticas recomendadas e implementación de NFS"). Los dominios de identificación de NFSv4.x son una de esas formas en las que un cliente y un servidor deben acordar los dominios de identificación cuando intentan autenticar usuarios y grupos en una exportación NFS. Uno de los efectos secundarios de una falta de coincidencia en el dominio de ID sería que el usuario o grupo apareciera como un usuario anónimo (esencialmente aplastado) para evitar acceso no deseado. Con NFSv4.x (y también

pNFS), es una buena práctica garantizar que los dominios de identificación de NFSv4.x coincidan en el cliente y el servidor.

nconectar

Como se mencionó anteriormente, nconnect en ONTAP puede ayudar a mejorar el rendimiento en algunas cargas de trabajo. Con pNFS, es importante entender que si bien nconnect puede mejorar el rendimiento al aumentar en gran medida la cantidad total de conexiones TCP al sistema de almacenamiento, también puede crear problemas cuando muchos clientes aprovechan la opción de montaje al saturar las conexiones TCP en el almacenamiento. El Hardware Universe de NetApp cubre los límites de conexión TCP por nodo.

Cuando se superan los límites de conexión TCP de un nodo, no se permiten nuevas conexiones TCP hasta que se liberen las conexiones existentes. Esto puede crear complicaciones en entornos que podrían experimentar fuertes tormentas.

La siguiente tabla muestra cómo pNFS con nconnect podría superar los límites de conexión TCP:

Número de clientes	valor de nconnect	Total de conexiones TCP potenciales por montaje, por nodo
1	4	4
100	4	400
1000	8	8000
10000	8	80000
10000	16	160000 [1]

[1] Supera la mayoría de los límites de conexión TCP de nodo único de ONTAP

Troncalización de sesión NFSv4,1

El enlace troncal de sesiones en ONTAP se puede utilizar para aumentar el rendimiento y la resiliencia de la ruta a los montajes NFSv4.x. Cuando se utiliza con pNFS, cada nodo de un clúster puede establecer un tronco de sesión. Sin embargo, los troncales de sesión requieren al menos dos interfaces por nodo, y pNFS requiere al menos una interfaz por nodo para funcionar según lo previsto. Además, todas las interfaces en la SVM deben ser enrutables a los clientes NFS. El enlace troncal de sesiones y pNFS no funcionan correctamente cuando también se aprovecha nconnect. Considere nconnect y el enlace troncal de sesiones como características mutuamente excluyentes.

"Obtenga más información sobre el enlace troncal NFS"

Conectividad de la interfaz de red

pNFS requiere una interfaz de red enrutable en cada nodo de un clúster para funcionar correctamente. Si existen otras interfaces de red que no se pueden enrutar a clientes NFS en el mismo SVM que el servidor NFS que aloja pNFS, ONTAP seguirá anunciando esas interfaces en la asignación de dispositivos a los clientes. Cuando el cliente NFS intenta acceder a los datos a través de las interfaces en una subred diferente, no podrá conectarse y se creará una interrupción. Se recomienda permitir únicamente interfaces de red en una SVM a las que los clientes puedan acceder cuando utilizan pNFS.

De forma predeterminada, pNFS requiere que cualquier LIF de datos en el SVM sea enrutable a las interfaces en los clientes NFS porque las listas de dispositivos pNFS se completarán con cualquier LIF de datos en el SVM. Como resultado, se podrían seleccionar LIF de datos no enrutables, lo que puede crear escenarios de interrupción. Como práctica recomendada, solo configure LIF de datos enrutables cuando utilice pNFS.

A partir de ONTAP 9.18.1 RC1 y versiones posteriores, puede especificar qué interfaces son elegibles para el tráfico pNFS por subred, lo que permite combinar interfaces enrutables y no enrutables. Comuníquese con el soporte de NetApp para obtener información sobre los comandos.

NFSv4.0

NFSv4.0 es una opción que se puede habilitar en un servidor NFS de ONTAP junto con NFSv4.1. Sin embargo, pNFS no funciona con NFSv4.0. Si NFSv4.0 está habilitado en el servidor NFS, los clientes podrían potencialmente montar sin saberlo esa versión del protocolo y no podrán aprovechar pNFS. Como resultado, es una buena práctica deshabilitar explícitamente NFSv4.0 al usar pNFS. NFSv4.1 aún debe estar habilitado y puede funcionar independientemente de NFSv4.0.

Referencias de NFSv4.1

Las referencias de NFSv4.1 localizarán la ruta de montaje desde un cliente a la interfaz de red en el nodo que posee un volumen. pNFS localiza la ruta de datos y la ruta de montaje se convierte en un servidor de metadatos.

Si bien las dos características se pueden usar juntas, el uso de referencias NFSv4.1 con pNFS puede generar el efecto no deseado de apilar múltiples servidores de metadatos en el mismo nodo y reducir la capacidad de distribuir servidores de metadatos entre múltiples nodos del clúster. Si los servidores de metadatos no se distribuyen de manera uniforme en un clúster cuando se usa pNFS, la CPU de un solo nodo puede verse sobrecargada con solicitudes de metadatos y crear un cuello de botella en el rendimiento.

Por ello, se recomienda evitar el uso de referencias NFSv4.1 al utilizar pNFS. En su lugar, distribuya los puntos de montaje en varias interfaces de red y nodos del clúster.

"Obtenga información sobre cómo habilitar o deshabilitar las referencias de NFSv4"

NFS Kerberos

Con NFS Kerberos, es posible cifrar la autenticación con krb5 y cifrar aún más los paquetes de datos con krb5i y krb5p. Esto se habilita en función de la interfaz por red en una SVM y se cubre con todo detalle en "Informe técnico de NetApp 4616: Kerberos de NFS en ONTAP con Microsoft Active Directory".

Dado que pNFS puede redirigir el tráfico de datos a través de nodos e interfaces de red en la SVM, NFS Kerberos debe estar habilitado y funcional en cada interfaz de red en la SVM. Si alguna interfaz de red en la SVM no está habilitada para Kerberos, entonces pNFS no podrá funcionar correctamente al intentar acceder a los volúmenes de datos en esas interfaces.

Por ejemplo, al ejecutar una prueba de lectura utilizando dd paralelo en un SVM habilitado para pNFS con dos interfaces de red (solo una habilitada para Kerberos), los archivos ubicados en la interfaz habilitada para Kerberos funcionaron bien, mientras que los archivos en el nodo con la interfaz sin Kerberos habilitado nunca pudieron completar sus lecturas. Cuando Kerberos se habilitó en ambas interfaces, todos los archivos pudieron funcionar como se esperaba.

Se puede utilizar NFS Kerberos con pNFS siempre que NFS Kerberos esté habilitado en todas las interfaces de red en la SVM. Tenga en cuenta que NFS Kerberos puede incurrir en una penalización de rendimiento

debido al cifrado/descifrado de los paquetes, por lo que es una buena práctica probar pNFS con NFS Kerberos exhaustivamente con sus cargas de trabajo para garantizar que cualquier impacto en el rendimiento no tenga un impacto excesivo en la carga de trabajo.

A continuación se muestra un ejemplo de rendimiento de lectura paralela al utilizar krb5 (autenticación) y krb5p (cifrado de extremo a extremo) con pNFS en un cliente RHEL 9.5. Krb5p vio una degradación del rendimiento del 70% en esta prueba.

Sabor Kerberos	MB/s	Tiempo de finalización
krb5	• File1-243 • File2-243 • File3-238 • File4-238	• File1-43 • File2-43,1 • File3-44 • File4-44,1
krb5p	• File1-72,9 • File2-72,8 • File3-71,4 • File4-71,2	• File1-143,9 • File2-144,1 • File3-146,9 • File4-147,3

"Obtenga más información sobre Kerberos con NFS para una seguridad sólida"

NFSv4.2

NFSv4.2 se agregó a ONTAP 9.8 y es la última versión de NFSv4.x disponible (RFC-7862). NFSv4.2 no tiene una opción explícita para habilitarlo/deshabilitarlo. En cambio, se habilita/deshabilita junto con NFSv4.1 (`-4.1 enabled`). Si un cliente admite NFSv4.2, negociará la versión más alta compatible de NFS durante el comando de montaje si no se especifica lo contrario con el `minorversion=2` Opción de montaje.

NFSv4.2 en ONTAP admite la siguiente funcionalidad:

- Etiquetas de seguridad (etiquetas MAC)
- Atributos ampliados
- Operaciones de archivos dispersos (FALLOCATE)

pNFS se introdujo con NFSv4.1, pero también es compatible con NFSv4.2, así como con sus características complementarias.

"Obtenga más información sobre la compatibilidad de ONTAP con NFSv4.2"

Comandos, estadísticas y registros de eventos de pNFS

Estos comandos CLI de ONTAP pertenecen específicamente a pNFS. Puede usarlos para configurar, solucionar problemas y recopilar estadísticas.

Habilitar NFSv4,1

```
nfs modify -vserver SVM -v4.1 enabled
```

Habilite pNFS

```
nfs modify -vserver SVM -v4.1-pnfs enabled
```

Mostrar dispositivos pNFS (privilegios avanzados)

```
pnfs devices show -vserver SVM
```

```
Vserver Name     Mapping ID      Volume MSID     Mapping Status
Generation
---------------  --------------- --------------- ---------------
-------------
SVM              17              2157024470      notavailable    2
SVM              18              2157024463      notavailable    2
SVM              19              2157024469      available       3
SVM              20              2157024465      available       4
SVM              21              2157024467      available       3
SVM              22              2157024462      available       1
```

Mostrar asignaciones de dispositivos pNFS (privilegios avanzados)

```
pnfs devices mappings show -vserver SVM
```

```
Vserver Name    Mapping ID      Dsid            LIF IP
--------------  --------------- --------------- --------------------
SVM             19              2449            10.x.x.x
SVM             20              2512            10.x.x.y
SVM             21              2447            10.x.x.x
SVM             22              2442            10.x.x.y
```

Capturar contadores de rendimiento específicos de pNFS (privilegios avanzados)

```
statistics start -object nfsv4_1 -vserver SVM -sample-id [optional-name]
```

Ver contadores de rendimiento específicos de pNFS (privilegios avanzados)

```
statistics show -object nfsv4_1 -vserver SVM
```

Ver la lista de contadores específicos de pNFS (privilegios avanzados)

```
statistics catalog counter show -object nfsv4_1 -counter *layout*|*device*
```

```
Object: nfsv4_1

Counter                     Description
--------------------------- ----------------------------------------------
getdeviceinfo_avg_latency   Average latency of NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_error         The number of failed NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_percent       Percentage of NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_success       The number of successful NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_total         Total number of NFSv4.1 GETDEVICEINFO
operations.
getdevicelist_avg_latency   Average latency of NFSv4.1 GETDEVICELIST
operations.
getdevicelist_error         The number of failed NFSv4.1 GETDEVICELIST
operations.
getdevicelist_percent       Percentage of NFSv4.1 GETDEVICELIST
operations.
getdevicelist_success       The number of successful NFSv4.1 GETDEVICELIST
operations.
getdevicelist_total         Total number of NFSv4.1 GETDEVICELIST
operations.
layoutcommit_avg_latency    Average latency of NFSv4.1 LAYOUTCOMMIT
operations.
layoutcommit_error          The number of failed NFSv4.1 LAYOUTCOMMIT
operations.
layoutcommit_percent        Percentage of NFSv4.1 LAYOUTCOMMIT operations.
layoutcommit_success        The number of successful NFSv4.1 LAYOUTCOMMIT
operations.
layoutcommit_total          Total number of NFSv4.1 LAYOUTCOMMIT
operations.
layoutget_avg_latency       Average latency of NFSv4.1 LAYOUTGET
operations.
layoutget_error             The number of failed NFSv4.1 LAYOUTGET
operations.
layoutget_percent           Percentage of NFSv4.1 LAYOUTGET operations.
layoutget_success           The number of successful NFSv4.1 LAYOUTGET
operations.
layoutget_total             Total number of NFSv4.1 LAYOUTGET operations.
```

```
layoutreturn_avg_latency    Average latency of NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_error          The number of failed NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_percent        Percentage of NFSv4.1 LAYOUTRETURN operations.
layoutreturn_success        The number of successful NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_total          Total number of NFSv4.1 LAYOUTRETURN
operations.
```

Ver conexiones de red activas para NFS

Puede verificar si se están realizando múltiples conexiones TCP al SVM con el `network connections active show` dominio.

Por ejemplo, si desea ver los troncales de sesión NFS, busque conexiones de los mismos clientes en diferentes interfaces por nodo:

```
cluster::*> network connections active show -node cluster-0* -vserver PNFS
              Vserver   Interface         Remote
      CID Ctx Name      Name:Local Port   Host:Port
Protocol/Service
--------- --- --------- ----------------- --------------------
----------------
Node: node-01
2304333128 14 PNFS      data1:2049        ubuntu22-224:740     TCP/nfs
2304333144 10 PNFS      data3:2049        ubuntu22-224:864     TCP/nfs
2304333151  5 PNFS      data1:2049        ubuntu22-226:848     TCP/nfs
2304333167 15 PNFS      data3:2049        ubuntu22-226:684     TCP/nfs
Node: node-02
2497668321 12 PNFS      data2:2049        ubuntu22-224:963     TCP/nfs
2497668337 18 PNFS      data4:2049        ubuntu22-224:859     TCP/nfs
2497668344 14 PNFS      data2:2049        ubuntu22-226:675     TCP/nfs
2497668360  7 PNFS      data4:2049        ubuntu22-226:903     TCP/nfs
```

Ver la información de la versión de NFS para los clientes conectados

También puede ver las conexiones NFS con el `nfs connected-clients show` dominio. Tenga en cuenta que la lista de clientes que se muestra son clientes que han tenido tráfico NFS activo en las últimas 48 horas. Es posible que los clientes NFS inactivos (incluso si aún están montados) no aparezcan hasta que se acceda al montaje. Puede filtrarlos para mostrar solo los clientes a los que accedió más recientemente especificando el `-idle-time` característica.

Por ejemplo, para ver clientes con actividad en los últimos 10 minutos para el pNFS SVM:

```
cluster::*> nfs connected-clients show -vserver PNFS -idle-time <10m>

 Node: node-01

Vserver: PNFS Data-Ip: 10.x.x.x Local Remote Client-Ip Protocol Volume
Policy Idle-Time Reqs Reqs Trunking

10.x.x.a nfs4.2 PNFS_root default 9m 10s 0 149 false 10.x.x.a nfs4.2
FG_0001 default 9m 10s 135847 0 false 10.x.x.b nfs4.2 PNFS_root default 8m
12s 0 157 false 10.x.x.b nfs4.2 FG_0001 default 8m 12s 52111 0 false
```

Información relacionada

- "Obtenga más información sobre NFS paralelo (pNFS) en ONTAP"

Dependencias de nomenclatura de archivos y directorios NFS y SMB

Obtenga información sobre las dependencias de nombres de archivos y directorios de ONTAP NFS y SMB

Las convenciones de nomenclatura de archivos y directorios dependen tanto de los sistemas operativos de los clientes de red como de los protocolos de uso compartido de archivos, además de la configuración de idioma del clúster ONTAP y de los clientes.

El sistema operativo y los protocolos de uso compartido de archivos determinan lo siguiente:

- Caracteres que puede utilizar un nombre de archivo
- Distinción entre mayúsculas y minúsculas de un nombre de archivo

ONTAP admite caracteres de varios bytes en nombres de archivos, directorios y qtrees, según la versión de ONTAP.

Obtenga información sobre los caracteres válidos en diferentes sistemas operativos para SVM NFS de ONTAP

Si accede a un archivo o directorio desde clientes con sistemas operativos diferentes, debe utilizar caracteres válidos en ambos sistemas operativos.

Por ejemplo, si utiliza UNIX para crear un archivo o directorio, no utilice dos puntos (:) en el nombre porque no se permiten dos puntos en los nombres de archivos o directorios de MS-dos. Debido a que las restricciones de caracteres válidos varían de un sistema operativo a otro, consulte la documentación del sistema operativo cliente para obtener más información acerca de los caracteres prohibidos.

Obtenga información sobre la distinción entre mayúsculas y minúsculas de los nombres de archivos y directorios en un entorno multiprotocolo ONTAP NFS

Los nombres de archivo y directorio distinguen mayúsculas y minúsculas para los

clientes NFS y no distinguen entre mayúsculas y minúsculas, pero sí lo hacen para los clientes SMB. Debe comprender las implicaciones que tiene en un entorno multiprotocolo y las acciones que podría tener que tomar al especificar la ruta al crear recursos compartidos de SMB y al acceder a datos dentro de los recursos compartidos.

Si un cliente SMB crea un directorio denominado `testdir`, los clientes SMB y NFS muestran el nombre del archivo como `testdir`. Sin embargo, si un usuario SMB intenta crear un nombre de directorio más adelante `TESTDIR` , el nombre no está permitido porque, para el cliente SMB, ese nombre existe actualmente. Si un usuario NFS crea posteriormente un directorio denominado `TESTDIR`, los clientes NFS y SMB muestran el nombre del directorio de forma diferente, de la siguiente manera:

- En los clientes NFS, puede ver los nombres de directorio a medida que se crearon, por ejemplo `testdir` y `TESTDIR`, porque los nombres de directorio distinguen entre mayúsculas y minúsculas.
- Los clientes SMB utilizan los nombres 8.3 para distinguir entre los dos directorios. Un directorio tiene el nombre del archivo base. A directorios adicionales se les asigna un nombre de archivo 8.3.
  - En clientes SMB, puede ver `testdir` y `TESTDI~1`.
  - ONTAP crea el `TESTDI~1` nombre del directorio para diferenciar los dos directorios.

    En este caso, debe usar el nombre 8.3 al especificar una ruta de recurso compartido mientras crea o modifica un recurso compartido en una máquina virtual de almacenamiento (SVM).

Del mismo modo para los archivos, si un cliente SMB lo crea `test.txt`, los clientes SMB y NFS muestran el nombre del archivo como `text.txt`. Sin embargo, si un usuario SMB intenta crear `Test.txt`, el nombre no está permitido porque, para el cliente SMB, ese nombre existe actualmente. Si un usuario NFS crea posteriormente un archivo denominado `Test.txt`, los clientes NFS y SMB muestran el nombre del archivo de forma diferente, de la siguiente manera:

- En los clientes NFS, verá los nombres de archivo a medida que se crearon y `test.txt` `Test.txt` , porque los nombres de archivo distinguen entre mayúsculas y minúsculas.
- Los clientes SMB utilizan los nombres 8.3 para distinguir entre los dos archivos. Un archivo tiene el nombre del archivo base. Se asigna un nombre de archivo 8.3 a archivos adicionales.
  - En clientes SMB, puede ver `test.txt` y `TEST~1.TXT`.
  - ONTAP crea el `TEST~1.TXT` nombre de archivo para diferenciar los dos archivos.

> Si se ha creado una asignación de caracteres con los comandos de asignación de caracteres CIFS de Vserver, una búsqueda de Windows que normalmente no distingue entre mayúsculas y minúsculas puede distinguir entre mayúsculas y minúsculas. Esto significa que las búsquedas de nombre de archivo solo serán sensibles a mayúsculas/minúsculas si se ha creado la asignación de caracteres y el nombre de archivo está utilizando esa asignación de caracteres.

Aprenda a crear nombres de archivos y directorios NFS de ONTAP

ONTAP crea y mantiene dos nombres para archivos o directorios en cualquier directorio que tenga acceso desde un cliente SMB: El nombre largo original y un nombre en formato 8.3.

Para los nombres de archivos o directorios que excedan el nombre de ocho caracteres o el límite de extensión de tres caracteres (para archivos), ONTAP genera un nombre de formato de 8.3 de la siguiente manera:

- Trunca el nombre del archivo o directorio original a seis caracteres, si el nombre supera los seis.
- Agrega una tilde (~) y un número, de uno a cinco, a los nombres de archivo o directorio que ya no son únicos después de truncarse.

  Si se queda sin números porque hay más de cinco nombres similares, crea un nombre único que no tiene relación con el nombre original.

- En el caso de los archivos, trunca la extensión del nombre de archivo a tres caracteres.

Por ejemplo, si un cliente NFS crea un archivo llamado `specifications.html`, el nombre de archivo de formato 8,3 creado por ONTAP es `specif~1.htm`. Si este nombre ya existe, ONTAP utiliza un número diferente al final del nombre de archivo. Por ejemplo, si un cliente NFS crea otro archivo denominado `specifications_new.html`, el formato 8,3 de `specifications_new.html` es `specif~2.htm`.

Obtenga información sobre el manejo de nombres de archivos, directorios y qtree de múltiples bytes en ONTAP NFS

A partir de ONTAP 9.5, la compatibilidad con nombres codificados UTF-8 de 4 bytes permite la creación y visualización de nombres de archivos, directorios y árboles que incluyen caracteres complementarios Unicode fuera del plano multilingüe básico (BMP). En las versiones anteriores, estos caracteres complementarios no se mostraba correctamente en entornos multiprotocolo.

Para habilitar la compatibilidad con nombres codificados UTF-8 de 4 bytes, hay disponible un nuevo código de idioma *utf8mb4* para las `vserver volume` familias de comandos y.

- Debe crear un nuevo volumen de una de las siguientes maneras:
- Configuración `-language` explícita de la opción volume:

  ```
  volume create -language utf8mb4 {…}
  ```

- Heredar `-language` la opción de volumen de una SVM que se haya creado o modificado para la opción:

  ```
  vserver [create|modify] -language utf8mb4 {…}``volume create {…}
  ```

- Si utiliza ONTAP 9,6 y versiones anteriores, no podrá modificar los volúmenes existentes para admitir utf8mb4; debe crear un nuevo volumen listo para utf8mb4 y después migrar los datos con las herramientas de copia basadas en cliente.

  Si utiliza ONTAP 9.7P1 o una versión posterior, puede modificar los volúmenes existentes para utf8mb4 con una solicitud de soporte. Para obtener más información, consulte "¿Se puede cambiar el idioma del volumen después de crearlo en ONTAP?".

+ Puede actualizar SVM para soporte utf8mb4, pero los volúmenes existentes conservan sus códigos de idioma originales.

+

> Los nombres de las LUN con caracteres UTF-8 de 4 bytes no se admiten actualmente.

- Los datos de caracteres Unicode se suelen representar en aplicaciones de sistemas de archivos Windows

que utilizan el formato de transformación Unicode de 16 bits (UTF-16) y en sistemas de archivos NFS que utilizan el formato de transformación Unicode de 8 bits (UTF-8).

En las versiones anteriores a ONTAP 9.5, los nombres incluidos los caracteres complementarios UTF-16 creados por los clientes de Windows se mostraban correctamente a otros clientes de Windows pero no se tradujeron correctamente a UTF-8 para los clientes NFS. Del mismo modo, los nombres con caracteres complementarios UTF-8 de los clientes NFS creados no se tradujeron correctamente a UTF-16 para los clientes Windows.

- Cuando se crean nombres de archivo en sistemas que ejecutan ONTAP 9.4 o una versión anterior que contienen caracteres complementarios válidos o no válidos, ONTAP rechaza el nombre de archivo y devuelve un error de nombre de archivo no válido.

  Para evitar este problema, utilice sólo los caracteres BMP en los nombres de archivo y evite utilizar caracteres complementarios, o actualice a ONTAP 9.5 o posterior.

Se permiten caracteres Unicode en nombres de qtree.

- Puede usar `volume qtree` la familia de comandos o System Manager para configurar o modificar los nombres de qtree.
- Los nombres de qtree pueden incluir caracteres de varios bytes en formato Unicode, como los caracteres japoneses y chinos.
- En versiones anteriores a ONTAP 9.5, sólo se admiten los caracteres BMP (es decir, los que podrían representarse en 3 bytes).

  > En las versiones anteriores a ONTAP 9.5, la ruta de unión del volumen principal del qtree puede contener nombres de qtree y directorio con caracteres Unicode. El `volume show` comando muestra estos nombres correctamente cuando el volumen primario tiene una configuración de idioma UTF-8. Sin embargo, si el idioma del volumen principal no es uno de los valores de idioma UTF-8, algunas partes de la ruta de unión se muestran utilizando un nombre NFS alternativo numérico.

- En las versiones 9.5 y posteriores, se admiten caracteres de 4 bytes en nombres de qtree, siempre y cuando el qtree se encuentre en un volumen habilitado para utf8mb4.

Configurar la asignación de caracteres para la traducción de nombres de archivos SMB en volúmenes NFS de ONTAP

Los clientes NFS pueden crear nombres de archivo que contengan caracteres que no son válidos para los clientes SMB y ciertas aplicaciones Windows. Puede configurar la asignación de caracteres para la traducción de nombres de archivo en volúmenes para permitir que los clientes SMB accedan a archivos con nombres NFS que, de lo contrario, no serían válidos.

Acerca de esta tarea

Cuando los clientes SMB acceden a los archivos creados por los clientes NFS, ONTAP observa el nombre del archivo. Si el nombre no es un nombre de archivo SMB válido (por ejemplo, si tiene un carácter "':'" incrustado en dos puntos), ONTAP devuelve el nombre de archivo 8.3 que se mantiene para cada archivo. Sin embargo, esto causa problemas para las aplicaciones que codifican información importante en nombres de archivos largos.

Por lo tanto, si comparte un archivo entre clientes en diferentes sistemas operativos, debe utilizar caracteres en los nombres de archivo válidos en ambos sistemas operativos.

Sin embargo, si tiene clientes NFS que crean nombres de archivo que contienen caracteres que no son nombres de archivo válidos para clientes SMB, puede definir un mapa que convierte los caracteres NFS no válidos en caracteres Unicode que tanto SMB como determinadas aplicaciones Windows aceptan. Por ejemplo, esta funcionalidad admite las aplicaciones CATIA MCAD y Mathematica, así como otras aplicaciones que tienen este requisito.

Puede configurar la asignación de caracteres de volumen a volumen.

Debe tener en cuenta lo siguiente al configurar la asignación de caracteres en un volumen:

- La asignación de caracteres no se aplica a través de puntos de unión.

  Debe configurar explícitamente la asignación de caracteres para cada volumen de unión.

- Debe asegurarse de que los caracteres Unicode que se utilizan para representar caracteres no válidos o ilegales son caracteres que normalmente no aparecen en los nombres de archivo; de lo contrario, se producen asignaciones no deseadas.

  Por ejemplo, si intenta asignar dos puntos (:) a un guión (-) pero el guión (-) se utilizó correctamente en el nombre del archivo, un cliente de Windows que intente acceder a un archivo denominado «'a-b'» tendría su solicitud asignada al nombre NFS de «'a:b'» (no al resultado deseado).

- Después de aplicar la asignación de caracteres, si la asignación aún contiene un carácter de Windows no válido, ONTAP vuelve a los nombres de archivo de Windows 8.3.
- En las notificaciones de FPolicy, los registros de auditoría de NAS y los mensajes de seguimiento de seguridad, se muestran los nombres de archivos asignados.
- Cuando se crea una relación de SnapMirror del tipo DP, la asignación de caracteres del volumen de origen no se replica en el volumen de DP de destino.
- Distinción entre mayúsculas y minúsculas: Debido a que los nombres de Windows asignados se convierten en nombres NFS, la búsqueda de los nombres sigue a la semántica NFS. Esto incluye el hecho de que las búsquedas de NFS distinguen mayúsculas de minúsculas. Esto significa que las aplicaciones que acceden a recursos compartidos asignados no deben depender de un comportamiento que no distingue mayúsculas y minúsculas de Windows. Sin embargo, el nombre 8.3 está disponible y no distingue mayúsculas y minúsculas.
- Asignaciones parciales o no válidas: Tras asignar un nombre para devolver a los clientes que realizan enumeración de directorios ("dir"), se comprueba la validez de Windows en el nombre Unicode resultante. Si ese nombre sigue teniendo caracteres no válidos, o si no es válido para Windows (p. ej., finaliza en "". o en blanco) se devuelve el nombre 8.3 en lugar del nombre no válido.

Paso

1. Configurar asignación de caracteres:

   ```
   vserver cifs character-mapping create -vserver vserver_name -volume
   volume_name -mapping mapping_text, ...
   ```

   El mapeo consta de una lista de pares de caracteres fuente-objetivo separados por "':'". Los caracteres son caracteres Unicode introducidos mediante dígitos hexadecimales. Por ejemplo: 3C:E03C.

   El primer valor de cada `mapping_text` par que está separado por dos puntos es el valor hexadecimal del carácter NFS que desea traducir, y el segundo valor es el valor Unicode que utiliza SMB. Las parejas de

asignación deben ser únicas (debe existir una asignación uno a uno).

- Asignación de origen

  La siguiente tabla muestra el conjunto de caracteres Unicode permisible para la asignación de origen:

Carácter Unicode	Carácter impreso	Descripción
0x01-0x19	No aplicable	Caracteres de control que no se imprimen
0x5C	\	Barra invertida
0x3A	:	Dos puntos
0x2A	*	Asterisco
0x3F	?	Signo de interrogación
0x22	"	Entre comillas
0x3C	<	Menor que
0x3E	>	Mayor que
0x7C		
Línea vertical	0xB1	±

- Asignación de objetivos

  Puede especificar caracteres de destino en el "'Área de uso privado'" de Unicode en el siguiente intervalo: U+E0000…U+F8FF.

Ejemplo

El siguiente comando crea una asignación de caracteres para un volumen denominado «data» en la máquina virtual de almacenamiento (SVM) vs1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  -----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

Comandos NFS de ONTAP para administrar asignaciones de caracteres para la traducción de nombres de archivos SMB

Puede gestionar la asignación de caracteres creando, modificando, mostrando información o eliminando asignaciones de caracteres de archivo utilizadas para la traducción del nombre del archivo SMB en volúmenes FlexVol.

Si desea…	Se usa este comando…
Cree nuevas asignaciones de caracteres de archivo	`vserver cifs character-mapping create`
Mostrar información acerca de las asignaciones de caracteres de archivo	`vserver cifs character-mapping show`
Modifique las asignaciones de caracteres de archivo existentes	`vserver cifs character-mapping modify`
Eliminar asignaciones de caracteres de archivo	`vserver cifs character-mapping delete`

Obtenga más información sobre `vserver cifs character-mapping` en el "Referencia de comandos del ONTAP".