Gestione el acceso a archivos mediante NFS

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/es-es/ontap/nfs-admin/enable-disable-nfsv3-task.html on April 24, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Gestione el acceso a archivos mediante NFS . . . 1
- Habilite o deshabilite NFSv3 . . . 1
- Activar o desactivar NFSv4.0 . . . 1
- Habilitar o deshabilitar NFSv4.1 . . . 1
- Gestione los límites de los grupos de almacenamiento de NFSv4 . . . 2
- Habilite o deshabilite pNFS . . . 4
- Control del acceso NFS a través de TCP y UDP . . . 5
- Controle las solicitudes NFS de puertos no reservados . . . 6
- Gestione el acceso NFS a volúmenes NTFS o qtrees para usuarios UNIX desconocidos . . . 6
- Consideraciones sobre los clientes que montan exportaciones NFS mediante un puerto no reservado . . . 7
- Realice una comprobación de acceso más estricta para los grupos de red mediante la verificación de dominios . . . 8
- Modifique los puertos que se utilizan para los servicios NFSv3 . . . 9
- Comandos para gestionar servidores NFS . . . 10
- Solucionar problemas del servicio de nombres . . . 11
- Verifique las conexiones del servicio de nombres . . . 14
- Comandos para administrar las entradas del conmutador de servicio de nombres . . . 15
- Comandos para gestionar la caché de servicio de nombres . . . 16
- Comandos para gestionar las asignaciones de nombres . . . 16
- Comandos para gestionar usuarios UNIX locales . . . 17
- Comandos para administrar grupos UNIX locales . . . 17
- Límites para usuarios, grupos y miembros de grupo de UNIX locales . . . 18
- Administrar límites para usuarios y grupos de UNIX locales . . . 18
- Comandos para administrar grupos de red locales . . . 19
- Comandos para administrar configuraciones de dominio NIS . . . 19
- Comandos para gestionar las configuraciones del cliente LDAP . . . 20
- Comandos para gestionar las configuraciones LDAP . . . 21
- Comandos para administrar plantillas de esquema de cliente LDAP . . . 21
- Comandos para gestionar las configuraciones de la interfaz de Kerberos de NFS . . . 22
- Comandos para gestionar configuraciones de dominio de Kerberos de NFS . . . 22
- Comandos para gestionar políticas de exportación . . . 23
- Comandos para gestionar las reglas de exportación . . . 23
- Configure la caché de credenciales NFS . . . 24
- Gestione las cachés de la política de exportación . . . 26
- Administrar bloqueos de archivos . . . 30
- Cómo funcionan los filtros de primera lectura y primera escritura de FPolicy con NFS . . . 35
- Modifique el ID de implementación del servidor NFSv4.1 . . . 36
- Gestione las ACL de NFSv4 . . . 37
- Gestione las delegaciones de archivos NFSv4 . . . 40
- Configure el bloqueo de archivos y registros de NFSv4 . . . 41
- Cómo funcionan las referencias de NFSv4 . . . 43
- Habilite o deshabilite las referencias de NFSv4 . . . 43
- Muestra las estadísticas de NFS . . . 44

Mostrar las estadísticas de DNS 45
Mostrar estadísticas NIS 47
Compatibilidad con VMware vStorage sobre NFS 49
Activar o desactivar VMware vStorage over NFS 49
Activa o desactiva la compatibilidad con rquota 50
Mejora del rendimiento de NFSv3 y NFSv4 mediante la modificación del tamaño de transferencia de TCP 51
Modifique el tamaño de transferencia máximo de TCP de NFSv3 y NFSv4 51
Configure el número de ID de grupo permitidos para los usuarios NFS 52
Controlar el acceso de usuario raíz a datos de estilo de seguridad NTFS 54

Gestione el acceso a archivos mediante NFS

Habilite o deshabilite NFSv3

Puede habilitar o deshabilitar NFSv3 modificando el `-v3` opción. De este modo, los clientes pueden acceder a archivos mediante el protocolo NFSv3. De forma predeterminada, NFSv3 está habilitado.

Paso

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el comando…
Habilite NFSv3	`vserver nfs modify -vserver vserver_name -v3 enabled`
Desactive NFSv3	`vserver nfs modify -vserver vserver_name -v3 disabled`

Activar o desactivar NFSv4.0

Puede activar o desactivar NFSv4.0 modificando el `-v4.0` opción. De este modo, los clientes pueden acceder a los archivos mediante el protocolo NFSv4.0. En ONTAP 9.9.1, NFSv4.0 está habilitado de forma predeterminada; en 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`
Deshabilite NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 disabled`

Habilitar o deshabilitar NFSv4.1

Puede activar o desactivar NFSv4,1 modificando el `-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`

Gestione los límites de los grupos de almacenamiento de 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

La `vserver nfs storepool show` comando muestra el número de recursos de la agrupación de almacenamiento 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 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 la `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 la `vserver nfs storepool blocked-client flush -client-ip <ip address>` comando para vaciar la caché de cliente bloqueada de storepool.
2. Utilice la `vserver nfs storepool blocked-client show` 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.
```

Habilite o deshabilite pNFS

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 el `-v4.1-pnfs` opción.

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

Lo que necesitará

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

Control del acceso NFS a través de TCP y UDP

Puede habilitar o deshabilitar el acceso de NFS a máquinas virtuales de almacenamiento (SVM) a través de TCP y UDP modificando el `-tcp` y.. `-udp` parámetros, 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 deshabilitar TCP con 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…
Habilitado a través de TCP	`vserver nfs modify -vserver vserver_name -tcp enabled`
Deshabilitado a través de 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`

Controle las solicitudes NFS de puertos no reservados

Puede rechazar las solicitudes de montaje de NFS de puertos no reservados habilitando el `-mount-rootonly` opción. Para rechazar todas las solicitudes NFS de puertos no reservados, puede habilitar el `-nfs-rootonly` opción.

Acerca de esta tarea

De forma predeterminada, la opción `-mount-rootonly` es `enabled`.

De forma predeterminada, 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`

Gestione el acceso NFS a volúmenes NTFS o qtrees para usuarios UNIX desconocidos

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.

Lo que necesitará

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 sobre los clientes que montan exportaciones NFS mediante un puerto no reservado

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

Si la `-mount-rootonly` La opción está habilitada, ONTAP no permite que los clientes NFS que utilizan puertos no reservados, lo cual significa que los puertos con números superiores a 1,023, no puedan montar exportaciones NFS.

Realice una comprobación de acceso más estricta para los grupos de red mediante la verificación de dominios

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 gestionarlo modificando el `-netgroup-dns-domain-search` 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
   ```

Modifique los puertos que se utilizan para los servicios NFSv3

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.

Lo que necesitará

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

Modifique un servidor NFS	`vserver nfs modify`
Eliminar un servidor NFS	`vserver nfs delete`
Oculte el `.snapshot` Lista de directorios en puntos de montaje NFSv3 Acceso explícito a la `.snapshot` se seguirá permitiendo el directorio aunque la opción esté activada.	`vserver nfs` comandos con el `-v3-hide-snapshot` opción habilitada

Consulte la página de manual de cada comando para obtener más información.

Solucionar problemas del servicio de nombres

Cuando los clientes experimentan errores de acceso debido a problemas del servicio de nombres, puede utilizar el `vserver services name-service getxxbyyy` familia de comandos para realizar manualmente varias búsquedas del servicio de nombres y examinar los detalles y los 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 mediante el `-is-tld-query -enabled false` de la `vserver services name-service dns modify` comando.

Información relacionada

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

Verifique las conexiones del servicio de nombres

A partir de ONTAP 9.2, puede comprobar los servidores de nombres DNS y LDAP para verificar que están 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` el campo es verdadero (el valor predeterminado 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 para administrar las entradas del conmutador de servicio de nombres

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`

Consulte la página de manual de cada comando para obtener más información.

Información relacionada

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

Comandos para gestionar la caché de servicio de nombres

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

"Comandos de ONTAP 9"

Comandos para gestionar las asignaciones de nombres

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`

Cambie la posición de dos asignaciones de nombre NOTA: No se permite un intercambio cuando la asignación de nombres está configurada con una entrada de cualificador de 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`

Consulte la página de manual de cada comando para obtener más información.

Comandos para gestionar usuarios UNIX locales

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`

Consulte la página de manual de cada comando para obtener más información.

Comandos para administrar grupos UNIX locales

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`

Consulte la página de manual de cada comando para obtener más información.

Límites para usuarios, grupos y miembros de grupo de UNIX locales

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 de UNIX locales

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`

Consulte la página de manual de cada comando para obtener más información.

Comandos para administrar grupos de red locales

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`

Consulte la página de manual de cada comando para obtener más información.

Comandos para administrar configuraciones de dominio NIS

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 a nivel de privilegio avanzado y superior.
Borrar estadísticas de NIS	`vserver services name-service nis-domain clear-statistics` Disponible a 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 a nivel de privilegio avanzado y superior.

Consulte la página de manual de cada comando para obtener más información.

Comandos para gestionar las configuraciones del cliente LDAP

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`

Consulte la página de manual de cada comando para obtener más información.

Comandos para gestionar las configuraciones LDAP

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`

Consulte la página de manual de cada comando para obtener más información.

Comandos para administrar plantillas de esquema de cliente LDAP

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 a 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 a nivel de privilegio avanzado y superior.
Eliminar una plantilla de esquema LDAP	`vserver services name-service ldap client schema delete` Disponible a nivel de privilegio avanzado y superior.

Consulte la página de manual de cada comando para obtener más información.

Comandos para gestionar las configuraciones de la interfaz de 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`

Consulte la página de manual de cada comando para obtener más información.

Comandos para gestionar configuraciones de dominio de 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`

Si desea…	Se usa este comando…
Elimine una configuración de dominio de Kerberos para NFS	`vserver nfs kerberos realm delete`

Consulte la página de manual de cada comando para obtener más información.

Comandos 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`

Consulte la página de manual de cada comando para obtener más información.

Comandos para gestionar las 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.

Consulte la página de manual de cada comando para obtener más información.

Configure la caché de credenciales NFS

Motivos para modificar el tiempo de funcionamiento de la caché de credenciales NFS

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.

Si…	La ventaja es…	La desventaja es…
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.
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.

Configure el tiempo de espera para las credenciales de usuario NFS almacenadas en caché

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 de 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

Volcar cachés de políticas de exportación

ONTAP usa varios cachés de políticas de exportación para almacenar información relacionada con las políticas de exportación para agilizar el acceso. Vaciado manual de las cachés de directivas de exportación (`vserver export-policy cache flush`) Quita información potencialmente obsoleta y fuerza a ONTAP a recuperar información actual de los recursos externos apropiados. 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 la opción `-node` parámetro para especificar el nodo en el que se 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.
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 la opción `-node` parámetro para especificar el nodo en el que se 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 la caché del grupo de red de directivas de exportación

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 directivas de exportación, puede utilizar la `vserver export-policy netgroup queue show` y.. `vserver export-policy netgroup cache show` comandos para mostrar el estado de la cola de netgroup y el contenido de la caché de netgroup.

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`

Consulte la página de manual de cada comando para obtener más información.

Compruebe si una dirección IP de cliente es miembro de un grupo de red

Al solucionar problemas de acceso de cliente NFS relacionados con los grupos de red, puede utilizar `vserver export-policy netgroup check-membership` Comando para ayudar a determinar si una IP de cliente es miembro de un determinado netgroup.

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 al grupo de redes a 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 la `vserver export-policy netgroup queue show` comando para supervisar la carga del netgroup y volver a intentar la comprobación después de que haya finalizado.

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

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

Acerca del bloqueo de archivos entre protocolos

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, operaciones de manipulación de archivos como `rm`, `rmdir`, y. `mv` Puede provocar un fallo en 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.

Cómo trata ONTAP bits de sólo lectura

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.

> 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.

Diferencias entre ONTAP y Windows al administrar bloqueos en los componentes de ruta de acceso compartida

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 acerca de "Cómo evitar que se cambie el nombre de los directorios mientras los clientes

acceden a ellos".

Mostrar información sobre bloqueos

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.

La `vserver locks show` el 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. Consulte la página de manual del comando para obtener más información.

Paso

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

Ejemplos

En el siguiente ejemplo, se muestra información de resumen para un bloqueo de 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
```

En el siguiente ejemplo se muestra información detallada sobre oplock y sharelock acerca del 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
```

Bloqueos de ruptura

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

La `vserver locks break` el comando solo está disponible en el nivel de privilegios avanzado y superior. La página man del comando contiene información detallada.

Pasos

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

   La página man del comando contiene información detallada.

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
   ```

Cómo funcionan los filtros de primera lectura y primera escritura de 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 este filtro se utiliza para eventos NFS, el `-file-session-io-grouping-count` y.. `-file -session-io-grouping-duration` Los ajustes 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 este filtro se utiliza para eventos NFS, el `-file-session-io-grouping-count` y.. `-file -session-io-grouping-duration` Los ajustes determinan la solicitud de primera 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
```

Modifique el ID de implementación del servidor NFSv4.1

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`
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

Ventajas de habilitar las ACL de NFSv4

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

Funcionamiento de las ACL de NFSv4

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 ACL (ACE) de la ACL que se han etiquetado con los indicadores de herencia correspondientes.

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 primaria se hereda aunque `-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 la `-chown-mode` el parámetro se ha establecido en `restricted` con comandos en la `vserver nfs` o. `vserver export-policy rule` Las familias, la propiedad de los archivos solo puede cambiarla el superusuario, incluso si los permisos de disco establecidos con ACL de NFSv4 permiten que un usuario no raíz cambie la propiedad del archivo. Para obtener más información, consulte las páginas de manual correspondientes.

Habilite o deshabilite la modificación de ACL de NFSv4

Cuando ONTAP recibe un `chmod` Comando para un archivo o directorio con una ACL, de forma predeterminada se conserva y se modifica la ACL para reflejar el cambio de bits

de modo. Puede deshabilitar el `-v4-acl-preserve` Parámetro para cambiar el comportamiento si desea que se corte 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
   ```

Cómo utiliza ONTAP las ACL de NFSv4 para determinar si pueden eliminar un archivo

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.

Habilite o deshabilite las ACL de NFSv4

Para habilitar o deshabilitar las ACL de NFSv4, puede modificar las `-v4.0-acl` y.. `-v4.1-acl` opciones. Estas opciones están desactivadas de forma predeterminada.

Acerca de esta tarea

La `-v4.0-acl` o. `-v4.1-acl` La opción controla la configuración y la visualización de 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…
Habilitar ACL de NFSv4.0	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
Desactive 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`

Modifique el límite máximo de ACE para ACL de NFSv4

Puede modificar el número máximo de ACE permitidos para cada ACL de NFSv4 mediante la modificación del 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 `192` para `1024`.

3. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Gestione las delegaciones de archivos NFSv4

Habilite o deshabilite las delegaciones de archivos de lectura de NFSv4

Para habilitar o deshabilitar las delegaciones de archivos de lectura de NFSv4, puede modificar la `-v4.0-read-delegation`o. opción. 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…
Habilite 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`
Deshabilite 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.

Habilite o deshabilite las delegaciones de archivos de escritura de NFSv4

Para habilitar o deshabilitar las delegaciones de archivos de escritura, puede modificar la `-v4.0-write-delegation`o. opción. 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`
Deshabilite las delegaciones de archivos de escritura de NFSv4	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled`
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

Acerca del bloqueo de archivos y registros de NFSv4

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 especificar el período de concesión del bloqueo de NFSv4 (es decir, el período de tiempo en el que ONTAP concede irrevocablemente un bloqueo a un cliente), puede modificar el `-v4-lease-seconds` 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 para esta opción es el período de gracia de bloqueo, que se puede establecer con `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 especificar el período de gracia de bloqueo de 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 el `-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
   ```

Cómo funcionan las referencias de NFSv4

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.

Habilite o deshabilite las referencias de NFSv4

Puede habilitar las referencias de NFSv4 en máquinas virtuales de almacenamiento (SVM) mediante las opciones `-v4-fsid-change` y.. `-v4.0-referrals`o.. 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.

Lo que necesitará

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…
Habilite las referencias de NFSv4	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled` `vserver nfs modify -vserver vserver_name -v4.0-referrals enabled`
Desactive las referencias a 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
```

Muestra las estadísticas de NFS

Puede mostrar estadísticas de NFS de las máquinas virtuales de almacenamiento (SVM) en el sistema de almacenamiento para supervisar el rendimiento y diagnosticar problemas.

Pasos

1. Utilice la `statistics catalog object show` Comando para identificar los objetos NFS desde los que se pueden ver datos.

   ```
   statistics catalog object show -object nfs*
   ```

2. Utilice la `statistics start` y opcional `statistics stop` comandos para recoger un ejemplo de datos de uno o más objetos.
3. Utilice la `statistics show` 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"

Mostrar las estadísticas de DNS

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 la `statistics catalog object show` Comando para identificar los objetos DNS desde los que puede ver datos.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Utilice la `statistics start` y.. `statistics stop` comandos para recoger un ejemplo de datos de uno o más objetos.
3. Utilice la `statistics show` 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"

Mostrar estadísticas NIS

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 la `statistics catalog object show` Comando para identificar los objetos NIS desde los que puede ver datos.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Utilice la `statistics start` y.. `statistics stop` comandos para recoger un ejemplo de datos de uno o más objetos.
3. Utilice la `statistics show` para ver los datos de ejemplo.

Seguimiento de 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"

Compatibilidad con VMware vStorage sobre 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?"

Activar o desactivar VMware vStorage over NFS

Puede habilitar o deshabilitar la compatibilidad de VMware vStorage sobre NFS en máquinas virtuales de almacenamiento (SVM) mediante el `vserver nfs modify` 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"

Activa o desactiva la compatibilidad con rquota

ONTAP admite la versión 1 del protocolo de cuota remota (rcupo v1). El protocolo rquota permite a los clientes NFS obtener información de cuotas para los usuarios desde una máquina remota. Puede habilitar rquota en máquinas virtuales de almacenamiento (SVM) mediante el `vserver nfs modify` comando.

Acerca de esta tarea

De forma predeterminada, rquota está desactivado.

Paso

1. Ejecute una de las siguientes acciones:

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 acerca de las cuotas, consulte "Gestión de almacenamiento lógico".

Mejora del rendimiento de NFSv3 y NFSv4 mediante la modificación del tamaño de transferencia de TCP

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.

Modifique el tamaño de transferencia máximo de TCP de NFSv3 y NFSv4

Puede modificar el `-tcp-max-xfer-size` Opción de configurar los tamaños máximos de transferencia 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, el `v3-tcp-max-read-size` y.. `v3-tcp-max-write-size` las opciones son obsoletas. Debe utilizar el `-tcp-max-xfer-size` en su lugar.

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 la `vserver nfs show -fields tcp-max-xfer-size` 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
```

Configure el número de ID de grupo permitidos para los usuarios NFS

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.

En la siguiente tabla se muestran los dos parámetros del `vserver nfs modify` Comando que determina 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. Compruebe el `-extended-groups-limit` Value y verifique si AUTH_SYS utiliza 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
```

Controlar el acceso de usuario raíz a datos de estilo de seguridad NTFS

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
```

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.