Gestione SMB con la interfaz de línea de comandos

ONTAP 9

NetApp
March 04, 2026

Tabla de contenidos

Gestione SMB con la interfaz de línea de comandos

Obtenga más información sobre SMB de ONTAP

Las funciones de acceso a archivos ONTAP están disponibles para el protocolo SMB. Puede habilitar un servidor CIFS, crear recursos compartidos y habilitar servicios de Microsoft.

SMB (bloque de mensajes del servidor) hace referencia a los dialectos modernos del protocolo del sistema común de archivos de Internet (CIFS). Seguirá viendo *CIFS* en la interfaz de línea de comandos (CLI) de ONTAP y en las herramientas de gestión de OnCommand.

Compatibilidad con servidores SMB

Obtenga más información sobre la compatibilidad con servidores SMB de ONTAP

Puede habilitar y configurar servidores SMB en máquinas virtuales de almacenamiento (SVM) para permitir que los clientes SMB accedan a los archivos del clúster.

- Cada SVM de datos del clúster puede vincularse a exactamente un dominio de Active Directory.
- No es necesario enlazar las SVM de datos con el mismo dominio.
- Pueden vincularse varias SVM al mismo dominio.

Debe configurar las SVM y las LIF que utiliza para proporcionar datos antes de poder crear un servidor SMB. Si la red de datos no es plano, también podría necesitar configurar espacios IP, dominios de retransmisión y subredes.

Información relacionada

"Gestión de redes"

Modificar servidores

"Administración del sistema"

Versiones y funcionalidades de SMB de ONTAP admitidas

Server Message Block (SMB) es un protocolo de uso compartido de archivos remoto que utilizan los servidores y clientes de Microsoft Windows. Todas las versiones de SMB son compatibles. Debe verificar que el servidor SMB de ONTAP admite los clientes y la funcionalidad que se requieren en su entorno.

La información más reciente sobre los clientes SMB y los controladores de dominio compatibles con ONTAP está disponible en *Interoperability Matrix Tool*.

SMB 2,0 y las versiones posteriores se habilitan de forma predeterminada para los servidores SMB de ONTAP, y se pueden habilitar o deshabilitar según sea necesario. SMB 1,0 puede habilitarse o deshabilitarse según sea necesario.

La configuración predeterminada de las conexiones SMB 1.0 y 2.0 con controladoras de dominio también depende de la versión ONTAP. Obtenga más información sobre `vserver cifs security modify` en el "Referencia de comandos del ONTAP". En el caso de entornos con servidores CIFS existentes que ejecuten SMB 1.0, debe migrar a una versión Lo antes posible. de SMB posterior con el fin de prepararse para las mejoras de seguridad y cumplimiento de normativas. Si quiere más información, póngase en contacto con su representante de NetApp.

La siguiente tabla muestra qué funciones de SMB son compatibles con cada versión de SMB. Algunas funciones de SMB se habilitan de forma predeterminada, por lo que algunas requieren más configuración.

Esta funcionalidad:	**Requiere activación:**	**Es compatible con ONTAP 9 para estas versiones SMB:**	
		3,0	3.1.1
Funcionalidad SMB 1.0 heredada		X	X
Asas duraderas		X	X
Operaciones compuestas		X	X
Operaciones asíncronas		X	X
Se han aumentado los tamaños de búfer de lectura y escritura		X	X
Mayor escalabilidad		X	X
Firma SMB	X	X	X
Formato de archivo de flujo de datos alternativo (ADS)	X	X	X
MTU grande (habilitada de forma predeterminada a partir de ONTAP 9.7)	X	X	X
Bloqueos oportunistas del arrendamiento		X	X
Recursos compartidos disponibles en todo momento	X	X	X

Esta funcionalidad:	Requiere activación:	Es compatible con ONTAP 9 para estas versiones SMB:	
Asas persistentes		X	X
Testigo		X	X
CIFRADO SMB: AES-128-CCM	X	X	X
Escalado horizontal (necesario por los recursos compartidos de CA)		X	X
Recuperación transparente tras fallas		X	X
Multicanal de SMB (a partir de ONTAP 9.4)	X	X	X
Integridad de la preautenticación			X
Recuperación tras fallos de cliente de clúster v.2 (CCFv2)			X
CIFRADO SMB: AES-128-GCM	X		X

Información relacionada

Aprenda a utilizar la firma ONTAP para mejorar la seguridad de la red

Establecer el nivel mínimo de seguridad de autenticación del servidor

Configurar el cifrado SMB necesario en servidores SMB para las transferencias de datos a través de SMB

"Interoperabilidad de NetApp"

Funciones de Windows no admitidas en SMB de ONTAP

Antes de utilizar CIFS en la red, debe tener en cuenta determinadas funciones de Windows que ONTAP no admite.

ONTAP no admite las siguientes funciones de Windows:

- Sistema de archivos cifrados (EFS)
- Registro de eventos del sistema de archivos NT (NTFS) en el diario de cambios

- Servicio de replicación de archivos de Microsoft (FRS)
- Servicio de Index Server de Microsoft Windows
- Almacenamiento remoto a través de la gestión de almacenamiento jerárquico (HSM)
- Gestión de cuotas desde clientes Windows
- Semántica de cuotas de Windows
- El archivo LMHOSTS
- Compresión nativa de NTFS

Configure los servicios de nombres NIS o LDAP en las SVM SMB de ONTAP

Con el acceso SMB, se siempre se realiza la asignación de usuario a un usuario UNIX, incluso al acceder a los datos de un volumen de estilo de seguridad NTFS. Si asigna usuarios de Windows a los usuarios UNIX correspondientes cuya información se almacena en almacenes de directorios NIS o LDAP, o si utiliza LDAP para la asignación de nombres, deberá configurar estos servicios de nombres durante la instalación de SMB.

Antes de empezar

Debe haber personalizado la configuración de la base de datos de servicios de nombres para que coincida con su infraestructura de servicios de nombres.

Acerca de esta tarea

Las SVM utilizan las bases de datos ns-switch de servicios de nombres para determinar el orden en el que buscar los orígenes de una base de datos de servicios de nombres determinada. El origen ns-switch puede ser cualquier combinación de `files` , , `nis` o `ldap`. En la base de datos de grupos, ONTAP intenta obtener las pertenencias a grupos de todos los orígenes configurados y, a continuación, utiliza la información consolidada de pertenencia a grupos para las comprobaciones de acceso. Si uno de estos orígenes no está disponible en el momento de obtener información del grupo UNIX, ONTAP no puede obtener las credenciales de UNIX completas y las comprobaciones de acceso posteriores podrían fallar. Por lo tanto, siempre debe comprobar que todas las fuentes del conmutador ns están configuradas para la base de datos de grupo en la configuración del conmutador ns.

El valor predeterminado es que el servidor SMB asigne todos los usuarios de Windows al usuario UNIX predeterminado que se almacena en la `passwd` base de datos local. Si desea utilizar la configuración predeterminada, es opcional configurar los servicios de nombre de usuario y grupo de UNIX NIS o LDAP, o la asignación de usuario LDAP para el acceso a SMB.

Pasos

1. Si la información de usuario, grupo y netgroup de UNIX es administrada por servicios de nombres NIS, configure los servicios de nombres NIS:

   a. Determine el orden actual de los servicios de nombres mediante el `vserver services name-service ns-switch show` comando.

      En este ejemplo, las tres bases de datos (`group`, `passwd` y `netgroup`) que se pueden utilizar `nis` como origen de servicio de nombres sólo se utilizan `files` como origen.

      ```
      vserver services name-service ns-switch show -vserver vs1
      ```

```
                                                          Source
Vserver         Database       Enabled         Order
--------------- ------------   ---------       ---------
vs1             hosts          true            dns,
                                                files
vs1             group          true            files
vs1             passwd         true            files
vs1             netgroup       true            files
vs1             namemap        true            files
```

Debe añadir el `nis` origen a `group` `passwd` las bases de datos y, opcionalmente, a la `netgroup` base de datos.

b. Ajuste el orden de la base de datos ns-switch del servicio de nombres como desee mediante el `vserver services name-service ns-switch modify` comando.

Para obtener el mejor rendimiento, no debe agregar un servicio de nombres a una base de datos del servicio de nombres a menos que planifique configurar ese servicio de nombres en la SVM.

Si modifica la configuración de más de una base de datos de servicio de nombres, debe ejecutar el comando por separado para cada base de datos de servicio de nombres que desee modificar.

En este ejemplo, `nis` y `files` se configuran como orígenes para las `group` `passwd` bases de datos y, en ese orden. El resto de las bases de datos de servicios de nombres no han cambiado.

```
vserver services name-service ns-switch modify -vserver vs1 -database group
-sources nis,files vserver services name-service ns-switch modify -vserver
vs1 -database passwd -sources nis,files
```

c. Compruebe que el orden de los servicios de nombres es correcto mediante el `vserver services name-service ns-switch show` comando.

```
vserver services name-service ns-switch show -vserver vs1
```

```
                                                          Source
Vserver         Database       Enabled         Order
--------------- ------------   ---------       ---------
vs1             hosts          true            dns,
                                                files
vs1             group          true            nis,
                                                files
vs1             passwd         true            nis,
                                                files
vs1             netgroup       true            files
vs1             namemap        true            files
```

d. Cree la configuración del servicio de nombres NIS:

```
vserver services name-service nis-domain create -vserver <vserver_name>
-domain <NIS_domain_name> -servers <NIS_server_IPaddress>,…

vserver services name-service nis-domain create -vserver vs1 -domain
example.com -servers 10.0.0.60
```

de host o una dirección IP para el servidor NIS.

e. Compruebe que el servicio de nombres NIS está configurado correctamente: `vserver services name-service nis-domain show vserver <vserver_name>`

```
vserver services name-service nis-domain show vserver vs1
```

```
Vserver       Domain              Server
------------- ------------------- ---------------
vs1           example.com         10.0.0.60
```

2. Si los servicios de nombres LDAP gestionan la información de usuarios, grupos y grupos de red de UNIX o la asignación de nombres, configure los servicios de nombres LDAP mediante la información ubicada "Gestión de NFS".

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

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

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

Tipos de base de datos

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

Tipo de base de datos	Define orígenes de servicio de nombres para…	Los orígenes válidos son…
hosts	Conversión de nombres de host a direcciones IP	archivos, dns
grupo	Búsqueda de información de grupo de usuarios	archivos, nis, ldap

Tipo de base de datos	Define orígenes de servicio de nombres para…	Los orígenes válidos son…
passwd	Búsqueda de información de usuario	archivos, nis, ldap
grupo de red	Buscando información de netgroup	archivos, nis, ldap
mapa de nombres	Asignando los nombres de usuario	archivos, ldap

Tipos de origen

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

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

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

nis	Servidores NIS externos tal como se especifica en la configuración de dominio NIS de la SVM	`vserver services name-service nis-domain`
ldap	Servidores LDAP externos tal como se especifica en la configuración del cliente LDAP de la SVM	`vserver services name-service ldap`
dns	Servidores DNS externos como se especifica en la configuración de DNS de la SVM	`vserver services name-service dns`

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

Protocolos utilizados para acceder a fuentes externas

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

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

Ejemplo

En el siguiente ejemplo, se muestra la configuración del switch del servicio de nombres para la SVM `svm_1`:

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

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

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

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

Gestione servidores SMB

Modificar los servidores SMB de ONTAP

Puede mover un servidor SMB de un grupo de trabajo a un dominio de Active Directory, de un grupo de trabajo a otro grupo de trabajo o de un dominio de Active Directory a un grupo de trabajo mediante el `vserver cifs modify` comando.

Acerca de esta tarea

También puede modificar otros atributos del servidor SMB, como el nombre del servidor SMB y el estado administrativo. Obtenga más información sobre `vserver cifs modify` en el "Referencia de comandos del ONTAP".

Opciones

- Mover el servidor SMB de un grupo de trabajo a un dominio de Active Directory:

  a. Defina el estado administrativo del servidor SMB en `down`.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

b. Mueva el servidor SMB del grupo de trabajo a un dominio de Active Directory: `vsserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`*

```
Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
```

Para crear una cuenta de máquina de Active Directory para el servidor SMB, debe proporcionar el nombre y la contraseña de una cuenta de Windows con suficiente Privileges para agregar equipos al `ou=`*`example`* `ou` contenedor dentro del *`example`* dominio .com.

A partir de ONTAP 9.7, el administrador de AD puede proporcionarle un URI a un archivo keytab como alternativa a proporcionarle un nombre y una contraseña a una cuenta de Windows con privilegios. Cuando reciba el URI, inclúyalo en el `-keytab-uri` parámetro con `vserver cifs` los comandos.

- Mover el servidor SMB de un grupo de trabajo a otro grupo de trabajo:
  a. Defina el estado administrativo del servidor SMB en `down`.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

  b. Modifique el grupo de trabajo para el servidor SMB: `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`new_workgroup_name`*

```
Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
```

- Mover el servidor SMB de un dominio de Active Directory a un grupo de trabajo:
  a. Defina el estado administrativo del servidor SMB en `down`.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

  b. Mueva el servidor SMB del dominio de Active Directory a un grupo de trabajo: `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`workgroup_name`*

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```

Para entrar en el modo de grupo de trabajo, el sistema debe desactivar todas las características basadas en dominios y eliminar su configuración automáticamente, incluidos los recursos compartidos disponibles continuamente, las instantáneas y AES. Sin embargo, las ACL de uso compartido configuradas por el dominio como "EXAMPLE.COM\userName" no funcionarán correctamente, pero ONTAP no las podrá quitar. Quite estas ACL compartidas Lo antes posible. utilizando herramientas externas una vez completado el comando. Si AES está activado, puede que se le solicite que proporcione el nombre y la contraseña de una cuenta de Windows con los privilegios suficientes para deshabilitarla en el dominio "example.com".

- Modifique otros atributos mediante el parámetro adecuado `vserver cifs modify` del comando.

Utilice opciones para personalizar los servidores SMB

Opciones disponibles para el servidor SMB de ONTAP

Resulta útil saber qué opciones hay disponibles cuando se piensa en cómo personalizar el servidor SMB. Aunque algunas opciones se utilizan para uso general en el servidor SMB, se utilizan varias para habilitar y configurar una funcionalidad SMB específica. Las opciones del servidor SMB se controlan con `vserver cifs options modify` la opción.

En la lista siguiente se especifican las opciones del servidor SMB que están disponibles en el nivel de privilegios de administrador:

- **Configuración del valor de tiempo de espera de la sesión SMB**

  La configuración de esta opción permite especificar el número de segundos de tiempo de inactividad antes de desconectar una sesión SMB. Una sesión inactiva es una sesión en la que un usuario no tiene archivos o directorios abiertos en el cliente. El valor predeterminado es 900 segundos.

- **Configuración del usuario UNIX predeterminado**

  La configuración de esta opción le permite especificar el usuario UNIX predeterminado que utiliza el servidor SMB. ONTAP crea automáticamente un usuario predeterminado denominado «'pcuser'» (con un UID de 65534), crea un grupo denominado «'pcuser'» (con un GID de 65534) y agrega el usuario predeterminado al grupo «'pcuser'». Cuando se crea un servidor SMB, ONTAP configura automáticamente «'pcuser'» como el usuario UNIX predeterminado.

- **Configuración del usuario UNIX invitado**

  Al configurar esta opción, puede especificar el nombre de un usuario UNIX al que se asignan los usuarios que inician sesión desde dominios que no son de confianza, lo que permite a un usuario de un dominio que no es de confianza conectarse con el servidor SMB. De forma predeterminada, esta opción no está configurada (no hay ningún valor predeterminado); por lo tanto, el valor predeterminado es no permitir que los usuarios de dominios que no son de confianza se conecten con el servidor SMB.

- **Activación o desactivación de la ejecución de Read GRANT para bits de modo**

  Habilitar o deshabilitar esta opción permite especificar si se permite a los clientes SMB ejecutar archivos ejecutables con bits de modo UNIX a los que tienen acceso de lectura, incluso cuando el bit ejecutable de UNIX no está establecido. Esta opción está deshabilitada de forma predeterminada.

- **Activación o desactivación de la capacidad de eliminar archivos de sólo lectura de clientes NFS**

  Al habilitar o deshabilitar esta opción, se determina si se permite que los clientes NFS eliminen archivos o carpetas con el conjunto de atributos de sólo lectura. La semántica de eliminación NTFS no permite la eliminación de un archivo o carpeta cuando se establece el atributo de sólo lectura. La semántica de eliminación de UNIX ignora el bit de sólo lectura, utilizando los permisos de directorio principal en su lugar para determinar si un archivo o una carpeta se pueden eliminar. La configuración predeterminada es `disabled`, que da como resultado una semántica de supresión NTFS.

- **Configuración de las direcciones del servidor del Servicio de nombres de Internet de Windows**

  La configuración de esta opción le permite especificar una lista de direcciones de servidor del Servicio de nombres Internet de Windows (WINS) como una lista delimitada por comas. Debe especificar direcciones IPv4. Las direcciones IPv6 no son compatibles. No hay un valor predeterminado.

En la lista siguiente se especifican las opciones del servidor SMB que están disponibles en el nivel de privilegio avanzado:

- **Concesión de permisos de grupo UNIX a usuarios de CIFS**

  La configuración de esta opción determina si el usuario CIFS entrante que no sea el propietario del archivo puede recibir el permiso de grupo. Si el usuario CIFS no es el propietario del archivo de estilo de seguridad UNIX y este parámetro se establece en `true`, se concede el permiso de grupo para el archivo. Si el usuario CIFS no es el propietario del archivo de estilo de seguridad UNIX y este parámetro se establece en `false`, se aplican las reglas UNIX normales para otorgar el permiso al archivo. Este parámetro se aplica a los archivos de estilo de seguridad de UNIX que tienen el permiso establecido `mode bits` como y no es aplicable a los archivos con el modo de seguridad NTFS o NFSv4. El valor predeterminado es `false`.

- **Activación o desactivación de SMB 1,0**

  SMB 1.0 está deshabilitado de forma predeterminada en una SVM para la cual se crea un servidor SMB en ONTAP 9.3.

  > A partir de ONTAP 9.3, SMB 1.0 está deshabilitado de forma predeterminada para los nuevos servidores SMB creados en ONTAP 9.3. Debe migrar a una versión Lo antes posible. posterior de SMB para preparar las mejoras de seguridad y cumplimiento de normativas. Si quiere más información, póngase en contacto con su representante de NetApp.

- **Activación o desactivación de SMB 2.x**

  SMB 2.0 es la versión mínima de SMB que admite la conmutación al nodo de respaldo de LIF. Si deshabilita SMB 2.x, ONTAP también deshabilita automáticamente SMB 3.X.

  SMB 2,0 solo es compatible con las SVM. La opción está habilitada de forma predeterminada en las SVM

- **Activación o desactivación de SMB 3,0**

  SMB 3.0 es la versión mínima de SMB que admite recursos compartidos disponibles de forma continua. Windows Server 2012 y Windows 8 son las versiones mínimas de Windows que admiten SMB 3.0.

  SMB 3,0 solo es compatible con las SVM. La opción está habilitada de forma predeterminada en las SVM

- **Activación o desactivación de SMB 3,1**

  Windows 10 es la única versión de Windows que admite SMB 3.1.

  SMB 3,1 solo es compatible con las SVM. La opción está habilitada de forma predeterminada en las SVM

- **Activación o desactivación de la descarga de copias ODX**

  La descarga de copias ODX la utilizan automáticamente clientes de Windows que son compatibles con esta tecnología. Esta opción está habilitada de forma predeterminada.

- **Activación o desactivación del mecanismo de copia directa para la descarga de copias ODX**

  El mecanismo de copia directa aumenta el rendimiento de la operación de descarga de copia cuando los clientes de Windows intentan abrir el archivo de origen de una copia en un modo que impide que se cambie el archivo mientras la copia está en curso. De forma predeterminada, el mecanismo de copia directa está habilitado.

- **Activación o desactivación de referencias automáticas a nodos**

  Con las referencias automáticas a nodos, el servidor SMB hace referencia automáticamente a una LIF de datos local al nodo que aloja los datos a los que se accede a través del recurso compartido solicitado.

- **Activación o desactivación de políticas de exportación para SMB**

  Esta opción está deshabilitada de forma predeterminada.

- **Activación o desactivación mediante puntos de unión como puntos de reanálisis**

  Si esta opción está habilitada, el servidor SMB expone puntos de unión a clientes SMB como puntos de reanálisis. Esta opción solo es válida para conexiones SMB 2.x o SMB 3.0. Esta opción está habilitada de forma predeterminada.

  Esta opción solo es compatible con las SVM. La opción está habilitada de forma predeterminada en las SVM

- **Configuración del número máximo de operaciones simultáneas por conexión TCP**

  El valor predeterminado es 255.

- **Activación o desactivación de la funcionalidad de grupos y usuarios locales de Windows**

  Esta opción está habilitada de forma predeterminada.

- **Activación o desactivación de la autenticación de usuarios locales de Windows**

  Esta opción está habilitada de forma predeterminada.

- **Activación o desactivación de la función de copia de sombra VSS**

  ONTAP utiliza la funcionalidad de copia de respaldo para realizar backups remotos de los datos almacenados mediante la solución Hyper-V mediante SMB.

  Esta opción solo es compatible con las SVM y solo con configuraciones de Hyper-V en SMB. La opción está habilitada de forma predeterminada en las SVM

- **Configuración de la profundidad del directorio de instantáneas**

  La configuración de esta opción permite definir la profundidad máxima de los directorios en los que crear instantáneas cuando se utiliza la función de copia oculta.

  Esta opción solo es compatible con las SVM y solo con configuraciones de Hyper-V en SMB. La opción está habilitada de forma predeterminada en las SVM

- **Activación o desactivación de las capacidades de búsqueda multidominio para la asignación de nombres**

  Si se habilita, cuando un usuario UNIX se asigna a un usuario de dominio de Windows mediante un comodín (*) en la parte de dominio del nombre de usuario de Windows (por ejemplo, *\joe), ONTAP busca el usuario especificado en todos los dominios con confianzas bidireccionales en el dominio principal. El dominio principal es el dominio que contiene la cuenta de equipo del servidor SMB.

  Como alternativa a la búsqueda en todos los dominios de confianza bidireccional, puede configurar una lista de dominios de confianza preferidos. Si esta opción está activada y se ha configurado una lista preferida, la lista preferida se utiliza para realizar búsquedas de asignación de nombres multidominio.

  La opción predeterminada es habilitar las búsquedas de asignación de nombres multidominio.

- **Configuración del tamaño del sector del sistema de archivos**

  Esta opción le permite configurar el tamaño del sector del sistema de archivos en bytes que ONTAP informa a clientes SMB. Hay dos valores válidos para esta opción `4096`: Y `512`. El valor predeterminado es `4096`. Es posible que deba establecer este valor en `512` si la aplicación Windows admite sólo un tamaño de sector de 512 bytes.

- **Activación o desactivación del control de acceso dinámico**

  Al habilitar esta opción, puede proteger objetos en el servidor SMB mediante el control de acceso dinámico (DAC), incluido el uso de auditorías para organizar políticas de acceso centrales y el uso de objetos de políticas de grupo para implementar políticas de acceso centrales. La opción está deshabilitada de forma predeterminada.

  Esta opción solo es compatible con las SVM.

- **Establecer las restricciones de acceso para sesiones no autenticadas (restringir anónimo)**

  Establecer esta opción determina cuáles son las restricciones de acceso para sesiones no autenticadas. Las restricciones se aplican a usuarios anónimos. De forma predeterminada, no hay restricciones de acceso para los usuarios anónimos.

- **Activación o desactivación de la presentación de ACL NTFS en volúmenes con seguridad efectiva UNIX (volúmenes de estilo de seguridad UNIX o volúmenes mixtos de estilo de seguridad con seguridad efectiva UNIX)**

  Al habilitar o deshabilitar esta opción, se determina cómo se presenta la seguridad de archivos y carpetas con seguridad UNIX a los clientes SMB. Si está habilitada, ONTAP presenta archivos y carpetas en volúmenes con seguridad UNIX para clientes de SMB como si tuviera seguridad de archivos NTFS con ACL de NTFS. Si está deshabilitada, ONTAP presenta volúmenes con seguridad UNIX como volúmenes FAT, sin seguridad de archivos. De forma predeterminada, los volúmenes se presentan como con seguridad de archivos NTFS con ACL NTFS.

- **Activación o desactivación de la funcionalidad de apertura falsa SMB**

  Al habilitar esta funcionalidad, se mejora el rendimiento de SMB 2.x y SMB 3.0, ya que se optimiza cómo ONTAP realiza solicitudes de apertura y cierre al consultar información sobre atributos de archivos y directorios. De manera predeterminada, la funcionalidad abierta falsa del SMB está habilitada. Esta opción solo es útil para las conexiones realizadas con SMB 2.x o posterior.

- **Activación o desactivación de las extensiones UNIX**

  Al habilitar esta opción se habilitan las extensiones UNIX en un servidor SMB. Las extensiones UNIX permiten visualizar la seguridad de estilo POSIX/UNIX a través del protocolo SMB. De forma predeterminada, esta opción está deshabilitada.

  Si tiene clientes SMB basados en UNIX, como clientes Mac OSX, en su entorno, debe habilitar extensiones UNIX. La habilitación de las extensiones UNIX permite al servidor SMB transmitir la información de seguridad de POSIX/UNIX a través de SMB al cliente basado en UNIX, lo que a continuación convierte la información de seguridad en la seguridad POSIX/UNIX.

- **Activación o desactivación de la compatibilidad para búsquedas cortas de nombres**

  Al habilitar esta opción, el servidor SMB puede realizar búsquedas en nombres cortos. Una consulta de búsqueda con esta opción habilitada intenta coincidir con 8.3 nombres de archivo junto con nombres de archivo largos. El valor por defecto de este parámetro es `false`.

- **Activación o desactivación del soporte para la publicidad automática de capacidades DFS**

  Habilitar o deshabilitar esta opción determina si los servidores SMB anuncian automáticamente capacidades DFS a clientes SMB 2.x y SMB 3.0 que se conectan a recursos compartidos. ONTAP utiliza referencias DFS en la implementación de enlaces simbólicos para el acceso a SMB. Si está habilitada, el servidor SMB siempre anuncia las capacidades DFS independientemente de si el acceso al enlace simbólico está habilitado. Si está deshabilitado, el servidor SMB anuncia capacidades DFS solo cuando los clientes se conectan a recursos compartidos donde se habilita el acceso al enlace simbólico.

- **Configuración del número máximo de créditos SMB**

  A partir de ONTAP 9.4, configurar la `-max-credits` opción le permite limitar el número de créditos que se otorgarán en una conexión SMB cuando los clientes y el servidor ejecuten SMB versión 2 o posterior. El valor predeterminado es 128.

- **Activación o desactivación de la compatibilidad con SMB multicanal**

  Al habilitar `-is-multichannel-enabled` la opción en ONTAP 9.4 y versiones posteriores, el servidor SMB puede establecer varias conexiones para una única sesión SMB cuando se implementan las NIC adecuadas en el clúster y sus clientes. Al hacerlo, se mejora el rendimiento y la tolerancia a fallos. El valor por defecto de este parámetro es `false`.

  Cuando se habilita SMB MultiChannel, también es posible especificar los siguientes parámetros:

  - El número máximo de conexiones permitidas por sesión multicanal. El valor predeterminado para este parámetro es 32.
  - Número máximo de interfaces de red anunciadas por sesión multicanal. El valor predeterminado para este parámetro es 256.

Configure las opciones del servidor SMB de ONTAP

Puede configurar las opciones del servidor SMB en cualquier momento después de crear un servidor SMB en una máquina virtual de almacenamiento (SVM).

Paso

1. Realice la acción deseada:

Si desea configurar opciones del servidor SMB…	Introduzca el comando…
En el nivel de privilegios de administrador	`vserver cifs options modify -vserver` *`vserver_name options`*
En el nivel de privilegios avanzados	a. `set -privilege advanced` b. `vserver cifs options modify -vserver` *`vserver_name options`* c. `set -privilege admin`

Obtenga más información sobre `vserver cifs options modify` las opciones del servidor SMB y configurarlas en el "Referencia de comandos del ONTAP".

Configure el permiso para otorgar grupos UNIX a los usuarios SMB de ONTAP

Puede configurar esta opción para conceder permisos de grupo para tener acceso a archivos o directorios aunque el usuario SMB entrante no sea el propietario del archivo.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Configure el permiso conceder grupo UNIX según corresponda:

Si desea	Introduzca el comando
Active el acceso a los archivos o directorios para obtener permisos de grupo incluso si el usuario no es el propietario del archivo	`vserver cifs options modify -grant-unix-group-perms-to-others true`
Desactive el acceso a los archivos o directorios para obtener permisos de grupo incluso si el usuario no es el propietario del archivo	`vserver cifs options modify -grant-unix-group-perms-to-others false`

3. Compruebe que la opción está establecida en el valor deseado: `vserver cifs options show -fields grant-unix-group-perms-to-others`
4. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Configura las restricciones de acceso al bloque de mensajes del servidor de ONTAP para usuarios anónimos

De forma predeterminada, un usuario anónimo y sin autenticar (también conocido como *null user*) puede tener acceso a cierta información de la red. Puede usar una opción de servidor SMB para configurar restricciones de acceso para el usuario anónimo.

Acerca de esta tarea

`-restrict-anonymous`La opción Servidor SMB corresponde a la `RestrictAnonymous` entrada del Registro en Windows.

Los usuarios anónimos pueden enumerar o enumerar determinados tipos de información del sistema de los hosts de Windows de la red, incluidos los nombres y detalles de usuario, las directivas de cuenta y los nombres de recursos compartidos. Puede controlar el acceso para el usuario anónimo especificando uno de tres ajustes de restricción de acceso:

Valor	Descripción
`no-restriction` (predeterminado)	Especifica que no hay restricciones de acceso para los usuarios anónimos.
`no-enumeration`	Especifica que sólo la enumeración está restringida a los usuarios anónimos.
`no-access`	Especifica que el acceso está restringido para usuarios anónimos.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Configure el valor Restringir anónimo: `vserver cifs options modify -vserver` *`vserver_name`* `-restrict-anonymous {no-restriction|no-enumeration|no-access}`
3. Compruebe que la opción está establecida en el valor deseado: `vserver cifs options show -vserver` *`vserver_name`*
4. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Información relacionada

Opciones de servidor disponibles

Gestione cómo se presenta la seguridad de archivos a los clientes SMB para los datos de estilo de seguridad UNIX

Obtenga más información sobre la presentación de la seguridad de archivos ONTAP a clientes pymes para datos de tipo de seguridad de UNIX

Puede elegir cómo desea presentar la seguridad de archivos a los clientes de SMB para los datos de estilo de seguridad de UNIX habilitando o deshabilitando la presentación de ACL NTFS a clientes SMB. Existen ventajas en cada entorno, que debe entender para

elegir el ajuste que mejor se ajuste a los requisitos de su negocio.

De forma predeterminada, ONTAP presenta los permisos de UNIX sobre volúmenes de estilo de seguridad de UNIX a clientes de SMB como ACL de NTFS. Hay escenarios en los que esto es deseable, incluyendo los siguientes:

- Desea ver y editar los permisos de UNIX mediante la ficha **Seguridad** del cuadro Propiedades de Windows.

  No puede modificar los permisos de un cliente Windows si el sistema UNIX no permite la operación. Por ejemplo, no puede cambiar la propiedad de un archivo que no posee, ya que el sistema UNIX no permite esta operación. Esta restricción impide a los clientes SMB omitir los permisos de UNIX establecidos en los archivos y carpetas.

- Los usuarios están editando y guardando archivos en el volumen de estilo de seguridad de UNIX utilizando ciertas aplicaciones de Windows, por ejemplo, Microsoft Office, donde ONTAP debe conservar los permisos de UNIX durante las operaciones de guardado.
- Hay ciertas aplicaciones de Windows en su entorno que esperan leer ACL NTFS en los archivos que utilizan.

En determinadas circunstancias, es posible que desee deshabilitar la presentación de permisos UNIX como ACL NTFS. Si esta funcionalidad está deshabilitada, ONTAP presenta volúmenes de estilo de seguridad UNIX como volúmenes FAT a clientes SMB. Hay motivos específicos por los que puede que desee presentar volúmenes de estilo de seguridad de UNIX como volúmenes FAT a clientes SMB:

- Sólo se pueden cambiar los permisos de UNIX mediante montajes en clientes UNIX.

  La pestaña Seguridad no está disponible cuando se asigna un volumen de estilo de seguridad UNIX en un cliente SMB. La unidad asignada parece formatearse con el sistema de archivos FAT, que no tiene permisos de archivo.

- Está utilizando aplicaciones a través de SMB que establecen ACL NTFS en archivos y carpetas a los que se tiene acceso, lo cual puede fallar si los datos residen en volúmenes de estilo de seguridad de UNIX.

  Si ONTAP informa del volumen como FAT, la aplicación no intenta cambiar una ACL.

Información relacionada

- Configurar estilos de seguridad en volúmenes FlexVol
- Configurar estilos de seguridad en qtrees

Configure la presentación de ACL NTFS a los clientes SMB de ONTAP para datos de estilo de seguridad de UNIX

Puede habilitar o deshabilitar la presentación de ACL NTFS a clientes SMB para datos de estilo de seguridad de UNIX (volúmenes de estilo de seguridad de UNIX y volúmenes mixtos de estilo de seguridad con seguridad efectiva de UNIX).

Acerca de esta tarea

Si habilita esta opción, ONTAP presenta archivos y carpetas en volúmenes con un estilo de seguridad UNIX efectivo para los clientes de SMB como si tuviera ACL NTFS. Si deshabilita esta opción, los volúmenes se presentan como volúmenes FAT a los clientes de SMB. El valor predeterminado es presentar ACL de NTFS a los clientes de SMB.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Configure la opción UNIX NTFS ACL: `vserver cifs options modify -vserver vserver_name -is-unix-nt-acl-enabled {true|false}`
3. Compruebe que la opción está establecida en el valor deseado: `vserver cifs options show -vserver vserver_name`
4. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Obtenga más información sobre la conservación de permisos UNIX para volúmenes de FlexVol SMB de ONTAP

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

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

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

Obtenga información sobre la gestión de permisos UNIX mediante la ficha Seguridad de Windows para servidores SMB de ONTAP

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

- Modificación de permisos de UNIX

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

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

- Cambiar los permisos de UNIX a los permisos NTFS

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

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

qtree de estilo de seguridad mixto, cambie el estilo de seguridad efectivo del archivo o carpeta de UNIX a NTFS.

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

Gestione la configuración de seguridad del servidor SMB

Obtenga más información sobre el manejo de la autenticación del cliente SMB de ONTAP

Antes de que los usuarios puedan crear conexiones SMB para acceder a los datos contenidos en la SVM, el dominio al que pertenece el servidor SMB debe autenticarse. El servidor SMB admite dos métodos de autenticación: Kerberos y NTLM (NTLMv1 o NTLMv2). Kerberos es el método predeterminado utilizado para autenticar usuarios de dominio.

Autenticación Kerberos

ONTAP admite la autenticación Kerberos al crear sesiones SMB autenticadas.

Kerberos es el servicio de autenticación principal para Active Directory. El servidor Kerberos o el servicio de centro de distribución de claves Kerberos (KDC) almacena y recupera información acerca de los principios de seguridad en Active Directory. A diferencia del modelo NTLM, los clientes de Active Directory que deseen establecer una sesión con otro equipo, como el servidor SMB, póngase en contacto directamente con un KDC para obtener sus credenciales de sesión.

Autenticación NTLM

La autenticación de clientes NTLM se realiza mediante un protocolo de respuesta a desafío basado en el conocimiento compartido de un secreto específico del usuario basado en una contraseña.

Si un usuario crea una conexión SMB con una cuenta de usuario local de Windows, el servidor SMB realiza la autenticación localmente con NTLMv2.

Obtenga más información sobre la configuración de seguridad del servidor SMB para la configuración de la recuperación ante desastres SVM de ONTAP

Antes de crear una SVM que está configurada como destino de recuperación de desastres en el que la identidad no se conserva (`-identity-preserve`la opción se establece en en `false` en la configuración de SnapMirror), debe conocer cómo se gestionan las configuraciones de seguridad del servidor SMB en la SVM de destino.

- La configuración de seguridad del servidor SMB no predeterminada no se replica en el destino.

  Cuando se crea un servidor SMB en la SVM de destino, todas las opciones de seguridad del servidor SMB se establecen en valores predeterminados. Cuando el destino de recuperación ante desastres de SVM se inicializa, se actualiza o se vuelve a sincronizar, la configuración de seguridad del servidor SMB en el origen no se replica en el destino.

- Debe configurar manualmente las opciones de seguridad del servidor SMB no predeterminadas.

  Si tiene configuradas las opciones de seguridad del servidor SMB no predeterminadas en la SVM de origen, debe configurar manualmente estas mismas opciones en la SVM de destino después de que el destino pase a ser de lectura y escritura (después de que se rompa la relación de SnapMirror).

Mostrar información sobre la configuración de seguridad del servidor SMB de ONTAP

Puede ver información acerca de la configuración de seguridad del servidor SMB en las máquinas virtuales de almacenamiento (SVM). Puede utilizar esta información para comprobar que la configuración de seguridad es correcta.

Acerca de esta tarea

Una configuración de seguridad mostrada puede ser el valor predeterminado para ese objeto o un valor no predeterminado que se configura mediante la CLI de ONTAP o mediante objetos de directiva de grupo de Active Directory (GPO).

No utilice `vserver cifs security show` el comando para servidores SMB en modo de grupo de trabajo, ya que algunas de las opciones no son válidas.

Paso

1. Ejecute una de las siguientes acciones:

Si desea mostrar información acerca de…	Introduzca el comando…
Toda la configuración de seguridad en una SVM especificada	`vserver cifs security show -vserver` *`vserver_name`*
Una configuración o configuración de seguridad específica en la SVM	`vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]` Puede introducir `-fields ?` para determinar qué campos puede utilizar.

Ejemplo

En el siguiente ejemplo, se muestran todas las opciones de seguridad de la SVM vs1:

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                          Kerberos Clock Skew:        5 minutes
                          Kerberos Ticket Age:        10 hours
                         Kerberos Renewal Age:        7 days
                         Kerberos KDC Timeout:        3 seconds
                          Is Signing Required:        false
               Is Password Complexity Required:        true
          Use start_tls For AD LDAP connection:        false
                     Is AES Encryption Enabled:        false
                        LM Compatibility Level:        lm-ntlm-ntlmv2-krb
                    Is SMB Encryption Required:        false
                       Client Session Security:        none
              SMB1 Enabled for DC Connections:        false
              SMB2 Enabled for DC Connections:        system-default
LDAP Referral Enabled For AD LDAP connections:        false
             Use LDAPS for AD LDAP connection:        false
    Encryption is required for DC Connections:        false
 AES session key enabled for NetLogon channel:        false
  Try Channel Binding For AD LDAP Connections:        false
```

Tenga en cuenta que la configuración mostrada depende de la versión de ONTAP en ejecución.

En el siguiente ejemplo, se muestra el desfase de reloj de Kerberos para SVM vs1:

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

            vserver kerberos-clock-skew
            ------- -------------------
            vs1     5
```

Información relacionada

Mostrar información acerca de las configuraciones de GPO

Configure la complejidad de la contraseña de ONTAP para usuarios locales de SMB

La complejidad de contraseña necesaria proporciona una seguridad mejorada para los usuarios de SMB locales en sus máquinas virtuales de almacenamiento (SVM). La función de complejidad de contraseña necesaria está activada de forma predeterminada. Puede deshabilitarla y volver a habilitarla en cualquier momento.

Antes de empezar

Los usuarios locales, los grupos locales y la autenticación de usuarios locales deben estar habilitados en el servidor CIFS.

Acerca de esta tarea

No utilice `vserver cifs security modify` el comando para un servidor CIFS en modo grupo de trabajo porque algunas de las opciones no son válidas.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea que la complejidad de contraseña requerida para los usuarios locales de la SMB sea…	Introduzca el comando…
Activado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required true`
Deshabilitado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required false`

2. Compruebe la configuración de seguridad para la complejidad necesaria de la contraseña: `vserver cifs security show -vserver` *`vserver_name`*

Ejemplo

El siguiente ejemplo muestra que la complejidad de contraseña necesaria está habilitada para los usuarios locales de SMB para SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
------- -------------------------------
vs1     true
```

Información relacionada

- Mostrar información sobre la configuración de seguridad del servidor
- Obtenga información sobre los usuarios y grupos locales
- Requisitos para las contraseñas de usuario local
- Cambiar las contraseñas de la cuenta de usuario local

Modifique la configuración de seguridad de Kerberos del servidor SMB de ONTAP

Puede modificar ciertos ajustes de seguridad Kerberos del servidor CIFS, incluyendo la hora de desfase de reloj de Kerberos máxima permitida, la duración de la incidencia de Kerberos y el número máximo de días de renovación de incidencias.

Acerca de esta tarea

La modificación de la configuración de Kerberos del servidor CIFS mediante `vserver cifs security modify` el comando modifica los ajustes solo en la única máquina virtual de almacenamiento (SVM) que especifique con el `-vserver` parámetro. Puede administrar de forma centralizada la configuración de seguridad Kerberos para todas las SVM del clúster que pertenecen al mismo dominio de Active Directory mediante objetos de directiva de grupo (GPO) de Active Directory.

Pasos

1. Ejecute una o varias de las siguientes acciones:

Si desea…	Introduzca…
Especifique el tiempo máximo permitido de inclinación del reloj Kerberos en minutos (9.13.1 y posteriores) o segundos (9.12.1 o anteriores).	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-clock-skew` *`integer_in_minutes`* El valor predeterminado es 5 minutos.
Especifique la duración del billete Kerberos en horas.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours` El valor predeterminado es 10 horas.
Especifique el número máximo de días de renovación de la tarjeta.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-renew-age` *`integer_in_days`* El valor predeterminado es 7 días.
Especifique el tiempo de espera para los sockets de los KDC después de lo cual todos los KDC están marcados como inaccesibles.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-kdc-timeout` *`integer_in_seconds`* El valor predeterminado es 3 segundos.

2. Compruebe la configuración de seguridad de Kerberos:

   `vserver cifs security show -vserver` *`vserver_name`*

Ejemplo

En el ejemplo siguiente se realizan los cambios siguientes en la seguridad de Kerberos: «'Kerberos Clock Skew» se establece en 3 minutos y «'Kerberos Ticket Age'» se establece en 8 horas para SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                    Kerberos Clock Skew:                    3 minutes
                    Kerberos Ticket Age:                    8 hours
                  Kerberos Renewal Age:                     7 days
                  Kerberos KDC Timeout:                     3 seconds
                    Is Signing Required:                false
         Is Password Complexity Required:                 true
   Use start_tls For AD LDAP connection:                 false
              Is AES Encryption Enabled:                 false
                 LM Compatibility Level:  lm-ntlm-ntlmv2-krb
             Is SMB Encryption Required:                 false
```

Información relacionada

"Mostrar información sobre la configuración de seguridad del servidor"

"Objetos de normativa de grupo compatibles"

"Aplicar objetos de directiva de grupo a servidores CIFS"

Establezca el nivel de seguridad de autenticación mínimo del servidor SMB de ONTAP

Puede establecer el nivel de seguridad mínimo del servidor SMB, también conocido como *LMCompatibilityLevel*, en el servidor SMB para satisfacer los requisitos de seguridad del negocio para el acceso de cliente SMB. El nivel de seguridad mínimo es el nivel mínimo de los tokens de seguridad que acepta el servidor SMB de los clientes SMB.

Acerca de esta tarea

- Los servidores SMB en modo de grupo de trabajo sólo admiten la autenticación NTLM. La autenticación Kerberos no es compatible.
- LmCompatibilityLevel se aplica sólo a la autenticación de cliente SMB, no a la autenticación de administrador.

Es posible configurar el nivel de seguridad de autenticación mínimo en uno de los cuatro niveles de seguridad compatibles.

Valor	Descripción
`lm-ntlm-ntlmv2-krb` (predeterminado)	La máquina virtual de almacenamiento (SVM) acepta seguridad de autenticación LM, NTLMv2 y Kerberos.

Valor	Descripción
`ntlm-ntlmv2-krb`	La SVM acepta la seguridad de autenticación NTLM, NTLMv2 y Kerberos. La SVM rechaza la autenticación LM.
`ntlmv2-krb`	La SVM acepta la seguridad de autenticación NTLMv2 y Kerberos. La SVM rechaza la autenticación LM y NTLM.
`krb`	La SVM solo acepta la seguridad de autenticación de Kerberos. La SVM deniega la autenticación LM, NTLM y NTLMv2.

Pasos

1. Establezca el nivel de seguridad de autenticación mínimo: `vserver cifs security modify -vserver` *`vserver_name`* `-lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. Verifique que el nivel de seguridad de autenticación esté definido en el nivel deseado: `vserver cifs security show -vserver` *`vserver_name`*

Información relacionada

Configurar el cifrado AES para la comunicación basada en Kerberos

Configure la seguridad SMB de ONTAP sólida para la comunicación basada en Kerberos mediante el cifrado AES

Para obtener la mayor seguridad con la comunicación basada en Kerberos, puede habilitar el cifrado AES-256 y AES-128 en el servidor SMB. De manera predeterminada, cuando crea un servidor SMB en la SVM, el cifrado Advanced Encryption Standard (AES) está deshabilitado. Debe habilitarla para aprovechar la seguridad robusta proporcionada por el cifrado AES.

La comunicación relacionada con Kerberos para SMB se utiliza durante la creación del servidor SMB en la SVM, así como durante la fase de configuración de la sesión SMB. El servidor SMB es compatible con los siguientes tipos de cifrado para la comunicación de Kerberos:

- AES 256
- AES 128
- DES
- RC4-HMAC

Si desea utilizar el tipo de cifrado de seguridad más alto para la comunicación de Kerberos, debe habilitar el cifrado AES para la comunicación de Kerberos en la SVM.

Cuando se crea el servidor SMB, el controlador de dominio crea una cuenta de equipo en Active Directory. En este momento, el KDC se da cuenta de las capacidades de cifrado de la cuenta de equipo en particular. Posteriormente, se selecciona un tipo de cifrado concreto para cifrar el ticket de servicio que el cliente presenta al servidor durante la autenticación.

A partir de ONTAP 9.12.1, puede especificar los tipos de cifrado que desea anunciar en el KDC de Active Directory (AD). Puede utilizar `-advertised-enc-types` la opción para habilitar los tipos de cifrado recomendados, y puede utilizarla para deshabilitar los tipos de cifrado más débiles. Aprenda a "Configurar el cifrado AES para la comunicación basada en Kerberos".

> Las nuevas instrucciones de AES (Intel AES ni) están disponibles en SMB 3.0, mejorando el algoritmo AES y acelerando el cifrado de datos con las familias de procesadores compatibles.a partir de SMB 3.1.1, AES-128-GCM reemplaza a AES-128-CCM como el algoritmo hash utilizado por el cifrado SMB.

Información relacionada

Modificar la configuración de seguridad del servidor

Configure el cifrado AES para la comunicación basada en Kerberos SMB de ONTAP

Para aprovechar la seguridad más fuerte con la comunicación basada en Kerberos, debe utilizar el cifrado AES-256 y AES-128 en el servidor SMB. A partir de ONTAP 9.13.1, el cifrado AES está habilitado de forma predeterminada. Si no desea que el servidor SMB seleccione los tipos de cifrado AES para la comunicación basada en Kerberos con el KDC de Active Directory (AD), puede deshabilitar el cifrado AES.

Si el cifrado AES está habilitado de forma predeterminada y si tiene la opción de especificar tipos de cifrado depende de su versión de ONTAP.

Versión de ONTAP	El cifrado AES está activado…	¿Puede especificar tipos de cifrado?
9.13.1 y posterior	De forma predeterminada	Sí
9.12.1	Manualmente	Sí
9.11.1 y anteriores	Manualmente	No

A partir de ONTAP 9.12,1, el cifrado AES se habilita y se deshabilita mediante la `-advertised-enc-types` opción, que le permite especificar los tipos de cifrado anunciados al KDC de AD. La configuración predeterminada es `rc4` AND `des`, pero cuando se especifica un tipo AES, se activa el cifrado AES. También puede utilizar la opción para desactivar explícitamente los tipos de cifrado RC4 y DES más débiles. En ONTAP 9.11,1 y versiones anteriores, debe usar `-is-aes-encryption-enabled` la opción para habilitar y deshabilitar el cifrado AES, y no se pueden especificar los tipos de cifrado.

Para mejorar la seguridad, la máquina virtual de almacenamiento (SVM) cambia su contraseña de cuenta de máquina en AD cada vez que se modifica la opción de seguridad AES. El cambio de la contraseña podría requerir credenciales AD administrativas para la unidad organizativa (OU) que contiene la cuenta del equipo.

Si una SVM se configura como un destino de recuperación ante desastres en el que la identidad no se conserva (`-identity-preserve`la opción se establece en en `false` en la configuración de SnapMirror), los ajustes de seguridad del servidor SMB no predeterminados no se replican en el destino. Si habilitó el cifrado AES en la SVM de origen, debe habilitarla manualmente.

Ejemplo 1. Pasos

ONTAP 9.12.1 y versiones posteriores

1. Ejecute una de las siguientes acciones:

Si desea que los tipos de cifrado AES para la comunicación Kerberos sean…	Introduzca el comando…
Activado	`vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256`
Deshabilitado	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

   Nota: La `-is-aes-encryption-enabled` opción está en desuso en ONTAP 9.12,1 y podría ser eliminada en una versión posterior.

2. Compruebe que el cifrado AES está activado o desactivado como desee: `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

Ejemplos

En el siguiente ejemplo, se habilitan los tipos de cifrado AES para el servidor SMB en la SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs1      aes-128,aes-256
```

En el ejemplo siguiente se habilitan los tipos de cifrado AES para el servidor SMB en la SVM vs2. Se solicita al administrador que introduzca las credenciales AD administrativas para la unidad organizativa que contiene el servidor SMB.

```
cluster1::> vserver cifs security modify -vserver vs2 -advertised-enc
-types aes-128,aes-256

Info: In order to enable SMB AES encryption, the password for the SMB
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs2      aes-128,aes-256
```

ONTAP 9.11.1 y anteriores

1. Ejecute una de las siguientes acciones:

Si desea que los tipos de cifrado AES para la comunicación Kerberos sean…	Introduzca el comando…
Activado	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled true`
Deshabilitado	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false`

2. Compruebe que el cifrado AES está activado o desactivado como desee: `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

   `is-aes-encryption-enabled`El campo muestra `true` si el cifrado AES está activado y `false` si está desactivado.

Ejemplos

En el siguiente ejemplo, se habilitan los tipos de cifrado AES para el servidor SMB en la SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs1      true
```

En el ejemplo siguiente se habilitan los tipos de cifrado AES para el servidor SMB en la SVM vs2. Se solicita al administrador que introduzca las credenciales AD administrativas para la unidad organizativa que contiene el servidor SMB.

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs2      true
```

Información relacionada

"El usuario de dominio no puede iniciar sesión en el clúster con el túnel de dominio"

Utilice la firma SMB para mejorar la seguridad de la red

Obtenga más información sobre el uso de la firma SMB de ONTAP para mejorar la seguridad de la red

La firma SMB ayuda a garantizar que el tráfico de red entre el servidor SMB y el cliente no se vea comprometido; esto evita los ataques de repetición. De forma predeterminada, ONTAP admite la firma SMB cuando lo solicita el cliente. De manera opcional, el administrador de almacenamiento puede configurar el servidor SMB para que requiera la

firma SMB.

Conozca cómo las políticas de firma afectan a la comunicación con servidores SMB de ONTAP

Además de la configuración de seguridad de firma SMB del servidor CIFS, dos políticas de firma SMB en clientes de Windows controlan la firma digital de las comunicaciones entre clientes y el servidor CIFS. Puede configurar el ajuste que cumpla con sus requisitos empresariales.

Las directivas SMB de cliente se controlan a través de la configuración de la directiva de seguridad local de Windows, que se configuran mediante Microsoft Management Console (MMC) o los GPO de Active Directory. Para obtener más información acerca de los problemas de firma SMB de cliente y de seguridad, consulte la documentación de Microsoft Windows.

A continuación, se muestran descripciones de las dos políticas de firma SMB en los clientes de Microsoft:

- `Microsoft network client: Digitally sign communications (if server agrees)`

  Esta configuración controla si la capacidad de firma SMB del cliente está habilitada. Está activado de forma predeterminada. Cuando se deshabilita esta configuración en el cliente, las comunicaciones del cliente con el servidor CIFS dependen de la configuración de firma SMB en el servidor CIFS.

- `Microsoft network client: Digitally sign communications (always)`

  Esta configuración controla si el cliente requiere la firma SMB para comunicarse con un servidor. Está desactivado de forma predeterminada. Cuando esta configuración está deshabilitada en el cliente, el comportamiento de la firma SMB se basa en la configuración de la política `Microsoft network client: Digitally sign communications (if server agrees)` y del servidor CIFS.

> ⓘ Si el entorno incluye clientes de Windows configurados para requerir la firma SMB, debe habilitar la firma SMB en el servidor CIFS. Si no lo hace, el servidor CIFS no puede proporcionar datos a estos sistemas.

Los resultados efectivos de la configuración de firma SMB del cliente y del servidor CIFS dependen de si las sesiones SMB utilizan SMB 1.0 o SMB 2.x y versiones posteriores.

En la tabla siguiente se resume el comportamiento efectivo de la firma SMB si la sesión utiliza SMB 1.0:

Cliente	No se requiere firma con ONTAP	Se requiere firma ONTAP
Firma desactivada y no requerida	No firmado	Firmado
Firma habilitada y no requerida	No firmado	Firmado
Firma desactivada y obligatoria	Firmado	Firmado
Firma habilitada y requerida	Firmado	Firmado

Es posible que los clientes Windows SMB 1 anteriores y algunos clientes SMB 1 distintos de Windows no puedan conectarse si la firma está deshabilitada en el cliente, pero es necesaria en el servidor CIFS.

En la tabla siguiente se resume el comportamiento efectivo de la firma SMB si la sesión utiliza SMB 2.x o SMB 3.0:

Para los clientes SMB 2.x y SMB 3.0, la firma SMB siempre está habilitada. No se puede deshabilitar.

Cliente	No se requiere firma con ONTAP	Se requiere firma ONTAP
No se requiere firma	No firmado	Firmado
Se requiere firma	Firmado	Firmado

En la tabla siguiente se resume el comportamiento de firma SMB de servidor y cliente de Microsoft predeterminado:

Protocolo	Algoritmo hash	Puede activar/desactivar	Se puede requerir o no se puede requerir	Valor predeterminado del cliente	Valor predeterminado del servidor	DC predeterminado
SMB 1,0	MD5	Sí	Sí	Habilitado (no es necesario)	Deshabilitado (no obligatorio)	Obligatorio
SMB 2.x	HMAC SHA-256	No	Sí	No es obligatorio	No es obligatorio	Obligatorio
SMB 3,0	AES-CMAC.	No	Sí	No es obligatorio	No es obligatorio	Obligatorio

Microsoft ya no recomienda utilizar `Digitally sign communications (if client agrees)` `Digitally sign communications (if server agrees)` la configuración de directiva de grupo o. Microsoft ya no recomienda utilizar `EnableSecuritySignature` la configuración del Registro. Estas opciones solo afectan al comportamiento de SMB 1 y se pueden reemplazar por la `Digitally sign communications (always)` configuración de directiva de grupo o la `RequireSecuritySignature` configuración del registro. También puede obtener más información en el blog de Microsoft.Conceptos básicos de The para la firma de SMB (cubriendo tanto SMB1 como SMB2)

Conozca el impacto en el rendimiento de la firma SMB de ONTAP

Cuando las sesiones SMB utilizan la firma SMB, todas las comunicaciones SMB a y desde clientes de Windows experimentan un impacto en el rendimiento, lo cual afecta tanto a los clientes como al servidor (es decir, los nodos del clúster que ejecuta la SVM que contiene el servidor SMB).

El impacto en el rendimiento muestra que el uso de CPU ha aumentado tanto en los clientes como en el servidor, aunque la cantidad de tráfico de red no cambia.

La magnitud del impacto en el rendimiento depende de la versión de ONTAP 9 que esté ejecutando. A partir de ONTAP 9.7, un nuevo algoritmo de descarga del cifrado puede permitir un mejor rendimiento en el tráfico de SMB firmado. La descarga de firma SMB se habilita de forma predeterminada cuando se habilita la firma SMB.

El rendimiento mejorado de la firma SMB requiere la funcionalidad de descarga de AES-ni. Consulte el Hardware Universe (HWU) para verificar que la descarga AES-ni es compatible con su plataforma.

Otras mejoras de rendimiento también son posibles si usted es capaz de utilizar SMB versión 3,11 que admite el algoritmo GCM mucho más rápido.

Según la red, la versión de ONTAP 9, la versión de SMB y la implementación de SVM, el impacto en el rendimiento de la firma SMB puede variar enormemente; puede verificarlo únicamente mediante pruebas en el entorno de red.

La mayoría de los clientes de Windows negocian la firma SMB de forma predeterminada si está habilitada en el servidor. Si necesita protección SMB para algunos de sus clientes Windows y la firma SMB está provocando problemas de rendimiento, puede deshabilitar la firma SMB en cualquiera de sus clientes Windows que no necesiten protección contra ataques de repetición. Para obtener información sobre cómo deshabilitar la firma SMB en clientes Windows, consulte la documentación de Microsoft Windows.

Recomendaciones de configuración de firma SMB de ONTAP

Puede configurar un comportamiento de firma SMB entre clientes SMB y el servidor CIFS para satisfacer sus requisitos de seguridad. La configuración que elija al configurar la firma SMB en el servidor CIFS depende de cuáles sean sus requisitos de seguridad.

Es posible configurar la firma SMB en el cliente o en el servidor CIFS. Tenga en cuenta las siguientes recomendaciones al configurar la firma SMB:

Si…	Recomendación…
Desea aumentar la seguridad de la comunicación entre el cliente y el servidor	Haga que se requiera la firma SMB en el cliente habilitando `Require Option (Sign always)` la configuración de seguridad en el cliente.
Es conveniente que todo el tráfico de SMB esté firmado a una determinada máquina virtual de almacenamiento (SVM)	Para requerir la firma SMB en el servidor CIFS, configure la configuración de seguridad para requerir la firma SMB.

Consulte la documentación de Microsoft para obtener más información acerca de la configuración de la seguridad del cliente de Windows.

Obtenga información sobre la configuración de firma SMB de ONTAP para varias LIFS de datos

Si habilita o deshabilita la firma SMB requerida en el servidor SMB, debe tener en cuenta las directrices para varias configuraciones de LIF de datos para una SVM.

Cuando configura un servidor SMB, puede haber varios LIF de datos configurados. Si es así, el servidor DNS contiene varias `A` entradas de registro para el servidor CIFS, todos utilizando el mismo nombre de host del

servidor SMB, pero cada uno con una dirección IP exclusiva. Por ejemplo, un servidor SMB que tiene dos LIF de datos configuradas puede tener las siguientes `A` entradas de registro DNS:

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

El comportamiento normal es que, al cambiar la configuración de firma SMB necesaria, solo las nuevas conexiones de clientes se ven afectadas por el cambio en la configuración de firma SMB. Sin embargo, hay una excepción a este comportamiento. Existe un caso en el que un cliente tiene una conexión existente con un recurso compartido y éste crea una nueva conexión con el mismo recurso compartido después de cambiar la configuración, manteniendo la conexión original. En este caso, tanto la conexión SMB nueva como la existente adoptan los nuevos requisitos de firma SMB.

Observe el siguiente ejemplo:

1. CLIENT1 se conecta a un recurso compartido sin necesidad de firma SMB mediante la ruta de acceso `O:\`.
2. El administrador de almacenamiento modifica la configuración del servidor SMB para requerir la firma SMB.
3. CLIENT1 se conecta al mismo recurso compartido con la firma SMB necesaria mediante la ruta de acceso `S:\` (manteniendo la conexión mediante la ruta `O:\`).
4. El resultado es que se utiliza la firma SMB cuando se accede a los datos `O:\` en `S:\` las unidades y.

Configure la firma ONTAP para el tráfico SMB entrante

Puede aplicar el requisito de que los clientes firmen mensajes SMB habilitando la firma SMB requerida. Si está habilitada, ONTAP solo acepta mensajes SMB si tienen firmas válidas. Si desea permitir la firma SMB, pero no la requiere, puede deshabilitar la firma SMB requerida.

Acerca de esta tarea

De manera predeterminada, la firma SMB requerida está deshabilitada. Es posible habilitar o deshabilitar la firma SMB requerida en cualquier momento.

> La firma SMB no está deshabilitada de forma predeterminada en las siguientes circunstancias:
>
> 1. La firma SMB necesaria está habilitada y el clúster se revierte a una versión de ONTAP que no admite la firma SMB.
> 2. Posteriormente, el clúster se actualiza a una versión de ONTAP que admite la firma SMB.
>
>   En estas circunstancias, la configuración de firma SMB configurada originalmente en una versión compatible de ONTAP se conserva mediante la reversión y la posterior actualización.

Cuando se configura una relación de recuperación ante desastres de una máquina virtual de almacenamiento (SVM), el valor que se selecciona para `-identity-preserve` la opción del `snapmirror create` comando determina los detalles de configuración que se replican en la SVM de destino.

Si establece `-identity-preserve` la opción en `true` (ID-preserve), la configuración de seguridad de firma SMB se replica en el destino.

Si establece `-identity-preserve` la opción en `false` (non-ID-preserve), la configuración de seguridad de firma SMB no se replica en el destino. En este caso, la configuración de seguridad del servidor CIFS en el destino se establece en los valores predeterminados. Si habilitó la firma SMB requerida en la SVM de origen, debe habilitar manualmente la firma SMB requerida en la SVM de destino.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea que la firma SMB sea…	Introduzca el comando…
Activado	`vserver cifs security modify -vserver vserver_name -is-signing-required true`
Deshabilitado	`vserver cifs security modify -vserver vserver_name -is-signing-required false`

2. Compruebe que la firma SMB necesaria esté habilitada o deshabilitada; para ello, determine si el valor del `Is Signing Required` campo de la salida del siguiente comando está establecido en el valor deseado: `vserver cifs security show -vserver vserver_name -fields is-signing-required`

Ejemplo

En el siguiente ejemplo, se habilita la firma SMB requerida para SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver  is-signing-required
-------- --------------------
vs1      true
```

Los cambios en la configuración de cifrado surten efecto para las nuevas conexiones. Las conexiones existentes no se ven afectadas.

Información relacionada

- "snapmirror create"

Determinar si las sesiones SMB de ONTAP están firmadas

Puede ver información sobre las sesiones SMB conectadas en el servidor CIFS. Puede usar esta información para determinar si las sesiones SMB están firmadas. Esto puede resultar útil para determinar si las sesiones de cliente SMB se conectan con la configuración de seguridad deseada.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea mostrar información acerca de…	Introduzca el comando…
Todas las sesiones firmados en una máquina virtual de almacenamiento (SVM) específica	`vserver cifs session show -vserver vserver_name -is-session-signed true`
Detalles de una sesión firmada con un ID de sesión específico en la SVM	`vserver cifs session show -vserver vserver_name -session-id integer -instance`

Ejemplos

El siguiente comando muestra información de sesión sobre las sesiones firmadas en la SVM vs1. El resultado de resumen predeterminado no muestra el campo de salida "'is Session Signed'":

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279 1       10.1.1.1         DOMAIN\joe          2          23s
```

El siguiente comando muestra información detallada de sesión, incluido si la sesión está firmada, en una sesión SMB con un ID de sesión de 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

Información relacionada

Supervisar estadísticas de sesión firmada por SMB

Supervisar las estadísticas de sesión firmadas por SMB de ONTAP

Es posible supervisar las estadísticas de sesiones SMB y determinar qué sesiones establecidas se han firmado y cuáles no.

Acerca de esta tarea

`statistics`El comando en el nivel de privilegio avanzado proporciona `signed_sessions` el contador que se puede utilizar para supervisar el número de sesiones SMB firmadas. El `signed_sessions` contador está disponible con los siguientes objetos de estadísticas:

- `cifs` Permite supervisar la firma SMB para todas las sesiones de SMB.
- `smb1` Permite supervisar la firma SMB para sesiones SMB 1,0.
- `smb2` Permite supervisar la firma SMB para sesiones SMB 2.x y SMB 3,0.

  Las estadísticas de SMB 3,0 se incluyen en la salida del `smb2` objeto.

Si desea comparar el Núm. De sesiones firmadas con el Núm. Total de sesiones, puede comparar la salida del `signed_sessions` contador con la salida del `established_sessions` contador.

Debe iniciar una colección de ejemplos de estadísticas para poder ver los datos resultantes. Puede ver los datos de la muestra si no detiene la recopilación de datos. Al detener la recopilación de datos, se proporciona una muestra fija. No detener la recopilación de datos le ofrece la posibilidad de obtener datos actualizados que puede utilizar para compararlos con consultas anteriores. La comparación puede ayudarle a identificar tendencias.

Pasos

1. Establezca el nivel de privilegio en AVANZADO:
   `set -privilege advanced`
2. Iniciar una recopilación de datos:
   `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Si no se especifica `-sample-id` el parámetro, el comando genera un identificador de muestra para usted y define esta muestra como la muestra predeterminada de la sesión CLI. El valor para `-sample-id` es una cadena de texto. Si ejecuta este comando durante la misma sesión de la CLI y no se especifica `-sample-id` el parámetro, el comando sobrescribe la muestra predeterminada anterior.

   Opcionalmente, puede especificar el nodo en el que se desea recoger estadísticas. Si no especifica el nodo, la muestra recopila estadísticas para todos los nodos del clúster.

   Obtenga más información sobre `statistics start` en el "Referencia de comandos del ONTAP".
3. Utilice `statistics stop` el comando para detener la recogida de datos para la muestra.

   Obtenga más información sobre `statistics stop` en el "Referencia de comandos del ONTAP" .
4. Ver estadísticas de firma SMB:

Si desea ver información acerca de…	**Introduzca…**
Sesiones firmadas	`show -sample-id sample_ID -counter signed_sessions
node_name [-node *node_name*]`	Sesiones firmadas y sesiones establecidas
`show -sample-id *sample_ID* -counter signed_sessions	established_sessions

   Si desea mostrar información de un solo nodo, especifique el `-node` parámetro opcional.

   Obtenga más información sobre `statistics show` en el "Referencia de comandos del ONTAP".
5. Vuelva al nivel de privilegio de administrador:
   `set -privilege admin`

Ejemplos

El siguiente ejemplo muestra cómo se pueden supervisar las estadísticas de firma de SMB 2.x y SMB 3.0 en vs1 de la máquina virtual de almacenamiento (SVM).

El siguiente comando cambia al nivel de privilegio avanzado:

```
cluster1::> set -privilege advanced

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

El siguiente comando inicia la recogida de datos de una nueva muestra:

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

El siguiente comando detiene la recogida de datos de la muestra:

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

El siguiente comando muestra sesiones SMB firmadas y sesiones SMB establecidas por nodo a partir de la muestra:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|established_sessions|node_name

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    established_sessions                                         0
    node_name                                                node1
    signed_sessions                                              0
    established_sessions                                         1
    node_name                                                node2
    signed_sessions                                              1
    established_sessions                                         0
    node_name                                                node3
    signed_sessions                                              0
    established_sessions                                         0
    node_name                                                node4
    signed_sessions                                              0
```

En el siguiente comando, se muestran las sesiones SMB firmadas para el nodo 2 en la muestra:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|node_name -node node2

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    node_name                                                node2
    signed_sessions                                              1
```

El siguiente comando vuelve a pasar al nivel de privilegios de administrador:

```
cluster1::*> set -privilege admin
```

Información relacionada

- Determinar si se han firmado las sesiones SMB
- "Información general sobre la gestión y el control del rendimiento"

Configurar el cifrado SMB necesario en servidores SMB para las transferencias de datos a través de SMB

Obtenga más información sobre el cifrado SMB de ONTAP

El cifrado SMB para las transferencias de datos a través de SMB es una mejora de seguridad que se puede habilitar o deshabilitar en servidores SMB. También puede configurar el valor de cifrado SMB deseado de forma compartida mediante una configuración de propiedad de recurso compartido.

De forma predeterminada, cuando crea un servidor SMB en la máquina virtual de almacenamiento (SVM), el cifrado SMB se deshabilita. Debe habilitarla para aprovechar la seguridad mejorada proporcionada por el cifrado SMB.

Para crear una sesión SMB cifrada, el cliente SMB debe admitir el cifrado SMB. Los clientes de Windows que empiezan con Windows Server 2012 y Windows 8 admiten el cifrado SMB.

El cifrado SMB en la SVM se controla mediante dos opciones de configuración:

- Una opción de seguridad del servidor SMB que habilita la funcionalidad en la SVM
- Una propiedad de recurso compartido SMB que configura la configuración de cifrado SMB de recurso compartido

Puede decidir si se requiere el cifrado para acceder a todos los datos en la SVM o si se requiere el cifrado SMB para acceder solo a los datos en recursos compartidos seleccionados. La configuración a nivel de SVM tiene preferencia en la configuración a nivel de recurso compartido.

La configuración efectiva del cifrado SMB depende de la combinación de las dos opciones y se describe en la siguiente tabla:

Cifrado SMB Server habilitado	Configuración de cifrado compartido de datos activada	Comportamiento de cifrado del servidor
Verdadero	Falso	El cifrado a nivel de servidor está habilitado para todos los recursos compartidos de la SVM. Con esta configuración, se produce el cifrado en toda la sesión SMB.
Verdadero	Verdadero	El cifrado a nivel de servidor se habilita para todos los recursos compartidos de la SVM, independientemente del cifrado a nivel de recurso compartido. Con esta configuración, se produce el cifrado en toda la sesión SMB.

Cifrado SMB Server habilitado	Configuración de cifrado compartido de datos activada	Comportamiento de cifrado del servidor
Falso	Verdadero	El cifrado a nivel de recurso compartido está habilitado para los recursos compartidos específicos. Con esta configuración, el cifrado se produce desde la conexión de árbol.
Falso	Falso	No hay ningún cifrado activado.

Los clientes SMB que no admiten cifrado no pueden conectarse a un servidor SMB o recurso compartido que requiera cifrado.

Los cambios en la configuración de cifrado surten efecto para las nuevas conexiones. Las conexiones existentes no se ven afectadas.

Obtenga información sobre el impacto en el rendimiento del cifrado de bloques de mensajes del servidor de ONTAP

Cuando las sesiones SMB utilizan el cifrado SMB, todas las comunicaciones SMB a y desde clientes de Windows experimentan un impacto en el rendimiento, lo cual afecta tanto a los clientes como al servidor (es decir, los nodos del clúster que ejecuta la SVM que contiene el servidor SMB).

El impacto en el rendimiento muestra que el uso de CPU ha aumentado tanto en los clientes como en el servidor, aunque la cantidad de tráfico de red no cambia.

La magnitud del impacto en el rendimiento depende de la versión de ONTAP 9 que esté ejecutando. A partir de ONTAP 9.7, un nuevo algoritmo de descarga del cifrado puede permitir un mejor rendimiento en el tráfico SMB cifrado. La descarga de cifrado SMB se habilita de forma predeterminada cuando se habilita el cifrado SMB.

El rendimiento del cifrado SMB mejorado requiere la capacidad de descarga de AES-ni. Consulte el Hardware Universe (HWU) para verificar que la descarga AES-ni es compatible con su plataforma.

Otras mejoras de rendimiento también son posibles si usted es capaz de utilizar SMB versión 3,11 que admite el algoritmo GCM mucho más rápido.

Según la red, la versión de ONTAP 9, la versión de SMB y la implementación de SVM, el impacto en el rendimiento del cifrado SMB puede variar enormemente; puede verificarlo únicamente mediante pruebas en su entorno de red.

El cifrado SMB está deshabilitado de forma predeterminada en el servidor SMB. Debe habilitar el cifrado SMB solo en aquellos recursos compartidos SMB o servidores SMB que requieran cifrado. Con el cifrado SMB, ONTAP realiza un procesamiento adicional de descifrar las solicitudes y cifrar las respuestas para cada solicitud. Por tanto, el cifrado SMB solo debe habilitarse cuando sea necesario.

Habilite o deshabilite el cifrado SMB de ONTAP para el tráfico entrante

Si desea requerir el cifrado SMB para el tráfico SMB entrante puede habilitarla en el servidor CIFS o en el nivel de recurso compartido. De manera predeterminada, no es

necesario el cifrado SMB.

Acerca de esta tarea

Puede habilitar el cifrado SMB en el servidor CIFS, que se aplica a todos los recursos compartidos del servidor CIFS. Si no desea usar el cifrado SMB necesario para todos los recursos compartidos en el servidor CIFS o si desea habilitar el cifrado SMB necesario para el tráfico SMB entrante de acuerdo con recurso compartido por recurso, puede deshabilitar el cifrado SMB requerido en el servidor CIFS.

Cuando se configura una relación de recuperación ante desastres de una máquina virtual de almacenamiento (SVM), el valor que selecciona para `-identity-preserve` la opción del `snapmirror create` comando determina los detalles de configuración que se replican en la SVM de destino.

Si establece `-identity-preserve` la opción en `true` (ID-preserve), la configuración de seguridad de cifrado SMB se replica en el destino.

Si establece `-identity-preserve` la opción en `false` (non-ID-preserve), la configuración de seguridad de cifrado SMB no se replica en el destino. En este caso, la configuración de seguridad del servidor CIFS en el destino se establece en los valores predeterminados. Si ha habilitado el cifrado SMB en la SVM de origen, debe habilitar manualmente el cifrado SMB del servidor CIFS en el destino.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea que el cifrado SMB para el tráfico SMB entrante en el servidor CIFS sea…	Introduzca el comando…
Activado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required true`
Deshabilitado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required false`

2. Compruebe que el cifrado SMB necesario en el servidor CIFS está habilitado o deshabilitado como desee: `vserver cifs security show -vserver` *`vserver_name`* `-fields is-smb-encryption-required`

   `is-smb-encryption-required`El campo muestra `true` si el cifrado SMB necesario está habilitado en el servidor CIFS y `false` si está deshabilitado.

Ejemplo

En el ejemplo siguiente se habilita el cifrado SMB requerido para el tráfico SMB entrante para el servidor CIFS en la SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

Información relacionada

- "snapmirror create"

Determine si los clientes están conectados mediante sesiones SMB de ONTAP cifradas

Puede mostrar información sobre las sesiones SMB conectadas para determinar si los clientes están utilizando conexiones SMB cifradas. Esto puede resultar útil para determinar si las sesiones de cliente SMB se conectan con la configuración de seguridad deseada.

Acerca de esta tarea

Las sesiones de clientes de SMB pueden tener uno de tres niveles de cifrado:

- `unencrypted`

  La sesión SMB no está cifrada. No se configura ni el cifrado a nivel de equipo virtual de almacenamiento (SVM) ni el nivel de recurso compartido.

- `partially-encrypted`

  El cifrado se inicia cuando se produce la conexión de árbol. Se configuró el cifrado a nivel de recurso compartido. El cifrado a nivel de SVM no está habilitado.

- `encrypted`

  La sesión SMB está totalmente cifrada. El cifrado de la SVM está habilitado. Es posible que el cifrado de nivel de recurso compartido esté habilitado o no. La configuración de cifrado a nivel de SVM sustituye la configuración de cifrado a nivel de recurso compartido.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea mostrar información acerca de…	Introduzca el comando…
Sesiones con una configuración de cifrado especificada para sesiones en una SVM especificada	`vserver cifs session show -vserver *vserver_name* {unencrypted
partially-encrypted	encrypted} -instance`

Si desea mostrar información acerca de…	Introduzca el comando…
La configuración de cifrado para un ID de sesión específico en una SVM especificada	`vserver cifs session show -vserver` *`vserver_name`* `-session-id` *`integer`* `-instance`

Ejemplos

El siguiente comando muestra información detallada de la sesión, incluida la configuración de cifrado, en una sesión SMB con un ID de sesión de 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                Open Shares: 1
                 Open Files: 1
                 Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

Supervise las estadísticas de cifrado del bloque de mensajes del servidor de ONTAP

Es posible supervisar las estadísticas de cifrado SMB y determinar qué sesiones establecidas y conexiones de uso compartido están cifradas y cuáles no lo están.

Acerca de esta tarea

`statistics`El comando en el nivel de privilegios avanzados proporciona los siguientes contadores, que puede utilizar para supervisar el número de sesiones SMB cifradas y conexiones compartidas:

Nombre del contador	Descripciones
`encrypted_sessions`	Proporciona el número de sesiones cifradas SMB 3.0
`encrypted_share_connections`	Proporciona el número de recursos compartidos cifrados en los que se ha producido una conexión de árbol
`rejected_unencrypted_sessions`	Da el número de configuraciones de sesión rechazadas debido a la falta de capacidad de cifrado del cliente
`rejected_unencrypted_shares`	Proporciona el número de asignaciones de recursos compartidos rechazadas debido a la falta de capacidad de cifrado del cliente

Estos contadores están disponibles con los siguientes objetos de estadísticas:

- `cifs` Permite supervisar el cifrado SMB para todas las sesiones de SMB 3,0.

  Las estadísticas de SMB 3,0 se incluyen en la salida del `cifs` objeto. Si desea comparar el Núm. De sesiones cifradas con el Núm. Total de sesiones, puede comparar la salida del `encrypted_sessions` contador con la salida del `established_sessions` contador.

  Si desea comparar el número de conexiones compartidas cifradas con el número total de conexiones compartidas, puede comparar la salida del `encrypted_share_connections` contador con la salida del contador `connected_shares`.

- `rejected_unencrypted_sessions` Proporciona la cantidad de veces que se ha intentado establecer una sesión SMB que requiere cifrado de un cliente que no admite cifrado SMB.
- `rejected_unencrypted_shares` Proporciona la cantidad de veces que se ha intentado conectarse a un recurso compartido SMB que requiere cifrado de un cliente que no admite cifrado SMB.

Debe iniciar una colección de ejemplos de estadísticas para poder ver los datos resultantes. Puede ver los datos de la muestra si no detiene la recopilación de datos. Al detener la recopilación de datos, se proporciona una muestra fija. No detener la recopilación de datos le ofrece la posibilidad de obtener datos actualizados que puede utilizar para compararlos con consultas anteriores. La comparación puede ayudarle a identificar tendencias.

Pasos

1. Establezca el nivel de privilegio en AVANZADO:
   `set -privilege advanced`
2. Iniciar una recopilación de datos:
   `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Si no se especifica `-sample-id` el parámetro, el comando genera un identificador de muestra para usted y define esta muestra como la muestra predeterminada de la sesión CLI. El valor para `-sample-id` es una cadena de texto. Si ejecuta este comando durante la misma sesión de la CLI y no se especifica `-sample-id` el parámetro, el comando sobrescribe la muestra predeterminada anterior.

Opcionalmente, puede especificar el nodo en el que se desea recoger estadísticas. Si no especifica el nodo, la muestra recopila estadísticas para todos los nodos del clúster.

Obtenga más información sobre `statistics start` en el "Referencia de comandos del ONTAP".

3. Utilice `statistics stop` el comando para detener la recogida de datos para la muestra.

   Obtenga más información sobre `statistics stop` en el "Referencia de comandos del ONTAP" .

4. Ver estadísticas de cifrado SMB:

Si desea ver información acerca de…	**Introduzca…**
Sesiones cifradas	`show -sample-id *sample_ID* -counter encrypted_sessions
node_name [-node *node_name*]`	Sesiones cifradas y sesiones establecidas
`show -sample-id *sample_ID* -counter encrypted_sessions	established_sessions
node_name [-node *node_name*]`	Conexiones de recursos compartidos cifradas
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`
Conexiones de recursos compartidos cifradas y recursos compartidos conectados	`show -sample-id *sample_ID* -counter encrypted_share_connections
connected_shares	*node_name* [-node *node_name*]`
Sesiones no cifradas rechazadas	`show -sample-id *sample_ID* -counter rejected_unencrypted_sessions
node_name [-node *node_name*]`	Se han rechazado conexiones compartidas sin cifrar
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

   Si desea mostrar información solo de un solo nodo, especifique el `-node` parámetro opcional.

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

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

Ejemplos

El ejemplo siguiente muestra cómo se pueden supervisar las estadísticas de cifrado de SMB 3.0 en vs1 de la máquina virtual de almacenamiento (SVM).

El siguiente comando cambia al nivel de privilegio avanzado:

```
cluster1::> set -privilege advanced

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

El siguiente comando inicia la recogida de datos de una nueva muestra:

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

El siguiente comando detiene la recogida de datos de esa muestra:

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

El siguiente comando muestra sesiones SMB cifradas y sesiones SMB establecidas por el nodo a partir de la muestra:

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2

    Counter                                 Value
    --------------------------  ----------------------
    established_sessions                       1
    encrypted_sessions                         1

2 entries were displayed
```

El siguiente comando muestra el número de sesiones SMB no cifradas rechazadas por el nodo a partir de la muestra:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2

    Counter                                     Value
    --------------------------    ----------------------
    rejected_unencrypted_sessions                 1

1 entry was displayed.
```

El siguiente comando muestra el número de recursos compartidos de SMB conectados y recursos compartidos de SMB cifrados mediante el nodo de la muestra:

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

    Counter                                     Value
    --------------------------    ----------------------
    connected_shares                              2
    encrypted_share_connections                   1

2 entries were displayed.
```

El siguiente comando muestra el número de conexiones de recursos compartidos SMB no cifradas rechazadas por el nodo a partir de la muestra:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

    Counter                                     Value
    -------------------------------    ----------------------
    rejected_unencrypted_shares                   1

1 entry was displayed.
```

Información relacionada

- Determinar qué estadísticas, objetos y contadores están disponibles en los servidores
- "Información general sobre la gestión y el control del rendimiento"

Comunicación segura de sesiones LDAP

Obtenga más información sobre la firma y el sellado LDAP en el bloque de mensajes del servidor ONTAP

A partir de ONTAP 9, puede configurar la firma y el sellado para habilitar la seguridad de la sesión LDAP en consultas a un servidor de Active Directory (AD). Debe configurar los

ajustes de seguridad del servidor CIFS en la máquina virtual de almacenamiento (SVM) para corresponder a los del servidor LDAP.

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

La firma y el sellado LDAP en el tráfico CIFS están habilitados en la SVM con `-session-security-for-ad-ldap` la opción para `vserver cifs security modify` el comando.

Habilite la firma y el sellado LDAP en los servidores SMB de ONTAP

Antes de que el servidor CIFS pueda utilizar la firma y el sellado para establecer una comunicación segura con un servidor LDAP de Active Directory, debe modificar la configuración de seguridad del servidor CIFS para habilitar la firma y el sellado LDAP.

Antes de empezar

Debe consultar al administrador del servidor AD para determinar los valores de configuración de seguridad adecuados.

Pasos

1. Configure las opciones de seguridad del servidor CIFS que permitan el tráfico firmado y sellado con servidores LDAP de Active Directory: `vserver cifs security modify -vserver` *`vserver_name`* `-session-security-for-ad-ldap {none|sign|seal}`

   Puede activar la firma (`sign`, integridad de datos), la firma y el sellado (`seal`, la integridad y el cifrado de los datos), o ninguno `none`, sin firma ni sellado). El valor predeterminado es `none`.

2. Compruebe que la configuración de seguridad de firma y sellado LDAP se ha definido correctamente: `vserver cifs security show -vserver` *`vserver_name`*

> Si la SVM utiliza el mismo servidor LDAP para consultar la asignación de nombres u otra información de UNIX, como usuarios, grupos y netgroups, debe habilitar la configuración correspondiente con `-session-security` la opción `vserver services name-service ldap client modify` del comando.

Configure LDAP sobre TLS

Exporte certificados de CA raíz autofirmados para las SVM SMB de ONTAP

Para utilizar LDAP sobre SSL/TLS para proteger la comunicación de Active Directory, primero debe exportar una copia del certificado raíz autofirmado del Servicio de certificados de Active Directory a un archivo de certificado y convertirlo en un archivo de texto ASCII. ONTAP utiliza este archivo de texto para instalar el certificado en la máquina virtual de almacenamiento (SVM).

Antes de empezar

El servicio de certificados de Active Directory ya debe estar instalado y configurado para el dominio al que pertenece el servidor CIFS. Puede encontrar información acerca de la instalación y configuración de Active

Director Certificate Services consultando la biblioteca de Microsoft TechNet.

"Biblioteca de Microsoft TechNet: technet.microsoft.com"

Paso

1. Obtenga un certificado de CA raíz del controlador de dominio en `.pem` formato de texto.

   "Biblioteca de Microsoft TechNet: technet.microsoft.com"

Después de terminar

Instale el certificado en la SVM.

Información relacionada

"Biblioteca de Microsoft TechNet"

Instale los certificados de CA raíz autofirmados en la SVM SMB de ONTAP

Si se requiere la autenticación LDAP con TLS al enlazar con servidores LDAP, primero debe instalar el certificado de CA raíz autofirmado en la SVM.

Acerca de esta tarea

Todas las aplicaciones de ONTAP que utilizan comunicaciones TLS pueden comprobar el estado del certificado digital mediante el protocolo de estado de certificado en línea (OCSP). Si OCSP está habilitado para LDAP over TLS, se rechazan los certificados revocados y la conexión falla.

Pasos

1. Instale el certificado de CA raíz autofirmado:
   a. Comience la instalación del certificado: `security certificate install -vserver vserver_name -type server-ca`

      La salida de la consola muestra el siguiente mensaje: `Please enter Certificate: Press <Enter> when done`

   b. Abra el `.pem` archivo de certificado con un editor de texto, copie el certificado, incluidas las líneas que empiezan por `-----BEGIN CERTIFICATE-----` y terminan por y `-----END CERTIFICATE-----`, a continuación, pegue el certificado después del símbolo del sistema.
   c. Compruebe que el certificado se muestra correctamente.
   d. Para completar la instalación, pulse Intro.
2. Compruebe que el certificado está instalado: `security certificate show -vserver vserver_name`

Información relacionada

- "instalación del certificado de seguridad"
- "Mostrar certificado de seguridad"

Habilite LDAP over TLS en el servidor SMB de ONTAP

Antes de que el servidor SMB pueda utilizar TLS para obtener comunicación segura con un servidor LDAP de Active Directory, debe modificar la configuración de seguridad del

servidor SMB para habilitar LDAP over TLS.

A partir de ONTAP 9.10.1, el enlace de canal LDAP se admite de forma predeterminada tanto para las conexiones LDAP de Active Directory (AD) como de los servicios de nombres. ONTAP intentará establecer la vinculación de canal con las conexiones LDAP solo si Start-TLS o LDAPS está habilitado junto con la seguridad de la sesión establecida en Sign o Seal. Para deshabilitar o volver a habilitar el enlace de canal LDAP con los servidores AD, utilice `-try-channel-binding-for-ad-ldap` el parámetro con `vserver cifs security modify` el comando.

Para obtener más información, consulte:

- "Obtenga más información sobre LDAP para SVM NFS de ONTAP"
- "2020 requisitos de enlace de canal LDAP y firma LDAP para Windows".

Pasos

1. Configure los ajustes de seguridad del servidor SMB que permitan una comunicación LDAP segura con los servidores LDAP de Active Directory: `vserver cifs security modify -vserver` *`vserver_name`* `-use-start-tls-for-ad-ldap true`
2. Compruebe que la configuración de seguridad LDAP over TLS está establecida en `true`: `vserver cifs security show -vserver` *`vserver_name`*

> Si la SVM utiliza el mismo servidor LDAP para consultar la asignación de nombres u otra información de UNIX (como usuarios, grupos y netgroups), también debe modificar la `-use-start-tls` opción mediante `vserver services name-service ldap client modify` el comando.

Configurar ONTAP SMB Multicanal para el rendimiento y la redundancia

A partir de ONTAP 9.4, puede configurar SMB MultiChannel para proporcionar varias conexiones entre ONTAP y clientes en una sola sesión SMB. Al hacerlo, se mejora el rendimiento y la tolerancia a fallos.

Antes de empezar

Solo se puede utilizar la funcionalidad multicanal de SMB cuando los clientes negocian en SMB 3.0 o versiones posteriores. De forma predeterminada, SMB 3.0 y las versiones posteriores se encuentran habilitadas en el servidor SMB de ONTAP.

Acerca de esta tarea

Los clientes de SMB detectan y utilizan automáticamente varias conexiones de red si se identifica una configuración adecuada en el clúster de ONTAP.

El número de conexiones simultáneas en una sesión SMB depende de las NIC que haya implementado:

- **1G NIC en el cluster ONTAP y cliente**

  El cliente establece una conexión por NIC y enlaza la sesión a todas las conexiones.

- **NIC 10G y mayor capacidad en cluster ONTAP** y cliente

  El cliente establece hasta cuatro conexiones por NIC y enlaza la sesión a todas las conexiones. El cliente puede establecer conexiones en varias NIC de 10 G y de mayor capacidad.

También puede modificar los siguientes parámetros (privilegios avanzados):

- `-max-connections-per-session`

  El número máximo de conexiones permitidas por sesión multicanal. El valor predeterminado es 32 conexiones.

  Si desea habilitar más conexiones que las predeterminadas, debe realizar ajustes comparables a la configuración del cliente, que también tiene un valor predeterminado de 32 conexiones.

- `-max-lifs-per-session`

  Número máximo de interfaces de red anunciadas por sesión multicanal. El valor predeterminado es 256 interfaces de red.

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Habilite multicanal de SMB en el servidor SMB:

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. Compruebe que ONTAP informa de sesiones multicanal de SMB:

```
vserver cifs session show
```

4. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Ejemplo

En el siguiente ejemplo, se muestra información sobre todas las sesiones SMB, donde se muestran varias conexiones para una sola sesión:

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User         Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

En el siguiente ejemplo, se muestra información detallada sobre una sesión SMB con el ID de sesión 1:

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                            Node: node1
                      Session ID: 1
                  Connection IDs: 138683,138684,138685
               Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                  Connected Time: 5s
                       Idle Time: 5s
               Protocol Version: SMB3
         Continuously Available: No
              Is Session Signed: false
                   NetBIOS Name: -
```

Configurar los mapas de usuario UNIX predeterminados de usuario de Windows en el servidor SMB

Configure el usuario UNIX SMB de ONTAP predeterminado

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

Acerca de esta tarea

De forma predeterminada, el nombre del usuario UNIX predeterminado es "'pcuser'", lo que significa que, de forma predeterminada, se activa la asignación de usuarios al usuario UNIX predeterminado. Puede especificar otro nombre que se utilizará como usuario UNIX predeterminado. El nombre que especifique debe existir en las bases de datos del servicio de nombres configuradas para la máquina virtual de almacenamiento (SVM). Si esta opción está establecida en una cadena nula, nadie puede acceder al servidor CIFS como usuario predeterminado de UNIX. Es decir, cada usuario debe tener una cuenta en la base de datos de contraseñas para poder acceder al servidor CIFS.

Para que un usuario pueda conectarse al servidor CIFS con la cuenta de usuario UNIX predeterminada, el usuario debe cumplir los siguientes requisitos previos:

- El usuario se autentica.
- El usuario se encuentra en la base de datos de usuarios Windows local del servidor CIFS, en el dominio principal del servidor CIFS o en un dominio de confianza (si las búsquedas de asignación de nombres multidominio están activadas en el servidor CIFS).
- El nombre de usuario no se asigna explícitamente a una cadena nula.

Pasos

1. Configure el usuario UNIX predeterminado:

Si desea …	Introduzca …
Utilizar el usuario UNIX predeterminado "'pcuser'"	`vserver cifs options modify -default -unix-user pcuser`
Utilice otra cuenta de usuario UNIX como usuario predeterminado	`vserver cifs options modify -default -unix-user` *`user_name`*
Desactive el usuario UNIX predeterminado	`vserver cifs options modify -default -unix-user ""`

```
vserver cifs options modify -default-unix-user pcuser
```

2. Compruebe que el usuario UNIX predeterminado está configurado correctamente: `vserver cifs options show -vserver` *`vserver_name`*

   En el siguiente ejemplo, tanto el usuario UNIX predeterminado como el usuario UNIX invitado en SVM vs1 están configurados para utilizar el usuario UNIX "'pcuser'":

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : pcuser
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

Configure el usuario UNIX SMB de ONTAP invitado

Configurar la opción de usuario UNIX invitado significa que los usuarios que inician sesión desde dominios que no son de confianza se asignan al usuario UNIX invitado y pueden conectarse al servidor CIFS. Como alternativa, si desea que la autenticación de usuarios de dominios que no son de confianza falle, no debe configurar el usuario UNIX invitado. El valor predeterminado es no permitir que los usuarios de dominios que no son de confianza se conecten al servidor CIFS (la cuenta UNIX invitada no está configurada).

Acerca de esta tarea

Debe tener en cuenta lo siguiente al configurar la cuenta de UNIX de invitado:

- Si el servidor CIFS no puede autenticar al usuario en un controlador de dominio para el dominio principal, un dominio de confianza o la base de datos local y esta opción está habilitada, el servidor CIFS considera al usuario como un usuario invitado y lo asigna al usuario UNIX especificado.
- Si esta opción se establece en una cadena nula, el usuario UNIX invitado estará deshabilitado.
- Debe crear un usuario UNIX para usarlo como usuario UNIX invitado en una de las bases de datos del servicio de nombres de máquina virtual de almacenamiento (SVM).
- Un usuario que inició sesión como usuario invitado es automáticamente miembro del grupo BUILTIN\guest en el servidor CIFS.
- La opción 'homedrs-public' se aplica sólo a los usuarios autenticados. Un usuario que ha iniciado sesión como usuario invitado no tiene un directorio principal y no puede acceder a los directorios principales de otros usuarios.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca…
Configure el usuario UNIX invitado	`vserver cifs options modify -guest -unix-user` *`unix_name`*
Deshabilite el usuario UNIX invitado	`vserver cifs options modify -guest -unix-user ""`

```
vserver cifs options modify -guest-unix-user pcuser
```

2. Compruebe que el usuario UNIX invitado está configurado correctamente: `vserver cifs options show -vserver vserver_name`

   En el siguiente ejemplo, tanto el usuario UNIX predeterminado como el usuario UNIX invitado en SVM vs1 están configurados para utilizar el usuario UNIX "'pcuser'":

   ```
   vserver cifs options show -vserver vs1
   ```

   ```
   Vserver: vs1

     Client Session Timeout : 900
     Default Unix Group     : -
     Default Unix User      : pcuser
     Guest Unix User        : pcuser
     Read Grants Exec       : disabled
     Read Only Delete       : disabled
     WINS Servers           : -
   ```

Asigne los grupos de administrador a la raíz de SMB de ONTAP

Si solo tiene clientes CIFS en su entorno y su máquina virtual de almacenamiento (SVM) está configurada como un sistema de almacenamiento multiprotocolo, debe tener al menos una cuenta de Windows con privilegios raíz para acceder a los archivos en la SVM; De lo contrario, no puede gestionar la SVM porque no tiene suficientes derechos de usuario.

Acerca de esta tarea

Si el sistema de almacenamiento se configuró como solo NTFS, `/etc` el directorio tiene una ACL en el nivel de archivos que permite que el grupo de administradores acceda a los archivos de configuración de ONTAP.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Configure la opción del servidor CIFS que asigna el grupo de administradores a la raíz, según corresponda:

Si desea…	Realice lo siguiente…
Asigne los miembros del grupo de administradores a la raíz	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled true` Todas las cuentas del grupo de administradores se consideran raíz, incluso si no tiene una `/etc/usermap.cfg` entrada que asigne las cuentas a raíz. Si crea un archivo utilizando una cuenta que pertenece al grupo de administradores, el archivo es propiedad de root cuando ve el archivo desde un cliente UNIX.
Desactive la asignación de los miembros del grupo de administradores a la raíz	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled false` Las cuentas del grupo de administradores ya no se asignan a raíz. Sólo se puede asignar explícitamente un solo usuario a la raíz.

3. Compruebe que la opción está establecida en el valor deseado: `vserver cifs options show -vserver` *`vserver_name`*
4. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Mostrar información sobre los tipos de usuarios que están conectados en sesiones SMB de ONTAP

Puede ver información acerca del tipo de usuarios que están conectados en sesiones SMB. Esto puede ayudarle a asegurarse de que solo el tipo adecuado de usuario se conecte a través de sesiones SMB en la máquina virtual de almacenamiento (SVM).

Acerca de esta tarea

Los siguientes tipos de usuarios pueden conectarse a través de sesiones SMB:

- `local-user`

  Se autentica como usuario CIFS local

- `domain-user`

  Autenticado como usuario de dominio (ya sea desde el dominio principal del servidor CIFS o desde un dominio de confianza)

- `guest-user`

  Autenticado como usuario invitado

- `anonymous-user`

  Autenticado como usuario anónimo o nulo

Pasos

1. Determine qué tipo de usuario está conectado en una sesión SMB: `vserver cifs session show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type`

Si desea mostrar información sobre tipos de usuario para las sesiones establecidas…	Introduzca el siguiente comando…
Para todas las sesiones con un tipo de usuario especificado	`vserver cifs session show -vserver *vserver_name* -user-type {local-user
domain-user	guest-user
anonymous-user}`	Para un usuario específico

Ejemplos

El siguiente comando muestra información de sesión sobre el tipo de usuario para las sesiones en SVM vs1 establecidas por el usuario "' iepubs\user1"':

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node      vserver session-id connection-id lif-address  address
windows-user         user-type
--------- ------- ---------- ------------ ------------ -------------
-------------------- -----------
pub1node1 pub1    1          3439441860    10.0.0.1     10.1.1.1
IEPUBS\user1         domain-user
```

Opciones de comando de ONTAP para limitar el consumo excesivo de recursos de cliente de Windows

Las opciones que incluyen `vserver cifs options modify` el comando le permiten controlar el consumo de recursos de los clientes de Windows. Esto puede ser útil si algún cliente está fuera de los límites normales del consumo de recursos, por ejemplo, si hay un número inusualmente alto de archivos abiertos, sesiones abiertas o peticiones de notificación de cambio.

```
`vserver cifs options modify`Se han agregado las siguientes opciones al
comando para controlar el consumo de recursos del cliente de Windows. Si
se supera el valor máximo de cualquiera de estas opciones, se deniega la
solicitud y se envía un mensaje EMS. También se envía un mensaje de
advertencia EMS cuando se alcanza el 80 % del límite configurado para
estas opciones.
```

- `-max-opens-same-file-per-tree`

Número máximo de apertura en el mismo archivo por árbol CIFS

- `-max-same-user-sessions-per-connection`

  Número máximo de sesiones abiertas por el mismo usuario por conexión

- `-max-same-tree-connect-per-session`

  Número máximo de conexiones de árbol en el mismo recurso compartido por sesión

- `-max-watches-set-per-tree`

  Número máximo de relojes (también conocido como *change notifics*) establecido por árbol

Obtenga más información sobre `vserver cifs options modify` en el "Referencia de comandos del ONTAP".

A partir de ONTAP 9.4, los servidores que ejecutan SMB versión 2 o posterior pueden limitar el número de solicitudes pendientes (*créditos SMB*) que el cliente puede enviar al servidor en una conexión SMB. La gestión de créditos SMB es iniciada por el cliente y controlada por el servidor.

La `-max-credits` opción controla el número máximo de solicitudes pendientes que se pueden otorgar en una conexión SMB. El valor predeterminado de esta opción es 128.

Mejore el rendimiento del cliente con los bloqueos oportunistas tradicionales y de arrendamiento

Obtenga información sobre cómo mejorar el rendimiento del cliente de bloque de mensajes del servidor de ONTAP con los bloqueos oportunistas de arrendamiento tradicionales

Los bloqueos oportunistas tradicionales (bloqueos oportunistas oportunistas oportunistas) y los bloqueos oportunistas de arrendamiento habilitan un cliente SMB en determinados escenarios de uso compartido de archivos para realizar el almacenamiento en caché en el lado del cliente de información de lectura anticipada, escritura subyacente y bloqueo. A continuación, un cliente puede leer o escribir en un archivo sin recordar periódicamente al servidor que necesita acceso al archivo en cuestión. Esto mejora el rendimiento al reducir el tráfico de red.

Los bloqueos oportunistas del arrendamiento son una forma mejorada de bloqueos oportunistas disponibles con el protocolo SMB 2.1 y versiones posteriores. Los bloqueos oportunistas de arrendamiento permiten a un cliente obtener y conservar el estado de almacenamiento en caché del cliente en múltiples abiertos de SMB originados por sí mismo.

Los bloqueos oportunistas pueden controlarse de dos formas:

- Mediante una propiedad de recurso compartido, utilizando el `vserver cifs share create` comando cuando se crea el recurso compartido, o el `vserver share properties` comando después de la creación.
- Mediante una propiedad de qtree, el uso `volume qtree create` del comando cuando se crea el qtree, o `volume qtree oplock` los comandos después de su creación.

Obtenga más información sobre la escritura de consideraciones sobre pérdida de datos en la caché del bloque de mensajes del servidor de ONTAP cuando se utilizan bloqueos oportunistas

En determinadas circunstancias, si un proceso tiene un oplock exclusivo en un archivo y un segundo proceso intenta abrir el archivo, el primer proceso debe invalidar los datos almacenados en caché y vaciar las escrituras y los bloqueos. A continuación, el cliente debe renunciar al oplock y acceder al archivo. Si hay un fallo de red durante este vaciado, se pueden perder los datos de escritura en caché.

- Posibilidades de pérdida de datos

  Cualquier aplicación que tenga datos en la caché de la escritura puede perder esos datos en el siguiente conjunto de circunstancias:

  - La conexión se realiza mediante SMB 1.0.
  - Tiene un oplock exclusivo en el archivo.
  - Se le indica que rompa ese oplock o cierre el archivo.
  - Durante el proceso de vaciado de la caché de escritura, la red o el sistema de destino genera un error.
- Gestión de errores y finalización de escritura

  La caché en sí no tiene ninguna gestión de errores. Las aplicaciones sí. Cuando la aplicación escribe en la caché, la escritura siempre se completa. Si la caché, a su vez, realiza una escritura en el sistema de destino a través de una red, debe asumir que la escritura se completa porque, si no lo hace, los datos se pierden.

Habilite o deshabilite los bloqueos oportunistas al crear recursos compartidos de SMB de ONTAP

Los bloqueos oportunistas permiten a los clientes bloquear archivos y contenido de la caché localmente, lo que puede aumentar el rendimiento de las operaciones de archivos. Los bloqueos oportunistas están habilitados en los recursos compartidos de SMB que residen en máquinas virtuales de almacenamiento (SVM). En algunas circunstancias, es posible que desee deshabilitar los bloqueos oportunistas. Puede habilitar o deshabilitar los bloqueos oportunistas de acuerdo con el recurso compartido por recurso compartido.

Acerca de esta tarea

Si los bloqueos oportunistas están habilitados en el volumen que contiene un recurso compartido pero la propiedad de recurso compartido de oplock para ese recurso compartido está deshabilitada, los bloqueos oportunistas se deshabilitan para ese recurso compartido. La deshabilitación de los bloqueos oportunistas en un recurso compartido tiene prioridad sobre la configuración de oplock de volumen. Al deshabilitar los bloqueos oportunistas del recurso compartido, se deshabilitan los bloqueos oportunistas oportunistas de arrendamiento y oportunistas.

Puede especificar otras propiedades de recursos compartidos además de especificar la propiedad de recursos compartidos de oplock mediante una lista delimitada por comas. También puede especificar otros parámetros de recursos compartidos.

Pasos

1. Realice la acción correspondiente:

Si desea…	Realice lo siguiente…
Habilite los bloqueos oportunistas del recurso compartido durante la creación de recursos compartidos	Introduzca el siguiente comando: `vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]` Si desea que el recurso compartido tenga sólo las propiedades de recurso compartido por defecto, que son `oplocks` `browsable` , y `changenotify` están activadas, no es necesario especificar el `-share -properties` parámetro al crear un recurso compartido SMB. Si desea una combinación de propiedades de recurso compartido que no sea la predeterminada, debe especificar el `-share-properties` parámetro con la lista de propiedades de recurso compartido que se utilizará para ese recurso compartido.
Deshabilite los bloqueos oportunistas del recurso compartido durante la creación de recursos compartidos	Introduzca el siguiente comando: `vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]` Al desactivar los bloqueos oportunistas, debe especificar una lista de propiedades de recurso compartido al crear el recurso compartido, pero no debe especificar la `oplocks` propiedad.

Información relacionada

Habilite o deshabilite los bloqueos oportunistas en los recursos compartidos de SMB existentes

Controlar el estado del plock

Comandos de ONTAP para habilitar o deshabilitar los bloqueos oportunistas en volúmenes y qtrees de SMB

Los bloqueos oportunistas permiten a los clientes bloquear archivos y contenido de la caché localmente, lo que puede aumentar el rendimiento de las operaciones de archivos. Debe conocer los comandos para habilitar o deshabilitar los bloqueos oportunistas en volúmenes o qtrees. También debe saber cuándo puede habilitar o deshabilitar los

bloqueos oportunistas de los volúmenes y qtrees.

- Los bloqueos oportunistas están habilitados en los volúmenes de forma predeterminada.
- No se pueden deshabilitar los bloqueos oportunistas cuando crea un volumen.
- Puede habilitar o deshabilitar los bloqueos oportunistas de los volúmenes existentes de las SVM en cualquier momento.
- Puede habilitar los bloqueos oportunistas en qtrees para SVM.

  La configuración del modo oplock es una propiedad del ID de qtree 0, el qtree predeterminado que tienen todos los volúmenes. Si no se especifica una configuración de oplock al crear un qtree, el qtree hereda la configuración oplock del volumen principal, que se habilita de forma predeterminada. Sin embargo, si se especifica una configuración de oplock en el nuevo qtree, tendrá prioridad sobre la configuración de oplock en el volumen.

Si desea…	Se usa este comando…
Habilite los bloqueos oportunistas en volúmenes o qtrees	`volume qtree oplocks` con el `-oplock-mode` parámetro establecido en `enable`
Deshabilite los bloqueos oportunistas en volúmenes o qtrees	`volume qtree oplocks` con el `-oplock-mode` parámetro establecido en `disable`

Información relacionada

Controlar el estado del plock

Habilite o deshabilite los bloqueos oportunistas en recursos compartidos de SMB de ONTAP existentes

Los bloqueos oportunistas están habilitados en recursos compartidos de SMB en máquinas virtuales de almacenamiento (SVM) de forma predeterminada. En algunas circunstancias, puede que desee deshabilitar los bloqueos oportunistas; de forma alternativa, si ha deshabilitado los bloqueos oportunistas en un recurso compartido anteriormente, puede que desee volver a habilitar los bloqueos oportunistas.

Acerca de esta tarea

Si los bloqueos oportunistas están habilitados en el volumen que contiene un recurso compartido, pero la propiedad de recurso compartido oplock de ese recurso compartido está deshabilitada, los bloqueos oportunistas se deshabilitan para ese recurso compartido. La deshabilitación de los bloqueos oportunistas en un recurso compartido tiene prioridad sobre el hecho de habilitar los bloqueos oportunistas en el volumen. Al deshabilitar los bloqueos oportunistas del recurso compartido, se deshabilitan los bloqueos oportunistas oportunistas de arrendamiento y oportunistas. Puede habilitar o deshabilitar los bloqueos oportunistas de los recursos compartidos existentes en cualquier momento.

Paso

1. Realice la acción correspondiente:

Si desea…	Realice lo siguiente…
Habilite los bloqueos oportunistas del recurso compartido modificando un recurso compartido existente	Introduzca el siguiente comando: `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties oplocks` Puede especificar propiedades de recursos compartidos adicionales que desea agregar mediante una lista delimitada por comas. Las propiedades recién agregadas se agregan a la lista existente de propiedades de recursos compartidos. Todas las propiedades de recurso compartido que haya especificado anteriormente permanecen vigentes.
Deshabilite los bloqueos oportunistas de un recurso compartido modificando un recurso compartido existente	Introduzca el siguiente comando: `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties oplocks` Puede especificar propiedades de recursos compartidos adicionales que desea quitar mediante una lista delimitada por comas. Las propiedades de recursos compartidos que se quitan se eliminan de la lista existente de propiedades de recursos compartidos; sin embargo, las propiedades de recursos compartidos configuradas previamente que no se quitan permanecen vigentes.

Ejemplos

El siguiente comando habilita los bloqueos oportunistas del recurso compartido denominado «'Engineering» en la máquina virtual de almacenamiento (SVM, antes conocida como Vserver) vs1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      oplocks
                                  browsable
                                  changenotify
                                  showsnapshot
```

El siguiente comando deshabilita los bloqueos oportunistas del recurso compartido denominado "'Engineering'" en SVM vs1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      browsable
                                  changenotify
                                  showsnapshot
```

Información relacionada

- Habilite o deshabilite los bloqueos oportunistas al crear recursos compartidos de SMB
- Controlar el estado del plock
- Agregar o eliminar propiedades de recursos compartidos en recursos compartidos existentes

Supervise el estado de bloqueo oportunista del bloque de mensajes del servidor de ONTAP

Puede supervisar y mostrar información sobre el estado de los plock. Puede usar esta información para determinar qué archivos tienen bloqueos oportunistas, cuál son el nivel de plocock y el nivel de estado de plocock y si se utiliza el leasing de plocock. También puede determinar la información acerca de los bloqueos que podría necesitar interrumpir manualmente.

Acerca de esta tarea

Puede mostrar información acerca de todos los bloqueos oportunistas en un formulario de resumen o en un formulario de lista detallado. También puede utilizar parámetros opcionales para mostrar información sobre un subconjunto más pequeño de bloqueos existentes. Por ejemplo, puede especificar que la salida devuelva solo los bloqueos con la dirección IP del cliente especificada o con la ruta especificada.

Puede mostrar la siguiente información acerca de los bloqueos oportunistas tradicionales y de arrendamiento:

- SVM, nodo, volumen y LIF en los que se establece el oplock
- Bloquear UUID
- Dirección IP del cliente con el oplock
- Ruta en la que se establece el oplock
- Protocolo de bloqueo (SMB) y tipo (oplock)
- Estado de bloqueo
- Nivel de plock
- Estado de la conexión y tiempo de caducidad del bloque de mensajes del servidor
- Abra el código de grupo si se concede un seguro de arrendamiento

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

Pasos

1. Muestra el estado de bloqueo oportunista mediante `vserver locks show` el comando.

Ejemplos

El siguiente comando muestra información predeterminada sobre todos los bloqueos. El bloqueo oportunista del archivo mostrado se concede con un `read-batch` nivel de bloqueo oportunista:

```
cluster1::> vserver locks show

Vserver: vs0
Volume   Object Path        LIF         Protocol  Lock Type   Client
-------- ------------------ ----------- --------- ----------- ----------
vol1     /vol1/notes.txt    node1_data1
                                        cifs      share-level 192.168.1.5
         Sharelock Mode: read_write-deny_delete
                                                  op-lock     192.168.1.5
         Oplock Level: read-batch
```

El siguiente ejemplo muestra información más detallada sobre el bloqueo en un archivo con la ruta `/data2/data2_2/intro.pptx`. Se otorga un bloqueo oportunista de concesión en el archivo con un `batch` nivel de bloqueo oportunista a un cliente con una dirección IP `10.3.1.3` de :

> Al mostrar información detallada, el comando proporciona una salida independiente para la información de plock y sharelock. En este ejemplo sólo se muestra la salida de la sección de plock.

```
cluster1::> vserver lock 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: ff1cbf29-bfef-4d91-ae06-062bf69212c3
              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
```

Información relacionada

Habilite o deshabilite los bloqueos oportunistas al crear recursos compartidos de SMB

Habilite o deshabilite los bloqueos oportunistas en los recursos compartidos de SMB existentes

Comandos para habilitar o deshabilitar bloqueos operacionales en volúmenes SMB y qtrees

Aplicar objetos de directiva de grupo a servidores SMB

Obtenga información sobre la aplicación de objetos de directiva de grupo a servidores SMB de ONTAP

El servidor SMB admite objetos de directiva de grupo (GPO), un conjunto de reglas conocidas como atributos de directiva de grupo_ que se aplican a equipos de un entorno de Active Directory. Puede utilizar los GPO para gestionar de forma centralizada la configuración de todas las máquinas virtuales de almacenamiento (SVM) del clúster que pertenece al mismo dominio de Active Directory.

Cuando se habilitan los GPO en el servidor SMB, ONTAP envía consultas LDAP al servidor de Active

Directory que solicita información de GPO. Si hay definiciones de GPO aplicables al servidor SMB, el servidor Active Directory devuelve la siguiente información de GPO:

- Nombre de GPO
- Versión de GPO actual
- Ubicación de la definición de GPO
- Listas de UUID (identificadores universales únicos) para conjuntos de directivas de GPO

Información relacionada

- Obtenga más información sobre la seguridad del acceso a archivos para servidores
- "Seguimiento de seguridad y auditoría de SMB y NFS"

Obtenga más información sobre los GPO para SMB de ONTAP compatibles

Aunque no todos los objetos de políticas de grupo (GPO) se aplican a las máquinas virtuales de almacenamiento (SVM) habilitadas para CIFS, las SVM pueden reconocer y procesar el conjunto de objetos de normativa de grupo correspondiente.

Actualmente, los siguientes GPO son compatibles con las SVM:

- Ajustes de configuración de directivas de auditoría avanzadas:

  Acceso a objetos: Escalonamiento de la directiva de acceso central

  Especifica el tipo de eventos que se auditarán para la configuración provisional de la directiva de acceso central (CAP), incluida la siguiente configuración:

  - No auditar
  - Auditar solo los eventos de éxito
  - Auditar solo los eventos de fallo
  - Auditar eventos de éxito y fallo

  > Si se establece cualquiera de las tres opciones de auditoría (sólo eventos de éxito de auditoría, auditar sólo eventos de fallo, auditar eventos de éxito y de fallo), ONTAP audita tanto eventos de éxito como de fallo.

  Se establece mediante la `Audit Central Access Policy Staging` configuración de `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO.

  > Para utilizar las opciones de GPO de configuración de directivas de auditoría avanzadas, la auditoría debe configurarse en la SVM habilitada para CIFS a la que desee aplicar estas opciones. Si la auditoría no está configurada en la SVM, la configuración de GPO no se aplicará y se descarta.

- Configuración del registro:

  - Intervalo de actualización de la directiva de grupo para la SVM habilitada para CIFS

    Se establece mediante el `Registry` GPO.

- Actualización aleatoria de directivas de grupo

  Se establece mediante el `Registry` GPO.

- Publicación de hash para BranchCache

  El GPO Hash Publication para BranchCache corresponde al modo operativo de BranchCache. Se admiten los tres modos de funcionamiento compatibles siguientes:

  - Por recurso compartido
  - Todos los recursos compartidos
  - Se desactiva mediante `Registry` GPO.

- Compatibilidad de la versión de hash para BranchCache

  Se admiten las tres configuraciones de la siguiente versión de hash:

  - BranchCache versión 1
  - BranchCache versión 2
  - Las versiones 1 y 2 de BranchCache se establecen mediante `Registry` GPO.

> Para usar la configuración de GPO de BranchCache, BranchCache debe configurarse en la SVM habilitada para CIFS a la que desea aplicar esta configuración. Si no se configura BranchCache en la SVM, no se aplicará la configuración de GPO y se descarta.

- Configuración de seguridad
  - Política de auditoría y registro de eventos
    - Auditar eventos de inicio de sesión

      Especifica el tipo de eventos de inicio de sesión que se van a auditar, incluida la siguiente configuración:

      - No auditar
      - Auditar solo los eventos de éxito
      - Auditoría de eventos de fallo
      - Audite los eventos de éxito y fallo definidos mediante la `Audit logon events` configuración del `Local Policies/Audit Policy` GPO.

> Si se establece cualquiera de las tres opciones de auditoría (sólo eventos de éxito de auditoría, auditar sólo eventos de fallo, auditar eventos de éxito y de fallo), ONTAP audita tanto eventos de éxito como de fallo.

    - Auditar el acceso a objetos

      Especifica el tipo de acceso al objeto que se va a auditar, incluida la siguiente configuración:

      - No auditar
      - Auditar solo los eventos de éxito
      - Auditoría de eventos de fallo

- Audite los eventos de éxito y fallo definidos mediante la `Audit object access` configuración del `Local Policies/Audit Policy` GPO.

  Si se establece cualquiera de las tres opciones de auditoría (sólo eventos de éxito de auditoría, auditar sólo eventos de fallo, auditar eventos de éxito y de fallo), ONTAP audita tanto eventos de éxito como de fallo.

- Método de retención de registros

  Especifica el método de retención del registro de auditoría, incluida la siguiente configuración:

  - Sobrescribir el registro de eventos cuando el tamaño del archivo de registro supere el tamaño máximo del registro
  - No sobrescriba el registro de eventos (borrar registro manualmente) establecido mediante la `Retention method for security log` configuración del `Event Log` GPO.

- Tamaño máximo del registro

  Especifica el tamaño máximo del registro de auditoría.

  Se establece mediante la `Maximum security log size` configuración de `Event Log` GPO.

  Para utilizar la configuración de directiva de auditoría y GPO de registro de eventos, la auditoría debe configurarse en la SVM habilitada para CIFS a la que desea aplicar esta configuración. Si la auditoría no está configurada en la SVM, la configuración de GPO no se aplicará y se descarta.

◦ Seguridad del sistema de archivos

Especifica una lista de archivos o directorios en los que se aplica la seguridad de archivos a través de un GPO.

Se establece mediante el `File System` GPO.

Debe existir la ruta de acceso del volumen donde se configura el GPO de seguridad del sistema de archivos en la SVM.

◦ Política de Kerberos

- Desviación máxima del reloj

  Especifica la tolerancia máxima en minutos para la sincronización del reloj del equipo.

  Se establece mediante la `Maximum tolerance for computer clock synchronization` configuración de `Account Policies/Kerberos Policy` GPO.

- Antigüedad máxima del billete

  Especifica la duración máxima en horas para el ticket de usuario.

  Se establece mediante la `Maximum lifetime for user ticket` configuración de `Account Policies/Kerberos Policy` GPO.

- Antigüedad máxima de renovación del boleto

  Especifica la duración máxima en días para la renovación de la tarjeta de usuario.

Se establece mediante la `Maximum lifetime for user ticket renewal` configuración de `Account Policies/Kerberos Policy` GPO.

- Asignación de derechos de usuario (derechos de privilegio)
  - Asuma la propiedad

    Especifica la lista de usuarios y grupos que tienen derecho a asumir la propiedad de cualquier objeto asegurable.

    Se establece mediante la `Take ownership of files or other objects` configuración de `Local Policies/User Rights Assignment` GPO.

  - Privilegio de seguridad

    Especifica la lista de usuarios y grupos que pueden especificar opciones de auditoría para el acceso a objetos de recursos individuales, como archivos, carpetas y objetos de Active Directory.

    Se establece mediante la `Manage auditing and security log` configuración de `Local Policies/User Rights Assignment` GPO.

  - Cambiar privilegio de notificación (comprobación de recorrido de derivación)

    Especifica la lista de usuarios y grupos que pueden recorrer los árboles de directorios aunque los usuarios y los grupos puedan no tener permisos en el directorio de recorrido.

El mismo privilegio es necesario para que los usuarios reciban notificaciones de cambios en archivos y directorios. Se establece mediante la `Bypass traverse checking` configuración de `Local Policies/User Rights Assignment` GPO.

- Valores del Registro
  - Firma Configuración requerida

    Especifica si la firma SMB necesaria está habilitada o deshabilitada.

Se establece mediante la `Microsoft network server: Digitally sign communications (always)` configuración de `Security Options` GPO.

- Restringir anónimo

Especifica cuáles son las restricciones para los usuarios anónimos e incluye las tres configuraciones de GPO siguientes:

- No hay enumeración de cuentas del Administrador de cuentas de seguridad (SAM):

  Esta configuración de seguridad determina qué permisos adicionales se conceden para las conexiones anónimas al equipo. Esta opción se muestra como `no-enumeration` en ONTAP si está habilitada.

  Se establece mediante la `Network access: Do not allow anonymous enumeration of`

`SAM accounts` configuración de `Local Policies/Security Options` GPO.

- No hay enumeración de cuentas y recursos compartidos de SAM

  Esta configuración de seguridad determina si se permite la enumeración anónima de cuentas SAM y recursos compartidos. Esta opción se muestra como `no-enumeration` en ONTAP si está habilitada.

  Se establece mediante la `Network access: Do not allow anonymous enumeration of SAM accounts and shares` configuración de `Local Policies/Security Options` GPO.

- Restringir el acceso anónimo a recursos compartidos y canalizaciones con nombre

  Esta configuración de seguridad restringe el acceso anónimo a recursos compartidos y tuberías. Esta opción se muestra como `no-access` en ONTAP si está habilitada.

  Se establece mediante la `Network access: Restrict anonymous access to Named Pipes and Shares` configuración de `Local Policies/Security Options` GPO.

  Cuando se muestra información sobre las políticas de grupo definidas y aplicadas, el `Resultant restriction for anonymous user` campo de salida proporciona información sobre la restricción resultante de los tres valores de GPO anónimos de restricción. Las posibles restricciones resultantes son las siguientes:

° `no-access`

Al usuario anónimo se le deniega el acceso a los recursos compartidos especificados y a las canalizaciones con nombre, y no se puede utilizar la enumeración de cuentas y recursos compartidos SAM. Esta restricción resultante se ve si el `Network access: Restrict anonymous access to Named Pipes and Shares` GPO está habilitado.

° `no-enumeration`

El usuario anónimo tiene acceso a los recursos compartidos y canalizaciones con nombre especificados, pero no puede utilizar la enumeración de cuentas y recursos compartidos SAM. Esta restricción resultante se observa si se cumplen las dos condiciones siguientes:

- El `Network access: Restrict anonymous access to Named Pipes and Shares` GPO está desactivado.
- `Network access: Do not allow anonymous enumeration of SAM accounts`O los `Network access: Do not allow anonymous enumeration of SAM accounts and shares` objetos de normativa de grupo están activados.

° `no-restriction`

El usuario anónimo tiene acceso completo y puede utilizar la enumeración. Esta restricción resultante se observa si se cumplen las dos condiciones siguientes:

- El `Network access: Restrict anonymous access to Named Pipes and Shares` GPO está desactivado.
- Los `Network access: Do not allow anonymous enumeration of SAM accounts` `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPO y están desactivados.

- Grupos restringidos

  Puede configurar grupos restringidos para administrar de forma centralizada la pertenencia a grupos integrados o definidos por el usuario. Cuando aplica un grupo restringido a través de una directiva de grupo, la pertenencia a un grupo local de servidor CIFS se establece automáticamente para que coincida con la configuración de la lista de miembros definida en la directiva de grupo aplicada.

Se establece mediante el `Restricted Groups` GPO.

- Configuración de la directiva de acceso central

  Especifica una lista de directivas de acceso central. Las políticas de acceso central y las reglas de política de acceso central asociadas determinan los permisos de acceso para varios archivos en la SVM.

Información relacionada

- Habilitar o deshabilitar la compatibilidad con GPO en los servidores
- Obtenga más información sobre la seguridad del acceso a archivos para servidores
- "Seguimiento de seguridad y auditoría de SMB y NFS"
- Modificar la configuración de seguridad del servidor
- Obtenga información sobre cómo usar BranchCache para almacenar en caché contenido compartido en una sucursal
- Aprenda a utilizar la firma ONTAP para mejorar la seguridad de la red
- Obtenga información sobre cómo configurar la comprobación de recorrido de derivación
- Configurar restricciones de acceso para usuarios anónimos

Requisitos del servidor SMB de ONTAP para GPO

Para utilizar objetos de directiva de grupo (GPO) con el servidor SMB, el sistema debe cumplir varios requisitos.

- Las licencias de SMB deben estar en el clúster. La licencia SMB se incluye con "ONTAP One". Si no tiene ONTAP One y la licencia no está instalada, póngase en contacto con su representante de ventas.
- Debe haber un servidor SMB configurado y Unido a un dominio de Windows Active Directory.
- El estado del administrador del servidor SMB debe ser on.
- Los GPO deben configurarse y aplicarse a la unidad organizativa (OU) de Active Directory de Windows que contiene el objeto de equipo servidor SMB.
- La compatibilidad con GPO debe estar habilitada en el servidor SMB.

Habilitar o deshabilitar la compatibilidad de GPO en los servidores SMB de ONTAP

Puede habilitar o deshabilitar la compatibilidad con objetos de directiva de grupo (GPO) en un servidor CIFS. Si habilita la compatibilidad de GPO en un servidor CIFS, los GPO aplicables definidos en la directiva de grupo (la directiva que se aplica a la unidad organizativa (OU) que contiene el objeto de equipo del servidor CIFS) se aplican al servidor CIFS.

Acerca de esta tarea

Los GPO no pueden habilitarse en servidores CIFS en modo de grupo de trabajo.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el comando…
Habilite los GPO	`vserver cifs group-policy modify -vserver vserver_name -status enabled`
Deshabilitar GPO	`vserver cifs group-policy modify -vserver vserver_name -status disabled`

2. Compruebe que el soporte de GPO está en el estado deseado: `vserver cifs group-policy show -vserver +vserver_name_`

   El estado de la directiva de grupo de los servidores CIFS en el modo de grupo se muestra como "desactivado".

Ejemplo

En el siguiente ejemplo, se habilita la compatibilidad de GPO en máquinas virtuales de almacenamiento (SVM) vs1:

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

            Vserver: vs1
Group Policy Status: enabled
```

Información relacionada

Obtenga más información sobre los GPO compatibles

Requisitos del servidor para GPO

Obtenga información sobre cómo actualizar GPO en servidores SMB

Actualizar manualmente la configuración de GPO en servidores SMB

Mostrar información acerca de las configuraciones de GPO

Cómo se actualizan los GPO en el servidor SMB

Obtenga información sobre la actualización de GPO en servidores SMB de ONTAP

De forma predeterminada, ONTAP recupera y aplica los cambios de objeto de directiva de grupo (GPO) cada 90 minutos. La configuración de seguridad se actualiza cada 16

horas. Si desea actualizar GPO para aplicar nuevas configuraciones de directivas de GPO antes de que ONTAP las actualice automáticamente, puede activar una actualización manual en un servidor CIFS con un comando ONTAP.

- De forma predeterminada, todos los GPO se verifican y actualizan según sea necesario cada 90 minutos.

  Este intervalo se puede configurar y se puede ajustar mediante `Refresh interval` `Random offset` los ajustes de y GPO.

  ONTAP consulta a Active Directory los cambios realizados en los GPO. Si los números de versión de GPO registrados en Active Directory son superiores a los del servidor CIFS, ONTAP recupera y aplica los nuevos GPO. Si los números de versión son los mismos, los GPO en el servidor CIFS no se actualizan.

- Configuración de seguridad los GPO se actualizan cada 16 horas.

  ONTAP recupera y aplica los GPO de configuración de seguridad cada 16 horas, independientemente de que estos GPO hayan cambiado o no.

  > El valor predeterminado de 16 horas no se puede cambiar en la versión actual de ONTAP. Es una configuración predeterminada del cliente Windows.

- Todos los GPO se pueden actualizar manualmente con un comando ONTAP.

  Este comando simula el `gpupdate.exe` comando Windows/force`.

Información relacionada

Actualizar manualmente la configuración de GPO en servidores SMB

Actualice manualmente la configuración de GPO en los servidores SMB de ONTAP

Si desea actualizar inmediatamente la configuración del objeto de directiva de grupo (GPO) en el servidor CIFS, puede actualizar manualmente la configuración. Sólo puede actualizar los ajustes modificados o puede forzar una actualización para todos los ajustes, incluidos los que se aplicaron anteriormente pero no se han modificado.

Paso

1. Ejecute la acción adecuada:

Si desea actualizar…	Introduzca el comando…
Ha cambiado la configuración de GPO	`vserver cifs group-policy update -vserver` *`vserver_name`*
Todas las configuraciones de GPO	`vserver cifs group-policy update -vserver` *`vserver_name`* `-force-reapply -all-settings true`

Información relacionada

Obtenga información sobre cómo actualizar GPO en servidores SMB

Mostrar información sobre las configuraciones de GPO SMB de ONTAP

Puede mostrar información acerca de las configuraciones de objeto de directiva de grupo (GPO) definidas en Active Directory y acerca de las configuraciones de GPO aplicadas al servidor CIFS.

Acerca de esta tarea

Puede mostrar información acerca de todas las configuraciones de GPO definidas en Active Directory del dominio al que pertenece el servidor CIFS o solo puede mostrar información acerca de las configuraciones de GPO aplicadas a un servidor CIFS.

Pasos

1. Mostrar información acerca de las configuraciones de GPO realizando una de las siguientes acciones:

Si desea mostrar información acerca de todas las configuraciones de directiva de grupo…	Introduzca el comando…
Definido en Active Directory	`vserver cifs group-policy show-defined -vserver vserver_name`
Aplicado a una máquina virtual de almacenamiento (SVM) habilitada para CIFS	`vserver cifs group-policy show-applied -vserver vserver_name`

Ejemplo

En el siguiente ejemplo, se muestran las configuraciones de GPO definidas en Active Directory al que pertenece la SVM habilitada para CIFS con el nombre vs1:

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache : version1
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
```

```
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
    Status: enabled
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication for Mode BranchCache: per-share
    Hash Version Support for BranchCache: version1
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
```

```
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

En el siguiente ejemplo, se muestran las configuraciones de GPO aplicadas a la SVM vs1 habilitada para CIFS:

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
-----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
```

```
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
```

```
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

Información relacionada

Habilitar o deshabilitar la compatibilidad con GPO en los servidores

Mostrar información sobre los GPO de grupo restringido SMB de ONTAP

Puede mostrar información detallada sobre los grupos restringidos que se definen como objetos de directiva de grupo (GPO) en Active Directory y que se aplican al servidor CIFS.

Acerca de esta tarea

De forma predeterminada, se muestra la siguiente información:

- Nombre de la política de grupo
- Versión de la directiva de grupo
- Enlace

  Especifica el nivel en el que se configura la directiva de grupo. Los valores de salida posibles incluyen los siguientes:

  - `Local` Cuando la política de grupo está configurada en ONTAP
  - `Site` cuando la política de grupo se configura en el nivel de sitio en el controlador de dominio
  - `Domain` cuando la política de grupo se configura en el nivel de dominio en el controlador de dominio
  - `OrganizationalUnit` Cuando la directiva de grupo se configura en el nivel de unidad organizativa (OU) en el controlador de dominio
  - `RSOP` para el conjunto resultante de políticas derivadas de todas las políticas de grupo definidas en varios niveles

- Nombre de grupo restringido
- Los usuarios y grupos que pertenecen al grupo restringido y que no pertenecen al mismo
- Lista de grupos a los que se agrega el grupo restringido

  Un grupo puede ser miembro de grupos distintos de los que se enumeran aquí.

Paso

1. Muestre información acerca de todos los GPO de grupo restringidos realizando una de las siguientes acciones:

Si desea mostrar información sobre todos los GPO de grupo restringidos…	Introduzca el comando…
Definido en Active Directory	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
Aplicado a un servidor CIFS	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

Ejemplo

En el siguiente ejemplo, se muestra información sobre los objetos de normativa de grupo restringidos definidos en el dominio de Active Directory al que pertenece la SVM habilitada para CIFS, llamada vs1:

```
cluster1::> vserver cifs group-policy restricted-group show-defined
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9
```

En el siguiente ejemplo, se muestra información sobre los objetos de normativa de grupo restringidos

aplicados a la SVM vs1 habilitada para CIFS:

```
cluster1::> vserver cifs group-policy restricted-group show-applied
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9
```

Información relacionada

Mostrar información acerca de las configuraciones de GPO

Muestra información sobre las políticas de acceso central de SMB de ONTAP

Puede mostrar información detallada acerca de las directivas de acceso central definidas en Active Directory. También puede mostrar información sobre las políticas de acceso central que se aplican al servidor CIFS a través de objetos de política de grupo (GPO).

Acerca de esta tarea

De forma predeterminada, se muestra la siguiente información:

- Nombre de SVM
- Nombre de la política de acceso central
- SID
- Descripción
- Hora de creación
- Tiempo de modificación
- Normas de los miembros

Los servidores CIFS en el modo de grupo de trabajo no se muestran porque no admiten los GPO.

Paso

1. Muestre información acerca de las directivas de acceso central realizando una de las siguientes acciones:

Si desea mostrar información sobre todas las directivas de acceso central…	Introduzca el comando…
Definido en Active Directory	`vserver cifs group-policy central-access-policy show-defined -vserver` *`vserver_name`*
Aplicado a un servidor CIFS	`vserver cifs group-policy central-access-policy show-applied -vserver` *`vserver_name`*

Ejemplo

El siguiente ejemplo muestra información de todas las directivas de acceso central definidas en Active Directory:

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name                 SID
-------- --------------------
--------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

El siguiente ejemplo muestra información de todas las políticas de acceso central que se aplican a las máquinas virtuales de almacenamiento (SVM) del clúster:

```
cluster1::> vserver cifs group-policy central-access-policy show-applied

Vserver    Name                 SID
-------- --------------------
---------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

Información relacionada

- Obtenga más información sobre la seguridad del acceso a archivos para servidores
- Mostrar información acerca de las configuraciones de GPO
- Muestra información acerca de las reglas de la política de acceso central

Mostrar información sobre las reglas de política de acceso central de SMB de ONTAP

Puede mostrar información detallada acerca de las reglas de directiva de acceso central asociadas a las directivas de acceso central definidas en Active Directory. También puede mostrar información sobre las reglas de políticas de acceso central que se aplican al servidor CIFS a través de los GPO de la política de acceso central (objetos de política de grupo).

Acerca de esta tarea

Puede mostrar información detallada acerca de las reglas de directiva de acceso central definidas y aplicadas. De forma predeterminada, se muestra la siguiente información:

- Nombre del Vserver
- Nombre de la regla de acceso central
- Descripción
- Hora de creación
- Tiempo de modificación
- Permisos actuales
- Permisos propuestos

- Recursos objetivo

Si desea mostrar información acerca de todas las reglas de directiva de acceso central asociadas con las directivas de acceso central…	Introduzca el comando…
Definido en Active Directory	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
Aplicado a un servidor CIFS	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

Ejemplo

En el siguiente ejemplo se muestra información de todas las reglas de directiva de acceso central asociadas a las directivas de acceso central definidas en Active Directory:

```
cluster1::> vserver cifs group-policy central-access-rule show-defined

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

El siguiente ejemplo muestra información de todas las reglas de políticas de acceso central asociadas con las políticas de acceso centrales aplicadas a las máquinas virtuales de almacenamiento (SVM) en el clúster:

```
cluster1::> vserver cifs group-policy central-access-rule show-applied

Vserver     Name
----------- --------------------
vs1         r1
            Description: rule #1
          Creation Time: Tue Oct 22 09:33:48 2013
      Modification Time: Tue Oct 22 09:33:48 2013
    Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
   Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1         r2
            Description: rule #2
          Creation Time: Tue Oct 22 10:27:57 2013
      Modification Time: Tue Oct 22 10:27:57 2013
    Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
   Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

Información relacionada

- Obtenga más información sobre la seguridad del acceso a archivos para servidores
- Mostrar información acerca de las configuraciones de GPO
- Muestra información sobre las políticas de acceso central

Comandos de ONTAP para gestionar contraseñas de cuentas de equipo de servidor SMB

Debe conocer los comandos para cambiar, restablecer y deshabilitar contraseñas, así como para configurar las programaciones de actualización automática. También puede configurar una programación en el servidor SMB para que la actualice automáticamente.

Si desea…	Se usa este comando…
Cambie la contraseña de la cuenta de dominio cuando ONTAP esté sincronizado con los servicios de AD	`vserver cifs domain password change`
Restablezca la contraseña de la cuenta de dominio cuando ONTAP no esté sincronizado con los servicios de AD	`vserver cifs domain password reset`
Configurar servidores SMB para cambios automáticos de contraseña de cuenta de equipo	`vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true`

Si desea…	Se usa este comando…
Deshabilite los cambios automáticos de contraseña de cuenta de equipo en servidores SMB	`vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false`

Obtenga más información sobre `vserver cifs domain password` en el "Referencia de comandos del ONTAP".

Gestione las conexiones del controlador de dominio

Mostrar información sobre los servidores detectados por el bloque de mensajes del servidor de ONTAP

Puede mostrar información relacionada con los servidores LDAP y las controladoras de dominio detectados en el servidor CIFS.

Paso

1. Para mostrar la información relacionada con los servidores detectados, introduzca el siguiente comando: `vserver cifs domain discovered-servers show`

Ejemplo

En el siguiente ejemplo, se muestran los servidores detectados para la SVM vs1:

```
cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

Información relacionada

- Restablecer y volver a detectar servidores
- Detener o iniciar servidores

Restablecer y volver a detectar los servidores SMB de ONTAP

La restauración y la nueva detección de servidores en el servidor CIFS permite que el servidor CIFS deseche la información almacenada sobre los servidores LDAP y las controladoras de dominio. Tras descartar información del servidor, el servidor CIFS vuelve a adquirir la información actual de estos servidores externos. Esto puede ser útil cuando los servidores conectados no responden adecuadamente.

Pasos

1. Introduzca el siguiente comando: `vserver cifs domain discovered-servers reset-servers -vserver vserver_name`
2. Mostrar información sobre los servidores recién redetectados: `vserver cifs domain discovered-servers show -vserver vserver_name`

Ejemplo

En el siguiente ejemplo, se restablecen y vuelven a detectar los servidores para la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1:

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver
vs1

cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

Información relacionada

- Muestra información sobre los servidores detectados
- Detener o iniciar servidores

Gestione la detección de controlador de dominio SMB de ONTAP

A partir de ONTAP 9.3, puede modificar el proceso predeterminado por el que se detectan los controladores de dominio (DC). Esto le permite limitar la detección a sus instalaciones o a un conjunto de centros de datos preferidos, lo que puede mejorar el rendimiento en función del entorno.

Acerca de esta tarea

De forma predeterminada, el proceso de detección dinámica detecta todos los centros de datos disponibles, incluidos los centros de datos preferidos, todos los centros de datos del sitio local y todos los centros de datos remotos. Esta configuración puede provocar latencia en autenticación y acceder a recursos compartidos en determinados entornos. Si ya ha determinado el grupo de DC que desea utilizar o si los DC remotos son inadecuados o inaccesibles, puede cambiar el método de descubrimiento.

En las versiones ONTAP 9.3 y posteriores, el `discovery-mode` parámetro del `cifs domain discovered-servers` comando permite seleccionar una de las siguientes opciones de detección:

- Se descubren todos los DC del dominio.

- Sólo se descubren los centros de datos del sitio local.

  `default-site`El parámetro del servidor SMB se puede definir para utilizar este modo con LIF que no están asignadas a un sitio en sites-and-services.

- No se realiza la detección del servidor, la configuración del servidor SMB depende únicamente de los centros de datos preferidos.

  Para utilizar este modo, primero debe definir los DC preferidos para el servidor SMB.

Antes de empezar

Debe estar en el nivel de privilegio avanzado.

Paso

1. Especifique la opción de detección deseada: `vserver cifs domain discovered-servers discovery-mode modify -vserver` *`vserver_name`* `-mode {all|site|none}`

   Opciones para el `mode` parámetro:

   - `all`

     Descubrir todos los DC disponibles (predeterminado).

   - `site`

     Limite el descubrimiento de DC a su sitio.

   - `none`

     Utilice sólo los centros de datos preferidos y no realice la detección.

Añada controladoras de dominio SMB de ONTAP preferidas

ONTAP detecta automáticamente controladoras de dominio a través de DNS. Opcionalmente, puede añadir uno o varios controladores de dominio a la lista de controladores de dominio preferidos para un dominio específico.

Acerca de esta tarea

Si ya existe una lista de controladores de dominio preferido para el dominio especificado, la nueva lista se combina con la lista existente.

Paso

1. Para agregar a la lista de controladores de dominio preferidos, introduzca el siguiente comando: `vserver cifs domain preferred-dc add -vserver` *`vserver_name`* `-domain` *`domain_name`* `-preferred-dc IP_address, …+`

   `-vserver` *`vserver_name`* Especifica el nombre de la máquina virtual de almacenamiento (SVM).

`-domain` *`domain_name`* Especifica el nombre completo de Active Directory del dominio al que pertenecen los controladores de dominio especificados.

`-preferred-dc` *`IP_address`*,... especifica una o más direcciones IP de los controladores de dominio preferidos, como una lista delimitada por comas, en orden de preferencia.

Ejemplo

El siguiente comando añade los controladores de dominio 172.17.102.25 y 172.17.102.24 a la lista de controladores de dominio preferidos que el servidor SMB en SVM vs1 utiliza para gestionar el acceso externo al dominio cifs.lab.example.com.

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

Información relacionada

Comandos para gestionar controladoras de dominio preferidas

Comandos de ONTAP para gestionar las controladoras de dominio SMB preferidas

Debe conocer los comandos para añadir, mostrar y eliminar controladoras de dominio preferidas.

Si desea…	Se usa este comando…
Agregar un controlador de dominio preferido	`vserver cifs domain preferred-dc add`
Mostrar los controladores de dominio preferidos	`vserver cifs domain preferred-dc show`
Quite una controladora de dominio preferida	`vserver cifs domain preferred-dc remove`

Obtenga más información sobre `vserver cifs domain preferred-dc` en el "Referencia de comandos del ONTAP".

Información relacionada

Añada controladores de dominio preferidos

Habilite las conexiones cifradas a los controladores de dominio SMB de ONTAP

A partir de ONTAP 9.8, puede especificar que se cifren las conexiones a los controladores de dominio.

Acerca de esta tarea

ONTAP requiere cifrado para las comunicaciones del controlador de dominio (DC) cuando la `-encryption -required-for-dc-connection` opción está establecida en `true`; el valor predeterminado es `false`. Cuando se establece la opción, solo se utilizará el protocolo SMB3 para las conexiones ONTAP-DC, ya que el cifrado solo es compatible con SMB3.

Cuando se requieren comunicaciones CC cifradas, la `-smb2-enabled-for-dc-connections` opción se

ignora, ya que ONTAP solo negocia conexiones SMB3. Si un controlador de dominio no admite SMB3 y cifrado, ONTAP no se conectará a él.

Paso

1. Habilitar la comunicación cifrada con el DC: `vserver cifs security modify -vserver` *`svm_name`* `-encryption-required-for-dc-connection true`

Utilice sesiones nulas para acceder al almacenamiento en entornos que no sean de Kerberos

Utilice sesiones nulas de SMB de ONTAP para acceder al almacenamiento en entornos que no sean Kerberos

El acceso de sesión nulo proporciona permisos para recursos de red, como datos del sistema de almacenamiento, y para servicios basados en cliente que se ejecutan en el sistema local. Una sesión nula se produce cuando un proceso de cliente utiliza la cuenta "system" para acceder a un recurso de red. La configuración de sesión nula es específica para la autenticación que no es de Kerberos.

Descubra cómo los sistemas de almacenamiento para pymes de ONTAP proporcionan un acceso nulo a la sesión

Debido a que los recursos compartidos de sesión nulos no requieren autenticación, los clientes que requieren acceso de sesión nulo deben tener sus direcciones IP asignadas en el sistema de almacenamiento.

De forma predeterminada, los clientes de sesión nula sin asignar pueden acceder a determinados servicios del sistema ONTAP, como la enumeración de recursos compartidos, pero se limitan a acceder a cualquier dato del sistema de almacenamiento.

> ONTAP admite los valores de configuración del Registro anónimo con la `-restrict-anonymous` opción. Esto permite controlar hasta qué punto los usuarios nulos no asignados pueden ver o acceder a los recursos del sistema. Por ejemplo, puede deshabilitar la enumeración de recursos compartidos y el acceso al recurso compartido IPC$ (recurso compartido de canalizaciones con nombre oculto). Obtenga más información acerca de `vserver cifs options modify` y `vserver cifs options show` y la `-restrict-anonymous` opción en el "Referencia de comandos del ONTAP".

A menos que se configure lo contrario, un cliente que ejecute un proceso local que solicite acceso al sistema de almacenamiento a través de una sesión nula sólo es miembro de grupos no restrictivos, como «'todos'». Para limitar el acceso de sesión nulo a los recursos del sistema de almacenamiento seleccionados, es posible que desee crear un grupo al que pertenecen todos los clientes de sesión nulos; al crear este grupo se le permite restringir el acceso al sistema de almacenamiento y establecer permisos de recursos del sistema de almacenamiento que se aplican específicamente a clientes de sesión nulos.

ONTAP proporciona una sintaxis de asignación en el `vserver name-mapping` conjunto de comandos para especificar la dirección IP de los clientes que permite el acceso a los recursos del sistema de almacenamiento mediante una sesión de usuario nula. Después de crear un grupo para usuarios nulos, puede especificar restricciones de acceso para los recursos del sistema de almacenamiento y permisos de recursos que se apliquen solo a sesiones nulas. El usuario nulo se identifica como inicio de sesión anónimo. Los usuarios nulos no tienen acceso a ningún directorio principal.

Todos los usuarios nulos que acceden al sistema de almacenamiento desde una dirección IP asignada se conceden permisos de usuario asignado. Considere las precauciones adecuadas para evitar el acceso no autorizado a sistemas de almacenamiento asignados con usuarios nulos. Para obtener la máxima protección, coloque el sistema de almacenamiento y todos los clientes que necesiten un acceso nulo al sistema de almacenamiento de usuarios en una red independiente, con el fin de eliminar la posibilidad de que se produzca una dirección IP «posing».

Información relacionada

Configurar restricciones de acceso para usuarios anónimos

Otorgue acceso de usuarios nulos a recursos compartidos del sistema de archivos SMB de ONTAP

Puede permitir el acceso a los recursos del sistema de almacenamiento por parte de clientes de sesión nulos asignando un grupo para que lo utilicen clientes de sesión nulos y registrando las direcciones IP de clientes de sesión nulos para añadirlas a la lista de clientes a los que el sistema de almacenamiento puede acceder a los datos mediante sesiones nulas.

Pasos

1. Utilice el `vserver name-mapping create` comando para asignar el usuario nulo a cualquier usuario válido de Windows, con un cualificador de IP.

   El siguiente comando asigna el usuario nulo al usuario1 con un nombre de host válido google.com:

   ```
   vserver name-mapping create -direction win-unix  -position 1 -pattern
   "ANONYMOUS LOGON" -replacement user1 - hostname google.com
   ```

   El siguiente comando asigna el usuario nulo a user1 con una dirección IP válida 10.238.2.54/32:

   ```
   vserver name-mapping create -direction win-unix  -position 2 -pattern
   "ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
   ```

2. Utilice `vserver name-mapping show` el comando para confirmar la asignación de nombres.

   ```
   vserver name-mapping show

   Vserver:   vs1
   Direction: win-unix
   Position Hostname         IP Address/Mask
   -------- --------         ----------------
   1        -                10.72.40.83/32      Pattern: anonymous logon
                                              Replacement: user1
   ```

3. Utilice `vserver cifs options modify –win-name-for-null-user` el comando para asignar la pertenencia de Windows al usuario nulo.

Esta opción sólo se aplica cuando hay una asignación de nombres válida para el usuario nulo.

```
vserver cifs options modify -win-name-for-null-user user1
```

4. Utilice el `vserver cifs options show` comando para confirmar la asignación del usuario nulo al usuario o grupo de Windows.

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```

Administrar alias NetBIOS para servidores SMB

Obtenga información sobre la administración de alias de NetBIOS para servidores SMB de ONTAP

Los alias NetBIOS son nombres alternativos para el servidor SMB que los clientes SMB pueden utilizar al conectarse con el servidor SMB. La configuración de alias NetBIOS para un servidor SMB puede ser útil cuando está consolidando datos de otros servidores de archivos en el servidor SMB y desea que el servidor SMB responda a los nombres de los servidores de archivos originales.

Puede especificar una lista de alias NetBIOS cuando cree el servidor SMB o en cualquier momento después de crear el servidor SMB. Puede agregar o quitar alias NetBIOS de la lista en cualquier momento. Puede conectarse al servidor SMB utilizando cualquiera de los nombres de la lista de alias NetBIOS.

Información relacionada

Muestra información acerca de NetBIOS sobre conexiones TCP

Agregue listas de alias de NetBIOS a los servidores SMB de ONTAP

Si desea que los clientes SMB se conecten al servidor SMB mediante un alias, puede crear una lista de alias NetBIOS o agregar alias NetBIOS a una lista existente de alias NetBIOS.

Acerca de esta tarea

- El nombre del alias NetBIOS puede tener una longitud máxima de 15 caracteres.
- Puede configurar hasta 200 alias NetBIOS en el servidor SMB.
- No se permiten los siguientes caracteres:

  @ # * ( ) = + [ ] | ; : " , < > \ / ?

Pasos

1. Agregue los alias de NetBIOS:

```
vserver cifs add-netbios-aliases -vserver vserver_name -netbios-aliases
NetBIOS_alias,…

vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases
alias_1,alias_2,alias_3
```

- Puede especificar uno o varios alias NetBIOS utilizando una lista delimitada por comas.
- Los alias NetBIOS especificados se agregan a la lista existente.
- Se crea una nueva lista de alias NetBIOS si la lista está vacía actualmente.

2. Compruebe que los alias de NetBIOS se han agregado correctamente: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

Información relacionada

- Eliminar alias NetBIOS de la lista para servidores SMB
- Mostrar la lista de alias NetBIOS para servidores SMB

Elimine los alias de NetBIOS de la lista de servidores SMB de ONTAP

Si no necesita alias NetBIOS específicos para un servidor CIFS, puede eliminar esos alias NetBIOS de la lista. También puede quitar todos los alias NetBIOS de la lista.

Acerca de esta tarea

Puede quitar más de un alias NetBIOS utilizando una lista delimitada por comas. Puede quitar todos los alias de NetBIOS de un servidor CIFS especificando - como valor para `-netbios-aliases` el parámetro.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea quitar…	Introduzca…
Alias NetBIOS específicos de la lista	`vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios -aliases _NetBIOS_alias_,...`
Todos los alias NetBIOS de la lista	`vserver cifs remove-netbios-aliases -vserver vserver_name -netbios-aliases -`

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

2. Verifique que se hayan eliminado los alias de NetBIOS especificados: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_2, ALIAS_3
```

Mostrar la lista de alias de NetBIOS para los servidores SMB de ONTAP

Puede mostrar la lista de alias NetBIOS. Esto puede resultar útil cuando desea determinar la lista de nombres a través de la cual los clientes SMB pueden realizar conexiones con el servidor CIFS.

Paso

1. Ejecute una de las siguientes acciones:

Si desea mostrar información acerca de…	Introduzca…
Alias de NetBIOS de un servidor CIFS	`vserver cifs show -display-netbios -aliases`
La lista de alias NetBIOS como parte de la información detallada del servidor CIFS	`vserver cifs show -instance`

En el siguiente ejemplo, se muestra información sobre los alias NetBIOS de un servidor CIFS:

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

En el siguiente ejemplo, se muestra la lista de alias NetBIOS como parte de la información detallada del servidor CIFS:

```
vserver cifs show -instance
```

```
                                        Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_SERVER
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                           Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

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

Información relacionada

- Agregar listas de alias NetBIOS a los servidores
- Comandos para administrar servidores

Determine si los clientes SMB de ONTAP están conectados mediante alias NetBIOS

Puede determinar si los clientes SMB están conectados mediante alias NetBIOS y, si es así, qué alias NetBIOS se utiliza para realizar la conexión. Esto puede ser útil para solucionar problemas de conexión.

Acerca de esta tarea

Debe utilizar el `-instance` parámetro para mostrar el alias de NetBIOS (si existe) asociado a una conexión SMB. Si el nombre del servidor CIFS o una dirección IP se utilizan para establecer la conexión SMB, la salida del `NetBIOS Name` campo es - (guión).

Paso

1. Realice la acción deseada:

Si desea mostrar información de NetBIOS para…	Introduzca…
Conexiones SMB	`vserver cifs session show -instance`
Conexiones que utilizan un alias NetBIOS especificado:	`vserver cifs session show -instance -netbios-name` *`netbios_name`*

En el siguiente ejemplo se muestra información sobre el alias NetBIOS utilizado para establecer la conexión SMB con el ID de sesión 1:

```
vserver cifs session show -session-id 1 -instance
```

```
                          Node: node1
                       Vserver: vs1
                    Session ID: 1
                 Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
                   Workstation: 10.2.2.50
    Authentication Mechanism: NTLMv2
                Windows User: EXAMPLE\user1
                   UNIX User: user1
                  Open Shares: 2
                   Open Files: 2
                   Open Other: 0
                Connected Time: 1d 1h 10m 5s
                     Idle Time: 22s
             Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: ALIAS1
       SMB Encryption Status: Unencrypted
```

Administrar varias tareas del servidor SMB

Detenga o inicie los servidores SMB de ONTAP

Puede detener el servidor CIFS en una SVM, que puede ser útil a la hora de realizar tareas mientras los usuarios no acceden a datos a través de recursos compartidos SMB. Puede reiniciar el acceso SMB iniciando el servidor CIFS. Al detener el servidor CIFS, también puede modificar los protocolos permitidos en la máquina virtual de almacenamiento (SVM).

Pasos

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el comando…
Detenga el servidor CIFS	`vserver cifs stop -vserver *vserver_name* [-foreground {true
false}]`	Inicie EL servidor CIFS
`vserver cifs start -vserver *vserver_name* [-foreground {true	false}]`

`-foreground` especifica si el comando debe ejecutarse en primer plano o en segundo plano. Si no

introduce este parámetro, se establece en `true`, y el comando se ejecuta en primer plano.

2. Compruebe que el estado administrativo del servidor CIFS sea correcto mediante `vserver cifs show` el comando.

Ejemplo

Los siguientes comandos inician el servidor CIFS en la SVM vs1:

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: VS1
                    NetBIOS Domain/Workgroup Name: DOMAIN
                      Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
```

Información relacionada

- Muestra información sobre los servidores detectados
- Restablecer y volver a detectar servidores

Mueva los servidores SMB de ONTAP a distintas unidades organizativas

El proceso de creación del servidor CIFS utiliza la unidad organizativa (OU) CN=Computers predeterminada durante la instalación, a menos que especifique una unidad organizativa diferente. Puede mover servidores CIFS a unidades organizativas diferentes tras la configuración.

Pasos

1. En el servidor Windows, abra el árbol **usuarios y equipos de Active Directory**.
2. Busque el objeto de Active Directory para la máquina virtual de almacenamiento (SVM).
3. Haga clic con el botón derecho del ratón en el objeto y seleccione **mover**.
4. Seleccione la unidad organizativa que desea asociar con la SVM

Resultados

El objeto SVM se coloca en la unidad organizativa seleccionada.

Modifique el dominio DNS dinámico antes de mover los servidores SMB de ONTAP

Si desea que el servidor DNS integrado en Active Directory registre de forma dinámica los registros DNS del servidor SMB en DNS cuando mueve el servidor SMB a otro dominio, debe modificar el DNS dinámico (DDNS) en la máquina virtual de almacenamiento (SVM) antes de mover el servidor SMB.

Antes de empezar

Los servicios de nombres DNS se deben modificar en la SVM para utilizar el dominio DNS que contiene los registros de ubicación del servicio para el nuevo dominio que contendrá la cuenta de equipo del servidor SMB. Si utiliza DDNS seguro, debe utilizar servidores de nombres DNS integrados en Active Directory.

Acerca de esta tarea

Si bien DDNS (si se configura en la SVM) agrega automáticamente los registros DNS de las LIF de datos al dominio nuevo, los registros DNS del dominio original no se eliminan automáticamente del servidor DNS original. Debe eliminarlos manualmente.

Para completar las modificaciones de DDNS antes de mover el servidor SMB, consulte el siguiente tema:

"Configure los servicios DNS dinámicos"

Únase a las SVM de SMB de ONTAP a los dominios de Active Directory

Puede unir una máquina virtual de almacenamiento (SVM) a un dominio de Active Directory sin eliminar el servidor SMB existente mediante la modificación del dominio con `vserver cifs modify` el comando. Puede volver a unirse al dominio actual o unirse a uno nuevo.

Antes de empezar

- La SVM ya debe tener una configuración de DNS.
- La configuración de DNS para la SVM debe poder servir el dominio de destino.

  Los servidores DNS deben contener los registros de ubicación de servicio (SRV) para el LDAP de dominio y los servidores del controlador de dominio.

Acerca de esta tarea

- El estado administrativo del servidor CIFS debe estar configurado para `down` continuar con la modificación del dominio de Active Directory.
- Si el comando se completa correctamente, el estado administrativo se establece automáticamente en `up`. Obtenga más información sobre `up` en el "Referencia de comandos del ONTAP".
- Al unirse a un dominio, este comando puede tardar varios minutos en completarse.

Pasos

1. Una la SVM al dominio del servidor CIFS: `vserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`* `-status-admin down`

   Obtenga más información sobre `vserver cifs modify` en el "Referencia de comandos del ONTAP". Si necesita reconfigurar DNS para el nuevo dominio, obtenga más información `vserver dns modify` en el "Referencia de comandos del ONTAP".

   Para crear una cuenta de máquina de Active Directory para el servidor SMB, debe proporcionar el nombre y la contraseña de una cuenta de Windows con suficiente Privileges para agregar equipos al `ou=` *`example`* `ou` contenedor dentro del *`example`* dominio .com.

   A partir de ONTAP 9.7, el administrador de AD puede proporcionarle un URI a un archivo keytab como alternativa a proporcionarle un nombre y una contraseña a una cuenta de Windows con privilegios. Cuando reciba el URI, inclúyalo en el `-keytab-uri` parámetro con `vserver cifs` los comandos.

2. Compruebe que el servidor CIFS se encuentra en el dominio de Active Directory deseado: `vserver cifs show`

Ejemplo

En el siguiente ejemplo, el servidor SMB «'CIFSSERVER1'» de la SVM vs1 se une al dominio example.com mediante la autenticación keytab:

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab

cluster1::> vserver cifs show

          Server       Status       Domain/Workgroup  Authentication
Vserver   Name         Admin        Name              Style
--------- -----------  ---------    ----------------  --------------
vs1       CIFSSERVER1  up           EXAMPLE          domain
```

Mostrar información acerca de las conexiones SMB NetBIOS over TCP de ONTAP

Puede mostrar información acerca de las conexiones NetBIOS sobre TCP (NBT). Esto puede ser útil para solucionar problemas relacionados con NetBIOS.

Paso

1. Utilice el `vserver cifs nbtstat` comando para mostrar información acerca de las conexiones NetBIOS a través de TCP.

> No se admite el servicio de nombres NetBIOS (NBNS) sobre IPv6.

Ejemplo

En el siguiente ejemplo se muestra la información del servicio de nombres NetBIOS que se muestra para "'cluster1'":

```
cluster1::> vserver cifs nbtstat

          Vserver: vs1
          Node:    cluster1-01
          Interfaces:
                   10.10.10.32
                   10.10.10.33
         Servers:
                   17.17.1.2  (active  )
         NBT Scope:
                  [ ]
         NBT Mode:
                  [h]
         NBT Name    NetBIOS Suffix   State   Time Left   Type
         ----------- ---------------  ------- ---------   -----
         CLUSTER_1   00               wins    57
         CLUSTER_1   20               wins    57

         Vserver: vs1
         Node:    cluster1-02
         Interfaces:
                 10.10.10.35
         Servers:
                 17.17.1.2  (active  )
         CLUSTER_1          00               wins          58
         CLUSTER_1          20               wins          58
         4 entries were displayed.
```

Comandos de ONTAP para gestionar servidores SMB

Debe conocer los comandos para crear, mostrar, modificar, detener, iniciar, Y eliminando servidores SMB. También hay comandos para restablecer y volver a detectar servidores, cambiar o restablecer contraseñas de cuentas de equipo, programar cambios para contraseñas de cuentas de equipo y agregar o quitar alias de NetBIOS.

Si desea…	Se usa este comando…
Cree un servidor SMB	`vserver cifs create`
Muestra información acerca de un servidor SMB	`vserver cifs show`
Modificar un servidor SMB	`vserver cifs modify`
Mover un servidor SMB a otro dominio	`vserver cifs modify`

Detener un servidor SMB	`vserver cifs stop`
Inicie un servidor SMB	`vserver cifs start`
Suprimir un servidor SMB	`vserver cifs delete`
Restablecer y volver a detectar servidores para el servidor SMB	`vserver cifs domain discovered-servers reset-servers`
Cambiar la contraseña de la cuenta de equipo del servidor SMB	`vserver cifs domain password change`
Restablezca la contraseña de la cuenta de máquina del servidor SMB	`vserver cifs domain password change`
Programar cambios automáticos de contraseña para la cuenta de equipo del servidor SMB	`vserver cifs domain password schedule modify`
Agregue alias NetBIOS para el servidor SMB	`vserver cifs add-netbios-aliases`
Elimine los alias de NetBIOS para el servidor SMB	`vserver cifs remove-netbios-aliases`

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

Información relacionada

"Qué sucede a los usuarios locales y grupos al eliminar servidores SMB"

Habilite el servicio de nombres NetBIOS SMB de ONTAP

A partir de ONTAP 9, el servicio de nombres NetBIOS (NBNS, a veces denominado Servicio de nombres Internet de Windows o WINS) está deshabilitado de forma predeterminada. Anteriormente, las máquinas virtuales de almacenamiento (SVM) habilitadas para CIFS enviaron registros de nombres independientemente de si se habilitó WINS en una red. Para limitar dichas emisiones a configuraciones en las que se necesita NBNS, debe habilitar NBNS explícitamente para servidores CIFS nuevos.

Antes de empezar

- Si ya está utilizando NBNS y actualiza a ONTAP 9, no es necesario completar esta tarea. NBNS continuará trabajando como antes.
- NBNS está habilitado en UDP (puerto 137).
- No se admite NBNS sobre IPv6.

Pasos

1. Configure el nivel de privilegio en Advanced.

```
set -privilege advanced
```

2. Habilite NBNS en un servidor CIFS.

```
vserver cifs options  modify -vserver <vserver name> -is-nbns-enabled
true
```

3. Vuelva al nivel de privilegio de administrador.

```
set -privilege admin
```

Utilice IPv6 para el acceso a SMB y los servicios SMB

Obtenga más información sobre los requisitos del bloque de mensajes del servidor de ONTAP para IPv6

Antes de poder utilizar IPv6 en el servidor SMB, debe saber qué versiones de ONTAP y SMB admiten y cuáles son los requisitos de licencia.

Requisitos para la licencia de ONTAP

No se requiere ninguna licencia especial para IPv6 cuando SMB tiene licencia. La licencia SMB se incluye con "ONTAP One". Si no tiene ONTAP One y la licencia no está instalada, póngase en contacto con su representante de ventas.

Requisitos de la versión del protocolo SMB

- Para las SVM, ONTAP es compatible con IPv6 en todas las versiones del protocolo SMB.

> No se admite el servicio de nombres NetBIOS (NBNS) sobre IPv6.

Descubre el soporte para IPv6 con acceso SMB de ONTAP y servicios CIFS

Si desea usar IPv6 en el servidor CIFS, debe saber cómo ONTAP admite IPv6 para el acceso SMB y la comunicación de redes para servicios CIFS.

Compatibilidad con clientes y servidores Windows

ONTAP ofrece compatibilidad con los servidores y clientes de Windows que admiten IPv6. A continuación se describe la compatibilidad con IPv6 del cliente Microsoft Windows y el servidor:

- Windows 7, Windows 8, Windows Server 2008, Windows Server 2012 y versiones posteriores admiten IPv6 tanto para el uso compartido de archivos SMB como para los servicios de Active Directory, incluidos los servicios DNS, LDAP, CLDAP y Kerberos.

  Si se han configurado direcciones IPv6, Windows 7 y Windows Server 2008 y versiones posteriores utilizan IPv6 de forma predeterminada para los servicios de Active Directory. Se admiten tanto la

autenticación NTLM como la autenticación Kerberos a través de conexiones IPv6.

Todos los clientes de Windows compatibles con ONTAP pueden conectarse a recursos compartidos de SMB mediante direcciones IPv6.

Para obtener la información más reciente sobre los clientes de Windows que admite ONTAP, consulte la "Matriz de interoperabilidad".

Los dominios NT no son compatibles con IPv6.

Compatibilidad adicional con servicios CIFS

Además de la compatibilidad con IPv6 para recursos compartidos de archivos SMB y servicios de Active Directory, ONTAP ofrece compatibilidad con IPv6 para lo siguiente:

- Servicios de cliente, incluidas carpetas sin conexión, perfiles de itinerancia, redirección de carpetas y versiones anteriores
- Servicios del lado del servidor, incluidos directorios iniciales dinámicos (funcionalidad de Home Directory), enlaces simbólicos y widgets, BranchCache, descarga de copias ODX, referencias automáticas a nodos, Y versiones anteriores
- Servicios de administración de acceso a archivos, incluido el uso de usuarios y grupos locales de Windows para el control de acceso y la administración de derechos, la configuración de permisos de archivos y políticas de auditoría mediante la CLI, el seguimiento de seguridad, la gestión de bloqueos de archivos y la supervisión de la actividad de SMB
- Auditoría multiprotocolo de NAS
- FPolicy
- Recursos compartidos disponibles de forma continua, protocolo de observación y VSS remoto (utilizado con configuraciones de Hyper-V en SMB)

Servicio de nombres y soporte del servicio de autenticación

La comunicación con los siguientes servicios de nombres se admite con IPv6:

- Controladores de dominio
- Servidores DNS
- Servidores LDAP
- Servidores KDC
- Servidores NIS

Descubra cómo los servidores SMB de ONTAP utilizan IPv6 para conectarse a servidores externos

Para crear una configuración que cumpla con sus requisitos, debe saber cómo usan IPv6 los servidores CIFS a la hora de realizar conexiones a servidores externos.

- Selección de direcciones de origen

  Si se intenta conectarse a un servidor externo, la dirección de origen seleccionada debe ser del mismo tipo que la dirección de destino. Por ejemplo, si se conecta a una dirección IPv6, la máquina virtual de almacenamiento (SVM) que aloja el servidor CIFS debe tener una LIF de datos o una LIF de gestión que

tenga una dirección IPv6 que se usará como dirección de origen. Del mismo modo, si se conecta a una dirección IPv4, la SVM debe tener una LIF de datos o una LIF de gestión que tenga una dirección IPv4 que se usará como dirección de origen.

- Para los servidores detectados dinámicamente mediante DNS, la detección de servidores se realiza de la siguiente manera:
  - Si IPv6 está deshabilitado en el clúster, solo se detectan direcciones de los servidores IPv4.
  - Si IPv6 está habilitado en el clúster, se detectan tanto las direcciones de los servidores IPv4 como IPv6. Cualquiera de los dos tipos puede utilizarse en función de la idoneidad del servidor al que pertenece la dirección y de la disponibilidad de LIF de gestión o datos IPv6 o IPv4. La detección dinámica de servidores se utiliza para detectar controladores de dominio y sus servicios asociados, como LSA, NETLOGON, Kerberos y LDAP.
- Conectividad del servidor DNS

  Si la SVM utiliza IPv6 al conectarse a un servidor DNS depende de la configuración de los servicios de nombres DNS. Si los servicios DNS se configuran para utilizar direcciones IPv6, las conexiones se realizan mediante IPv6. Si lo desea, la configuración de los servicios de nombres DNS puede utilizar direcciones IPv4 para que las conexiones con los servidores DNS sigan usando direcciones IPv4. Las combinaciones de direcciones IPv4 e IPv6 pueden especificarse al configurar los servicios de nombres DNS.

- Conectividad del servidor LDAP

  Si la SVM utiliza IPv6 al conectarse a un servidor LDAP depende de la configuración del cliente LDAP. Si el cliente LDAP está configurado para usar direcciones IPv6, las conexiones se realizan mediante IPv6. Si lo desea, la configuración del cliente LDAP puede usar direcciones IPv4 a fin de que las conexiones con servidores LDAP sigan usando direcciones IPv4. Al configurar la configuración del cliente LDAP, se pueden especificar las combinaciones de direcciones IPv4 e IPv6.

  > La configuración del cliente LDAP se utiliza al configurar LDAP para los servicios de nombre de usuario, grupo y grupo de redes de UNIX.

- Conectividad del servidor NIS

  Si la SVM utiliza IPv6 al conectarse a un servidor NIS depende de la configuración de los servicios de nombres NIS. Si los servicios NIS se configuran para utilizar direcciones IPv6, las conexiones se realizan mediante IPv6. Si lo desea, la configuración de los servicios de nombres NIS puede utilizar direcciones IPv4 para que las conexiones con los servidores NIS sigan usando direcciones IPv4. Las combinaciones de direcciones IPv4 e IPv6 pueden especificarse al configurar los servicios de nombres NIS.

  > Los servicios de nombres NIS se utilizan para almacenar y administrar objetos de usuario, grupo, grupo de red y nombre de host de UNIX.

Información relacionada

- Habilitar IPv6 para servidores
- Supervisar y mostrar información sobre sesiones IPv6

Habilite IPv6 para los servidores SMB de ONTAP

Las redes IPv6 no se habilitan durante la configuración del clúster. Un administrador de clúster debe habilitar IPv6 después de que la configuración del clúster se haya

completado a fin de usar IPv6 para SMB. Cuando el administrador de clúster habilita IPv6, se habilita para todo el clúster.

Paso

1. Habilitar IPv6: `network options ipv6 modify -enabled true`

   IPv6 está habilitado. Se pueden configurar LIF de datos IPv6 para el acceso SMB.

Información relacionada

- Supervisar y mostrar información sobre sesiones IPv6
- "Visualice la red mediante System Manager"
- "Habilitación de IPv6 en el clúster"
- "opciones de red ipv6 modificar"

Obtenga información sobre cómo deshabilitar IPv6 para servidores SMB de ONTAP

Aunque IPv6 esté habilitado en el clúster mediante una opción de red, no puede deshabilitar IPv6 para SMB con el mismo comando. En su lugar, ONTAP deshabilita IPv6 cuando el administrador de clúster deshabilita la última interfaz habilitada para IPv6 en el clúster. Debe comunicarse con el administrador de clúster acerca de la gestión de las interfaces IPv6 habilitadas.

Información relacionada

- "Visualizar la red de ONTAP mediante System Manager"

Supervise y muestre información acerca de las sesiones SMB de IPv6 ONTAP

Puede supervisar y mostrar información sobre las sesiones SMB conectadas mediante redes IPv6. Esta información es útil para determinar qué clientes se conectan mediante IPv6, así como otra información útil sobre las sesiones SMB de IPv6.

Paso

1. Realice la acción deseada:

Si desea determinar si…	Introduzca el comando…
Las sesiones SMB a una máquina virtual de almacenamiento (SVM) se conectan mediante IPv6	`vserver cifs session show -vserver` *`vserver_name`* `-instance`
IPv6 se utiliza para sesiones SMB a través de una dirección LIF especificada	`vserver cifs session show -vserver` *`vserver_name`* `-lif-address` *`LIF_IP_address`* `-instance` *`LIF_IP_address`* Es la dirección IPv6 de la LIF de datos.

Configurar el acceso a archivos mediante SMB

Configurar estilos de seguridad

Cómo afectan los estilos de seguridad al acceso a los datos

Obtén más información sobre los estilos de seguridad del bloque de mensajes del servidor de ONTAP y sus efectos

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

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

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

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

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

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

volúmenes de FlexGroup.

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

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

Información relacionada

- "Referencia de comandos del ONTAP"

Obtén información sobre dónde y cuándo establecer los estilos de seguridad de SMB de ONTAP

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

Decida qué estilos de seguridad de SMB se utilizarán en las SVM de ONTAP

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

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

Estilo de seguridad	Elija si…
UNIX	• Un administrador de UNIX gestiona el sistema de ficheros. • La mayoría de los usuarios son clientes NFS. • Una aplicación que accede a los datos utiliza un usuario UNIX como cuenta de servicio.

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

Obtenga información sobre la herencia del estilo de seguridad del bloque de mensajes del servidor de ONTAP

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

Los estilos de seguridad se heredan de la siguiente manera:

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

Obtenga más información sobre la conservación de permisos UNIX para volúmenes de FlexVol SMB de ONTAP

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

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

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

Obtenga información sobre la gestión de permisos UNIX mediante la ficha Seguridad de Windows para servidores SMB de ONTAP

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

- Modificación de permisos de UNIX

  Puede usar la pestaña Seguridad de Windows para ver y cambiar los permisos de UNIX para un volumen o un qtree de estilo de seguridad mixto. Si utiliza la ficha Seguridad de Windows principal para cambiar los

permisos de UNIX, primero debe quitar la ACE existente que desea editar (esto establece los bits de modo en 0) antes de realizar los cambios. De forma alternativa, puede utilizar el editor avanzado para cambiar los permisos.

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

- Cambiar los permisos de UNIX a los permisos NTFS

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

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

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

Configure los estilos de seguridad SMB en volúmenes raíz de SVM de ONTAP

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

Pasos

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

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

2. Muestre y verifique la configuración, incluido el estilo de seguridad del volumen raíz de la SVM que creó: `vserver show -vserver` *`vserver_name`*

Configure los estilos de seguridad de SMB en volúmenes de ONTAP FlexVol

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

Pasos

1. Ejecute una de las siguientes acciones:

Si el volumen de FlexVol…	Usar el comando…

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

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

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

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

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

```
volume show -volume volume_name -instance
```

Configure los estilos de seguridad de SMB en qtrees de ONTAP

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

Pasos

1. Ejecute una de las siguientes acciones:

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

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

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

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

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

Cree y gestione volúmenes de datos en espacios de nombres NAS

Obtenga más información sobre la creación y la gestión de volúmenes de datos de bloque de mensajes del servidor de ONTAP en espacios de nombres NAS

Para gestionar el acceso a archivos en un entorno NAS, debe gestionar volúmenes de datos y puntos de unión en la máquina virtual de almacenamiento (SVM). Esto incluye planificar la arquitectura de espacios de nombres, crear volúmenes con o sin puntos de unión, montar o desmontar volúmenes, y mostrar información sobre volúmenes de datos y espacios de nombres de servidores NFS o servidores CIFS.

Crear volúmenes de datos del bloque de mensajes del servidor de ONTAP con puntos de unión especificados

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

Antes de empezar

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

> Los siguientes caracteres no se pueden utilizar en la ruta de unión: * # " > < | ? \
>
> Además, la longitud de la ruta de unión no puede ser superior a 255 caracteres.

Pasos

1. Cree el volumen con un punto de unión: `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path` *`junction_path`*

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

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

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

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

2. Compruebe que el volumen se creó con el punto de unión deseado: `volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-junction`

Ejemplo

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

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

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

Crear volúmenes de datos del bloque de mensajes del servidor de ONTAP sin especificar puntos de unión

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

Antes de empezar

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

Pasos

1. Cree el volumen sin un punto de unión mediante el siguiente comando: `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}`

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

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

2. Compruebe que el volumen se creó sin un punto de unión: `volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-junction`

Ejemplo

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

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

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

Monte o desmonte volúmenes SMB de ONTAP existentes en el espacio de nombres NAS

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

Acerca de esta tarea

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

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

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

Pasos

1. Realice la acción deseada:

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

Si desea…	Introduzca los comandos…

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

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

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

Ejemplos

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

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

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

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

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

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

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

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

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

Puede ver información sobre los volúmenes montados para las máquinas virtuales de almacenamiento (SVM) y los puntos de unión a los que están montados los volúmenes. También puede determinar qué volúmenes no están montados en un punto de unión.

Esta información se puede usar para comprender y gestionar el espacio de nombres de la SVM.

Pasos

1. Realice la acción deseada:

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

Ejemplos

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

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

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

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

Configurar las asignaciones de nombres

Obtenga más información sobre ONTAP la configuración de las asignaciones de nombres del bloque de mensajes del servidor

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

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

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

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

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

Sin embargo, puede asignar un grupo de usuarios individuales a un usuario específico. Por ejemplo, puede

asignar todos los usuarios de AD que comiencen o terminen con la palabra SALES a un usuario UNIX específico y al UID del usuario.

Obtenga más información sobre la asignación de nombres SMB de ONTAP

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

- Para la asignación de Windows a UNIX

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

- De asignación de UNIX a Windows

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

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

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

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

Obtenga información sobre las búsquedas multidominio de SMB de ONTAP para asignaciones de usuario de UNIX a nombre de usuario de Windows

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

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

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

- *Confianza bidireccional*

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

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

- *Confianza saliente*

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

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

- *Confianza entrante*

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

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

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

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

Patrón	Sustitución	Resultado
raíz	*\\administrador	El usuario UNIX «'root'» está asignado al usuario denominado «'Administrator'». Todos los dominios de confianza se buscan en orden hasta que se encuentre el primer usuario coincidente denominado «'Administrator'».

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

Cómo se realizan las búsquedas de nombres multidominio

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

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

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

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

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

Obtenga más información sobre las reglas de conversión de asignación de nombres SMB de ONTAP

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

Crear asignación de nombres de SMB de ONTAP

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

Acerca de esta tarea

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

Paso

1. Crear una asignación de nombres: `vserver name-mapping create -vserver` *`vserver_name`* `-direction {krb-unix|win-unix|unix-win} -position` *`integer`* `-pattern text -replacement` *`text`*

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

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

Ejemplos

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

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

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

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

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

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

Configure el usuario SMB de ONTAP predeterminado

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

Acerca de esta tarea

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

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

Pasos

1. Ejecute una de las siguientes acciones:

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

Comandos de la ONTAP para gestionar asignaciones de nombre del bloque de mensajes del servidor

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

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

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

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

Configurar las búsquedas de asignación de nombres multidominio

Habilitar o deshabilitar las búsquedas de asignación de nombres multidominio de SMB de ONTAP

Con las búsquedas de asignación de nombres multidominio, puede utilizar una tarjeta comodín (*) en la parte de dominio de un nombre de Windows al configurar la asignación de nombres de usuario de UNIX a Windows. El uso de un comodín (*) en la parte de dominio del nombre permite a ONTAP buscar en todos los dominios que tienen una confianza bidireccional con el dominio que contiene la cuenta de equipo del servidor CIFS.

Acerca de esta tarea

Como alternativa a la búsqueda en todos los dominios de confianza bidireccional, puede configurar una lista de dominios de confianza preferidos. Cuando se configura una lista de dominios de confianza preferidos, ONTAP utiliza la lista de dominios de confianza preferidos en lugar de los dominios de confianza en ambas direcciones detectados para realizar búsquedas de asignación de nombres multidominio.

- Las búsquedas de asignación de nombres multidominio están activadas de manera predeterminada.
- Esta opción está disponible en el nivel de privilegio avanzado.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

Si desea que las búsquedas de asignación de nombres multidominio sean…	Introduzca el comando…
Activado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-trusted-domain-enum -search-enabled true`

Si desea que las búsquedas de asignación de nombres multidominio sean…	Introduzca el comando…
Deshabilitado	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled false`

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

Información relacionada

Opciones de servidor disponibles

Restablece y vuelve a detectar dominios SMB de ONTAP de confianza

Puede forzar la redetección de todos los dominios de confianza. Esto puede ser útil cuando los servidores de dominio de confianza no responden adecuadamente o las relaciones de confianza han cambiado. Solo se detectan los dominios con una confianza bidireccional con el dominio principal, que es el dominio que contiene la cuenta de equipo del servidor CIFS.

Paso

1. Restablezca y vuelva a detectar dominios de confianza mediante el `vserver cifs domain trusts rediscover` comando.

```
vserver cifs domain trusts rediscover -vserver vs1
```

Información relacionada

Muestra información sobre los dominios de confianza detectados

Mostrar información sobre los dominios SMB de ONTAP de confianza detectados

Puede mostrar información acerca de los dominios de confianza detectados para el dominio principal del servidor CIFS, que es el dominio que contiene la cuenta de equipo del servidor CIFS. Esto puede ser útil si desea saber qué dominios de confianza se descubren y cómo se ordenan dentro de la lista de dominios de confianza detectados.

Acerca de esta tarea

Sólo se descubren los dominios con confianzas bidireccionales con el dominio principal. Dado que el controlador de dominio (DC) del dominio principal devuelve la lista de dominios de confianza en un orden determinado por el DC, no se puede predecir el orden de los dominios de la lista. Al mostrar la lista de dominios de confianza, puede determinar el orden de búsqueda para las búsquedas de asignación de nombres multidominio.

La información que se muestra sobre el dominio de confianza se agrupa por nodos y máquina virtual de almacenamiento (SVM).

Paso

1. Muestra información sobre los dominios de confianza detectados mediante `vserver cifs domain trusts show` el comando.

```
vserver cifs domain trusts show -vserver vs1
```

```
   Node: node1
Vserver: vs1

Home Domain             Trusted Domain
---------------------   ----------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM

   Node: node2
Vserver: vs1

Home Domain             Trusted Domain
---------------------   ----------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM
```

Información relacionada

Restablecer y volver a detectar dominios de confianza

Agregue, elimine o reemplace los dominios SMB de confianza de ONTAP en las listas preferidas

Puede agregar o quitar dominios de confianza de la lista de dominios de confianza preferidos para el servidor SMB o puede modificar la lista actual. Si configura una lista de dominios de confianza preferidos, esta lista se utiliza en lugar de los dominios de confianza bidireccionales detectados al realizar búsquedas de asignación de nombres multidominio.

Acerca de esta tarea

- Si va a agregar dominios de confianza a una lista existente, la nueva lista se combina con la lista existente con las nuevas entradas colocadas al final Los dominios de confianza se buscan en el orden en que aparecen en la lista de dominios de confianza.
- Si va a quitar dominios de confianza de la lista existente y no especifica una lista, se elimina toda la lista de dominios de confianza de la máquina virtual de almacenamiento (SVM) especificada.
- Si modifica la lista existente de dominios de confianza, la nueva lista sobrescribe la lista existente.

> Debe introducir solo los dominios de confianza bidireccional en la lista de dominios de confianza preferidos. Aunque puede introducir dominios de confianza de salida o de entrada en la lista de dominios preferidos, no se utilizan al realizar búsquedas de asignación de nombres multidominio. ONTAP omite la entrada para el dominio unidireccional y pasa al siguiente dominio de confianza bidireccional de la lista.

Paso

1. Ejecute una de las siguientes acciones:

Si desea hacer lo siguiente con la lista de dominios de confianza preferidos…	Usar el comando…
Agregar dominios de confianza a la lista	`vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...`
Quitar dominios de confianza de la lista	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`
Modifique la lista existente	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

Ejemplos

El siguiente comando añade dos dominios de confianza (cifs1.example.com y cifs2.example.com) a la lista de dominios de confianza preferida utilizada por SVM vs1:

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

El siguiente comando quita dos dominios de confianza de la lista utilizada por SVM vs1:

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

El siguiente comando modifica la lista de dominios de confianza utilizada por SVM vs1. La nueva lista sustituye a la lista original:

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

Información relacionada

Muestra información sobre la lista de dominios de confianza preferidos

Mostrar información sobre la lista de dominios de confianza de SMB de ONTAP preferida

Puede mostrar información acerca de los dominios de confianza que se encuentran en la lista de dominios de confianza preferidos y el orden en que se realizan búsquedas si las búsquedas de asignación de nombres multidominio están habilitadas. Puede configurar una lista de dominios de confianza preferida como alternativa al uso de la lista de

dominios de confianza detectados automáticamente.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea mostrar información sobre lo siguiente…	Usar el comando…
Todos los dominios de confianza preferidos en el clúster agrupados por máquinas virtuales de almacenamiento (SVM)	`vserver cifs domain name-mapping-search show`
Todos los dominios de confianza preferidos para una SVM especificada	`vserver cifs domain name-mapping-search show -vserver` *`vserver_name`*

El siguiente comando muestra información sobre todos los dominios de confianza preferidos en el clúster:

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver         Trusted Domains
--------------  ---------------------------------
vs1             CIFS1.EXAMPLE.COM
```

Información relacionada

Agregar, eliminar o reemplazar dominios confiables en listas preferidas

Crear y configurar recursos compartidos de SMB

Obtenga más información sobre la creación y configuración de recursos compartidos de SMB de ONTAP

Antes de que los usuarios y las aplicaciones puedan acceder a los datos en el servidor CIFS mediante SMB, debe crear y configurar recursos compartidos de SMB, que es un punto de acceso con nombre en un volumen. Puede personalizar los recursos compartidos especificando parámetros de recurso compartido y propiedades de recurso compartido. Puede modificar un recurso compartido existente en cualquier momento.

Cuando se crea un recurso compartido de SMB, ONTAP crea una ACL predeterminada para el recurso compartido con permisos de control completo para todos.

Los recursos compartidos de SMB están ligados al servidor CIFS en la máquina virtual de almacenamiento (SVM). Los recursos compartidos de SMB se eliminan si la SVM se elimina o el servidor CIFS con el que está asociado se elimina de la SVM. Si vuelve a crear el servidor CIFS en la SVM, debe volver a crear los recursos compartidos SMB.

Información relacionada

- Obtenga información sobre los usuarios y grupos locales
- "Configuración de SMB para Microsoft Hyper-V y SQL Server"

- Configurar la asignación de caracteres para la traducción de nombres de archivos en volúmenes

Obtenga información sobre los recursos compartidos administrativos predeterminados de bloques de mensajes del servidor de ONTAP

Cuando se crea un servidor CIFS en la máquina virtual de almacenamiento (SVM), los recursos compartidos administrativos predeterminados se crean automáticamente. Debe comprender cuáles son esos recursos compartidos predeterminados y cómo se utilizan.

ONTAP crea los siguientes recursos compartidos administrativos predeterminados al crear el servidor CIFS:

> A partir de ONTAP 9.8, el recurso compartido admin$ ya no se crea de forma predeterminada.

- ipc$
- Admin$ (solo ONTAP 9.7 y versiones anteriores)
- r$

Puesto que los recursos compartidos que terminan con el carácter $ son recursos compartidos ocultos, los recursos compartidos administrativos predeterminados no son visibles desde Mi PC, pero puede verlos utilizando carpetas compartidas.

Cómo se utilizan los recursos compartidos predeterminados ipc$ y admin$

Los recursos compartidos ipc$ y admin$ los utilizan ONTAP y los administradores de Windows no pueden utilizarlos para acceder a los datos que residen en la SVM.

- ipc$ share

  el recurso compartido ipc$ es un recurso que comparte las canalizaciones con nombre que son esenciales para la comunicación entre programas. el recurso compartido ipc$ se utiliza durante la administración remota de un equipo y cuando se visualizan los recursos compartidos de un equipo. No puede cambiar la configuración de recursos compartidos, las propiedades de recursos compartidos ni las ACL del recurso compartido ipc$. Tampoco puede cambiar el nombre del recurso compartido ipc$ ni eliminarlo.

- Recurso compartido admin$ (solo ONTAP 9.7 y versiones anteriores)

  > A partir de ONTAP 9.8, el recurso compartido admin$ ya no se crea de forma predeterminada.

  El recurso compartido admin$ se usa durante la administración remota de la SVM. La ruta de este recurso siempre es la ruta al raíz de SVM. No se pueden cambiar las configuraciones de recursos compartidos, las propiedades de recursos compartidos ni las ACL del recurso compartido admin$. Tampoco puede cambiar el nombre del recurso compartido admin$ ni eliminarlo.

Cómo se utiliza el recurso compartido c$ predeterminado

El recurso compartido c$ es un recurso compartido administrativo que puede usar el administrador de clústeres o SVM para acceder al volumen raíz de SVM y administrarlo.

A continuación se muestran las características de la cuota c$:

- La ruta de este recurso compartido siempre es la ruta al volumen raíz de la SVM y no se puede modificar.

- La ACL predeterminada para el recurso compartido c$ es Administrator / Full Control.

  Este usuario es BUILTIN\Administrator. De forma predeterminada, BUILTIN\Administrator puede asignar al recurso compartido y ver, crear, modificar o eliminar archivos y carpetas en el directorio raíz asignado. Se debe tener cuidado al administrar archivos y carpetas en este directorio.

- Es posible cambiar la ACL del recurso compartido de c$.
- Puede cambiar la configuración de c$ share y las propiedades share.
- No se puede eliminar el recurso compartido c$.
- El administrador de SVM puede acceder al resto del espacio de nombres de la SVM desde el recurso compartido c$ asignado cruzando las uniones del espacio de nombres.
- Se puede acceder al recurso compartido c$ mediante Microsoft Management Console.

Información relacionada

Configurar permisos de archivos avanzados mediante la pestaña Seguridad de Windows

Obtenga más información sobre ONTAP los requisitos de nomenclatura para recursos compartidos de bloque de mensajes del servidor

Tenga en cuenta los requisitos de nomenclatura de los recursos compartidos de ONTAP al crear recursos compartidos de SMB en el servidor de SMB.

Las convenciones de nomenclatura de los recursos compartidos para ONTAP son las mismas que para Windows e incluyen los siguientes requisitos:

- El nombre de cada recurso compartido debe ser exclusivo para el servidor SMB.
- Los nombres de recurso compartido no distinguen mayúsculas de minúsculas.
- La longitud máxima del nombre compartido es de 80 caracteres.
- Se admiten los nombres de los recursos compartidos Unicode.
- Los nombres de los recursos compartidos que terminan con el carácter $ son recursos compartidos ocultos.
- Para ONTAP 9.7 y anteriores, los recursos compartidos administrativos admin$, ipc$ y c$ se crean automáticamente en cada servidor CIFS y son nombres de recursos compartidos reservados. A partir de ONTAP 9.8, el recurso compartido admin$ ya no se crea automáticamente.
- No se puede usar el nombre del recurso compartido ONTAP_ADMIN$ al crear un recurso compartido.
- Se admiten los nombres de uso compartido que contienen espacios:
  - No puede utilizar un espacio como primer carácter ni como último carácter en un nombre de recurso compartido.
  - Los nombres de los recursos compartidos deben escribirse entre comillas.

    Las comillas simples se consideran parte del nombre del recurso compartido y no se pueden utilizar en lugar de comillas.

- Los siguientes caracteres especiales se admiten cuando se asigna el nombre a los recursos compartidos de SMB:

```
! @ # $ % & ' _ - . ~ ( ) { }
```

- Los siguientes caracteres especiales no se admiten cuando se asigna el nombre a los recursos compartidos de SMB:

```
** [ ] " / \ : ; | < > , ? * =
```

Obtenga más información sobre los requisitos de sensibilidad de casos del directorio SMB de ONTAP al crear recursos compartidos en un entorno multiprotocolo

Si crea recursos compartidos en una SVM donde se utiliza el esquema de nomenclatura 8.3 para distinguir entre nombres de directorio donde solo hay diferencias de mayúsculas y minúsculas entre los nombres, debe utilizar el nombre 8.3 en la ruta de acceso compartido para garantizar que el cliente se conecte a la ruta de directorio deseada.

En el siguiente ejemplo, se crearon dos directorios llamados "'testdir'" y "'TESTDIR'" en un cliente Linux. La ruta de unión del volumen que contiene los directorios es `/home`. La primera salida es de un cliente Linux y la segunda es de un cliente SMB.

```
 ls -l
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:24 TESTDIR
```

```
dir

 Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

Al crear un recurso compartido en el segundo directorio, debe utilizar el nombre 8.3 en la ruta de acceso al recurso compartido. En este ejemplo, la ruta de acceso de recurso compartido al primer directorio es `/home/testdir` y la ruta de acceso de recurso compartido al segundo directorio es `/home/TESTDI~1`.

Utilizar las propiedades de recursos compartidos de SMB

Obtenga más información sobre el uso de propiedades de recursos compartidos SMB de ONTAP

Puede personalizar las propiedades de los recursos compartidos SMB.

Las propiedades de recursos compartidos disponibles son las siguientes:

Comparta propiedades	Descripción
`oplocks`	Esta propiedad especifica que el recurso compartido utiliza bloqueos oportunistas, también conocidos como almacenamiento en caché en el cliente.
`browsable`	Esta propiedad permite a los clientes de Windows examinar el recurso compartido.
`showsnapshot`	Esta propiedad especifica que los clientes pueden ver y recorrer las instantáneas.
`changenotify`	Esta propiedad especifica que el recurso compartido admite peticiones de notificación de cambio. Para los recursos compartidos en una SVM, esta es una propiedad inicial predeterminada.
`attributecache`	Esta propiedad permite que el atributo de archivo que almacena en caché en el recurso compartido SMB proporcione un acceso más rápido a los atributos. El valor predeterminado es deshabilitar el almacenamiento en caché de atributos. Esta propiedad debe estar habilitada sólo si hay clientes que se conectan a recursos compartidos a través de SMB 1.0. Esta propiedad de recurso compartido no es aplicable si los clientes se conectan a recursos compartidos a través de SMB 2.x o SMB 3.0.
`continuously-available`	Esta propiedad permite a los clientes SMB que lo admiten abrir archivos de una forma persistente. Los archivos abiertos de esta manera están protegidos contra eventos disruptivos, como la conmutación por error y la devolución.
`branchcache`	Esta propiedad especifica que el recurso compartido permite a los clientes solicitar hash de BranchCache en los archivos dentro de este recurso compartido. Esta opción solo es útil si se especifica «'por recurso compartido» como modo operativo en la configuración de BranchCache CIFS.
`access-based-enumeration`	Esta propiedad especifica que *Access Based Enumeration* (ABE) está habilitado en este recurso compartido. Las carpetas compartidas filtradas POR ABE son visibles para un usuario en función de los derechos de acceso de ese usuario individual, lo que impide la visualización de carpetas u otros recursos compartidos a los que el usuario no tiene derechos de acceso.

Comparta propiedades	Descripción
`namespace-caching`	Esta propiedad especifica que los clientes SMB que se conectan a este recurso compartido pueden almacenar en caché los resultados de enumeración de directorios que devuelven los servidores CIFS, lo que puede proporcionar un mejor rendimiento. De forma predeterminada, los clientes de SMB 1 no almacenan en caché los resultados de la enumeración de directorios. Dado que los resultados de enumeración de directorios de caché de los clientes SMB 2 y SMB 3 son los mismos, al especificar esta propiedad de recurso compartido, se proporcionan ventajas de rendimiento solo para las conexiones de cliente SMB 1.
`encrypt-data`	Esta propiedad especifica que se debe utilizar el cifrado SMB al acceder a este recurso compartido. Los clientes de SMB que no admiten cifrado al acceder a los datos de SMB no podrán acceder a este recurso compartido.

Agregue o elimine propiedades de recurso compartido en recursos compartidos SMB de ONTAP existentes

Puede personalizar un recurso compartido SMB existente agregando o quitando propiedades de recurso compartido. Esto puede ser útil para cambiar la configuración de recursos compartidos con el fin de satisfacer los requisitos en constante cambio del entorno.

Antes de empezar

Debe existir el recurso compartido cuyas propiedades desea modificar.

Acerca de esta tarea

Directrices para añadir propiedades de recurso compartido:

- Puede agregar una o más propiedades de recursos compartidos mediante una lista delimitada por comas.
- Todas las propiedades de recurso compartido que haya especificado anteriormente permanecen vigentes.

  Las propiedades recién agregadas se agregan a la lista existente de propiedades de recursos compartidos.

- Si especifica un nuevo valor para las propiedades de recurso compartido que ya se han aplicado al recurso compartido, el valor recién especificado reemplazará al valor original.
- No puede quitar las propiedades de recurso compartido `vserver cifs share properties add` con el comando.

  Puede utilizar el `vserver cifs share properties remove` comando para eliminar propiedades de recurso compartido.

Directrices para eliminar propiedades de recurso compartido:

- Puede quitar una o varias propiedades de recursos compartidos mediante una lista delimitada por comas.
- Las propiedades de recurso compartido que ha especificado previamente pero no las quita permanecen vigentes.

Pasos

1. Introduzca el comando correspondiente:

Si desea…	Introduzca el comando…
Añada propiedades de recurso compartido	`vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`
Quite las propiedades de uso compartido	`vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`

2. Compruebe la configuración de la propiedad de recurso compartido: `vserver cifs share show -vserver vserver_name -share-name share_name`

Ejemplos

El siguiente comando agrega la `showsnapshot` propiedad de recurso compartido a un recurso compartido denominado “hare1” en SVM VS1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share1  /share1   oplocks      -          Everyone / Full
Control
                             browsable
                             changenotify
                             showsnapshot
```

El siguiente comando elimina la `browsable` propiedad de recurso compartido de un recurso compartido denominado «hare2» en SVM VS1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share2  /share2   oplocks      -          Everyone / Full
Control
                             changenotify
```

Información relacionada

Comandos para gestionar recursos compartidos

Optimice el acceso de usuario de SMB de ONTAP con la configuración de recursos compartidos de force-group

Cuando se crea un recurso compartido desde la línea de comandos de ONTAP a datos con seguridad efectiva de UNIX, se puede especificar que todos los archivos creados por los usuarios de SMB en ese recurso compartido pertenecen al mismo grupo, conocido como el *force-group*, que debe ser un grupo predefinido en la base de datos de grupos UNIX. El uso de un grupo de fuerza facilita el acceso de los usuarios SMB que pertenecen a varios grupos a los archivos.

Especificar un grupo de fuerza solo es significativo si el recurso compartido está en un qtree UNIX o mixto. No es necesario establecer un grupo forzado para los recursos compartidos de un volumen NTFS o un qtree ya que el acceso a los archivos de estos recursos compartidos está determinado por permisos de Windows, no por GID de UNIX.

Si se ha especificado un grupo de fuerza para un recurso compartido, lo siguiente se convierte en verdadero del recurso compartido:

- Los usuarios de SMB del grupo de fuerza que acceden a este recurso compartido se cambian temporalmente al GID del grupo de fuerza.

  Este GID permite acceder a los archivos de este recurso compartido a los que no se puede acceder normalmente con su GID o UID principal.

- Todos los archivos de este recurso compartido creados por usuarios SMB pertenecen al mismo grupo de fuerzas, independientemente del GID primario del propietario del archivo.

Cuando los usuarios de SMB intentan acceder a un archivo creado por NFS, los GID principales de los usuarios de SMB determinan los derechos de acceso.

El grupo de fuerza no afecta al modo en que los usuarios NFS acceden a los archivos de este recurso compartido. Un archivo creado por NFS adquiere el GID del propietario del archivo. La determinación de los permisos de acceso se basa en el UID y el GID primario del usuario NFS que intenta acceder al archivo.

El uso de un grupo de fuerza facilita el acceso de los usuarios SMB que pertenecen a varios grupos a los archivos. Por ejemplo, si desea crear un recurso compartido para almacenar las páginas web de la empresa y proporcionar acceso de escritura a los usuarios de los departamentos de Ingeniería y Marketing, puede crear

un recurso compartido y proporcionar acceso de escritura a un grupo de fuerza denominado "'webgroup1'". Debido al grupo de fuerza, todos los archivos creados por los usuarios de SMB en este recurso compartido son propiedad del grupo "'webgroup1'". Además, a los usuarios se les asigna automáticamente el GID del grupo "'webgroup1'" al acceder al recurso compartido. Como resultado, todos los usuarios pueden escribir en este recurso compartido sin necesidad de gestionar los derechos de acceso de los usuarios en los departamentos de ingeniería y marketing.

Información relacionada

Crear recursos compartidos con la configuración de recursos compartidos de grupo forzado

Cree recursos compartidos SMB de ONTAP con la configuración de recursos compartidos force-group

Puede crear un recurso compartido de SMB con la configuración de recurso compartido de grupo forzado si desea que los usuarios de SMB que acceden a datos de volúmenes o qtrees con seguridad de archivos UNIX consideren que ONTAP pertenece al mismo grupo UNIX.

Paso

1. Cree el recurso compartido de SMB: `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path path -force-group-for-create` *`UNIX_group_name`*

   Si la ruta UNC (`\\servername\sharename\filepath`) del recurso compartido contiene más de 256 caracteres (excluyendo el valor inicial`\\` en la ruta UNC), la pestaña **Seguridad** del cuadro Propiedades de Windows no estará disponible. Se trata de un problema del cliente Windows y no de un problema de ONTAP. Para evitar este problema, no cree recursos compartidos con rutas UNC con más de 256 caracteres.

   Si desea quitar el grupo de fuerza después de crear el recurso compartido, puede modificar el recurso compartido en cualquier momento y especificar una cadena vacía como valor para `-force-group-for-create` el parámetro. Si quita el grupo de fuerza modificando el recurso compartido, todas las conexiones existentes a este recurso compartido siguen teniendo el grupo de fuerza establecido anteriormente como GID primario.

Ejemplo

El siguiente comando crea un recurso compartido 'webpages' que es accesible en la web `/corp/companyinfo` en el directorio en el que todos los archivos que los usuarios de SMB crean están asignados al grupo webgroup1:

```
vserver cifs share create -vserver vs1 -share-name webpages -path
/corp/companyinfo -force-group-for-create webgroup1
```

Información relacionada

Optimice el acceso de los usuarios con la configuración de uso compartido de grupo forzado

Ver información sobre recursos compartidos SMB de ONTAP mediante MMC

Puede ver información sobre los recursos compartidos de SMB en la SVM y realizar algunas tareas de gestión con Microsoft Management Console (MMC). Antes de ver los recursos compartidos, tiene que conectar MMC a la SVM.

Acerca de esta tarea

Puede realizar las siguientes tareas en recursos compartidos contenidos en las SVM mediante MMC:

- Ver recursos compartidos
- Ver sesiones activas
- Ver archivos abiertos
- Enumera la lista de sesiones, archivos y conexiones de árbol del sistema
- Cierre los archivos abiertos en el sistema
- Cierre las sesiones abiertas
- Cree/gestione recursos compartidos

> Las vistas que muestran las capacidades anteriores son específicas de los nodos y no del clúster. Por lo tanto, cuando utiliza MMC para conectarse al nombre de host del servidor SMB (es decir, cifs01.domain.local), se le enrutará, en función de cómo haya configurado DNS, a una única LIF dentro del clúster.

MMC para ONTAP no admite las siguientes funciones:

- Creación de nuevos usuarios/grupos locales
- Gestión/visualización de usuarios/grupos locales existentes
- Ver eventos o registros de rendimiento
- Reducida
- Servicios y aplicaciones

En las instancias en las que la operación no es compatible, es posible que se produzcan `remote procedure call failed` errores.

"Preguntas más frecuentes: Uso de MMC de Windows con ONTAP"

Pasos

1. Para abrir la MMC de Administración de equipos en cualquier servidor de Windows, en **Panel de control**, seleccione **Herramientas administrativas** > **Administración de equipos**.
2. Seleccione **Acción** > **conectar a otro ordenador**.

   Aparece el cuadro de diálogo Seleccionar equipo.
3. Escriba el nombre del sistema de almacenamiento o haga clic en **examinar** para buscar el sistema de almacenamiento.
4. Haga clic en **OK**.

   MMC se conecta a SVM.
5. En el panel de navegación, haga clic en **carpetas compartidas** > **recursos compartidos**.

   Se muestra una lista de recursos compartidos de la SVM en el panel de visualización derecho.
6. Para mostrar las propiedades de uso compartido de un recurso compartido, haga doble clic en él para abrir el cuadro de diálogo **Propiedades**.
7. Si no puede conectarse al sistema de almacenamiento mediante MMC, puede agregar al usuario al grupo

BUILTIN\Administrators o BUILTIN\Power Users mediante uno de los siguientes comandos del sistema de almacenamiento:

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

Comandos de ONTAP para gestionar recursos compartidos de SMB

Se deben usar `vserver cifs share` `vserver cifs share properties` los comandos y para gestionar recursos compartidos de SMB.

Si desea…	Se usa este comando…
Cree un recurso compartido de SMB	`vserver cifs share create`
Mostrar los recursos compartidos de SMB	`vserver cifs share show`
Modificar un recurso compartido de SMB	`vserver cifs share modify`
Eliminar un recurso compartido de SMB	`vserver cifs share delete`
Agregar propiedades de recurso compartido a un recurso compartido existente	`vserver cifs share properties add`
Quitar propiedades de recurso compartido de un recurso compartido existente	`vserver cifs share properties remove`
Muestra información sobre las propiedades de uso compartido	`vserver cifs share properties show`

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

Acceso seguro a archivos mediante ACL de uso compartido de SMB

Obtenga más información sobre la gestión de ACL de nivel de recurso compartido de bloque de mensajes del servidor de ONTAP

Puede cambiar las ACL de nivel compartido para otorgar a los usuarios más o menos derechos de acceso al recurso compartido. Puede configurar ACL de nivel compartido usando usuarios y grupos de Windows o usuarios y grupos de UNIX.

De forma predeterminada, la ACL de nivel de recurso compartido proporciona un control total al grupo estándar denominado Everyone. El control total en la ACL significa que todos los usuarios en el dominio y

todos los dominios de confianza tienen acceso completo al recurso compartido. Puede controlar el nivel de acceso a una ACL de nivel de recurso compartido mediante Microsoft Management Console (MMC) en un cliente Windows o la línea de comandos de ONTAP. "Crear listas de control de acceso a recursos compartidos".

Las siguientes directrices se aplican cuando se utiliza MMC:

- Los nombres de usuario y de grupo especificados deben ser nombres de Windows.
- Sólo puede especificar permisos de Windows.

Cuando se utiliza la línea de comandos de ONTAP, se aplican las siguientes directrices:

- Los nombres de usuario y de grupo especificados pueden ser nombres de Windows o nombres UNIX.

  Si no se especifica un tipo de usuario y grupo al crear o modificar ACL, el tipo predeterminado es usuarios y grupos de Windows.

- Sólo puede especificar permisos de Windows.

Cree listas de control de acceso compartido de SMB de ONTAP

La configuración de permisos de uso compartido mediante la creación de listas de control de acceso (ACL) para recursos compartidos de SMB permite controlar el nivel de acceso a un recurso compartido para usuarios y grupos.

Acerca de esta tarea

Puede configurar ACL de nivel compartido utilizando nombres de usuarios o grupos locales o de dominio de Windows o nombres de usuarios o grupos de UNIX.

Antes de crear una nueva ACL, debe suprimir la ACL de recurso compartido por defecto `Everyone / Full Control` , que representa un riesgo de seguridad.

En modo de grupo de trabajo, el nombre de dominio local es el nombre del servidor SMB.

Pasos

1. Elimine la ACL predeterminada para compartir:`Vserver cifs share access-control delete -vserver <vserver_name> -share <share_name> -user-or-group everyone`
2. Configure la nueva ACL:

Si desea configurar las ACL utilizando…	Introduzca el comando…
Usuario de Windows	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\user_name> -permission <access_right>`

Si desea configurar las ACL utilizando…	Introduzca el comando…
Grupo Windows	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\group_name> -permission <access_right>`
Usuario UNIX	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-user> -user-or-group <UNIX_user_name> -permission <access_right>`
Grupo UNIX	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-group> -user-or-group <UNIX_group_name> -permission <access_right>`

3. Verifique que la ACL aplicada al recurso compartido es correcta mediante `vserver cifs share access-control show` el comando.

Ejemplo

El siguiente comando otorga `Change` permisos al grupo de Windows “Equipo de ventas” para el recurso compartido “ventas” en la SVM “vs1.example.com”:

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
Permission
--------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\Sales Team     windows     Change
```

El siguiente comando `Read` otorga permiso al grupo UNIX «engineering» para el recurso compartido «eng» en la SVM «vs2.example.com»:

```
cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                Share       User/Group               User/Group  Access
Vserver         Name        Name                     Type
Permission
--------------- ----------- -------------------      -----------
-----------
vs2.example.com  c$         BUILTIN\Administrators   windows
Full_Control
vs2.example.com  eng        engineering              unix-group  Read
```

Los siguientes comandos dan `Change` permiso al grupo local de Windows denominado «Tiger Team» y `Full_Control` permiso al usuario local de Windows denominado «Sue Chang» para el recurso compartido «datavol5» en la SVM «VS1»:

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    Tiger Team         windows     Change
vs1            datavol5    Sue Chang          windows     Full_Control
```

Comandos ONTAP para administrar listas de control de acceso a recursos compartidos SMB

Debe conocer los comandos para gestionar las listas de control de acceso (ACL) de SMB, lo que incluye crear, mostrar, modificar y eliminar dichas listas.

Si desea…	Se usa este comando…
Cree una nueva ACL	`vserver cifs share access-control create`
Mostrar ACL	`vserver cifs share access-control show`
Modificar una ACL	`vserver cifs share access-control modify`
Eliminar una ACL	`vserver cifs share access-control delete`

Acceso seguro a archivos mediante permisos de archivo

Configurar permisos avanzados de archivos NTFS mediante la pestaña Seguridad de Windows para SVM SMB de ONTAP

Puede configurar permisos de archivo NTFS estándar en archivos y carpetas mediante la ficha **Seguridad de Windows** de la ventana Propiedades de Windows.

Antes de empezar

El administrador que realiza esta tarea debe tener suficientes permisos NTFS para cambiar los permisos en los objetos seleccionados.

Acerca de esta tarea

La configuración de los permisos de archivo NTFS se realiza en un host de Windows agregando entradas a las listas de control de acceso discrecional NTFS (DACL) asociadas con un descriptor de seguridad NTFS. El descriptor de seguridad se aplica entonces a los archivos y directorios NTFS. La interfaz gráfica de usuario de Windows se encarga automáticamente de estas tareas.

Pasos

1. En el menú **Herramientas** del Explorador de Windows, seleccione **asignar unidad de red**.
2. Complete el cuadro de diálogo **asignar unidad de red**:

   a. Seleccione una letra **Unidad**.

   b. En el cuadro **Folder**, escriba el nombre del servidor CIFS que contiene el recurso compartido que contiene los datos a los que desea aplicar los permisos y el nombre del recurso compartido.

      Si el nombre de su servidor CIFS es "CIFS_SERVER’ y su recurso compartido se llama "hare1", debe escribir `\\CIFS_SERVER\share1`.

      Puede especificar la dirección IP de la interfaz de datos para el servidor CIFS en lugar del nombre del servidor CIFS.

   c. Haga clic en **Finalizar**.

   La unidad seleccionada está montada y lista con la ventana del Explorador de Windows que muestra archivos y carpetas contenidos en el recurso compartido.

3. Seleccione el archivo o directorio para el que desea establecer los permisos de archivo NTFS.
4. Haga clic con el botón secundario del ratón en el archivo o directorio y seleccione **Propiedades**.
5. Seleccione la ficha **Seguridad**.

   La ficha **Seguridad** muestra la lista de usuarios y grupos para los que se ha establecido el permiso NTFS. El cuadro **permisos para** muestra una lista de permisos permitir y denegar que están en vigor para cada usuario o grupo seleccionado.

6. Haga clic en **Avanzado**.

   La ventana Propiedades de Windows muestra información sobre los permisos de archivo existentes asignados a usuarios y grupos.

7. Haga clic en **Cambiar permisos**.

   Se abrirá la ventana permisos.

8. Realice las acciones deseadas:

Si desea…	Haga lo siguiente…
Configure permisos NTFS avanzados para un nuevo usuario o grupo	a. Haga clic en **Agregar**. b. En el cuadro **Escriba el nombre del objeto que desea seleccionar** , escriba el nombre del usuario o grupo que desea agregar. c. Haga clic en **OK**.
Cambiar los permisos NTFS avanzados de un usuario o grupo	a. En el cuadro **permisos de entrada:** , seleccione el usuario o grupo cuyos permisos avanzados desea cambiar. b. Haga clic en **Editar**.
Quitar permisos NTFS avanzados para un usuario o grupo	a. En el cuadro **Entradas de permisos:** , seleccione el usuario o grupo que desea quitar. b. Haga clic en **Quitar**. c. Vaya al paso 13.

   Si va a agregar permisos NTFS avanzados en un nuevo usuario o grupo o si va a cambiar los permisos avanzados de NTFS en un usuario o grupo existente, se abrirá el cuadro Entrada de permisos para <Object> .

9. En el cuadro **aplicar a**, seleccione cómo desea aplicar esta entrada de permiso de archivo NTFS.

   Si está configurando permisos de archivo NTFS en un solo archivo, el cuadro **aplicar a** no está activo. El valor **aplicar a** se establece de forma predeterminada en **este objeto sólo**.

10. En el cuadro **permisos** , seleccione los cuadros **permitir** o **Denegar** para los permisos avanzados que desea establecer en este objeto.

    ◦ Para permitir el acceso especificado, seleccione el cuadro **permitir**.

- Para no permitir el acceso especificado, seleccione el cuadro **Denegar**. Puede establecer permisos en los siguientes derechos avanzados:
- **Control total**

  Si elige este derecho avanzado, todos los demás derechos avanzados se seleccionan automáticamente (permitir o denegar derechos).

- **Carpeta Traverse / archivo de ejecución**
- **Lista de carpetas / lectura de datos**
- **Leer atributos**
- **Leer atributos extendidos**
- **Crear archivos / escribir datos**
- **Crear carpetas / anexar datos**
- **Escribir atributos**
- **Escriba atributos extendidos**
- **Eliminar subcarpetas y archivos**
- **Eliminar**
- **Leer permisos**
- **Cambiar permisos**
- **Tome la propiedad**

  Si alguno de los cuadros de permisos avanzados no se puede seleccionar, se debe a que los permisos se heredan del objeto primario.

11. Si desea que las subcarpetas y los archivos de este objeto hereden estos permisos, seleccione la casilla **aplicar estos permisos a objetos y/o contenedores dentro de este contenedor únicamente**.
12. Haga clic en **OK**.
13. Después de terminar de agregar, quitar o editar permisos NTFS, especifique la configuración de herencia para este objeto:

    - Seleccione el cuadro **incluir permisos heredables del primario de este objeto**.

      Este es el valor predeterminado.

    - Seleccione el cuadro **Reemplazar todos los permisos de objeto secundario con permisos heredables de este objeto** .

      Esta configuración no está presente en el cuadro permisos si está estableciendo permisos de archivo NTFS en un solo archivo.

Tenga cuidado al seleccionar este ajuste. Esta configuración quita todos los permisos existentes en todos los objetos secundarios y los reemplaza con la configuración de permisos de este objeto. Podría quitar sin darse cuenta los permisos que no desea quitar. Especialmente importante cuando se configuran permisos en un volumen o un qtree de estilo de seguridad mixto. Si los objetos secundarios tienen un estilo de seguridad efectivo de UNIX, al propagar los permisos NTFS a esos objetos secundarios, ONTAP cambia estos objetos del estilo de seguridad de UNIX al estilo de seguridad NTFS y todos los permisos de UNIX de esos objetos secundarios se sustituyen por permisos NTFS.

- Seleccione ambas casillas.
- Seleccione ninguna casilla.

14. Haga clic en **Aceptar** para cerrar el cuadro **permisos**.
15. Haga clic en **Aceptar** para cerrar el cuadro **Configuración avanzada de seguridad para <Object>**.

Para obtener más información acerca de cómo establecer permisos NTFS avanzados, consulte la documentación de Windows.

Información relacionada

- Crear descriptores de seguridad NTFS en servidores
- Muestra información sobre la seguridad de archivos en volúmenes de estilo de seguridad NTFS
- Muestra información sobre la seguridad de archivos en volúmenes mixtos de estilo de seguridad
- Muestra información sobre la seguridad de archivos en volúmenes de estilo de seguridad UNIX

Comandos ONTAP para permisos de archivos SMB NTFS

Puede configurar los permisos de archivo NTFS en archivos y directorios mediante la interfaz de línea de comandos de ONTAP. Esto le permite configurar permisos de archivo NTFS sin necesidad de conectarse a los datos mediante un recurso compartido SMB en un cliente Windows.

Puede configurar los permisos de archivo NTFS agregando entradas a las listas de control de acceso discrecional (DACL) de NTFS que están asociadas con un descriptor de seguridad de NTFS. El descriptor de seguridad se aplica entonces a los archivos y directorios NTFS.

Sólo puede configurar permisos de archivo NTFS mediante la línea de comandos. No puede configurar las ACL de NFSv4 mediante la CLI.

Pasos

1. Cree un descriptor de seguridad NTFS.

```
vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
ntfs_security_descriptor_name -owner owner_name -group primary_group_name
-control-flags-raw raw_control_flags
```

2. Agregue DACL al descriptor de seguridad NTFS.

```
vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
-rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
```

```
{this-folder|sub-folders|files}
```

3. Cree una directiva de seguridad de archivos/directorios.

```
vserver security file-directory policy create -vserver svm_name -policy-name
policy_name
```

Obtenga información sobre los permisos de archivos UNIX que brindan control de acceso al acceder a archivos a través de servidores SMB de ONTAP

Un volumen FlexVol puede tener uno de los tres tipos de estilo de seguridad: NTFS, UNIX o mixto. Es posible acceder a los datos a través de SMB independientemente del estilo de seguridad; no obstante, se necesitan permisos adecuados de archivos UNIX para acceder a los datos con una seguridad efectiva de UNIX.

Cuando se accede a los datos a través de SMB, existen varios controles de acceso que se utilizan para determinar si un usuario está autorizado a realizar una acción solicitada:

- Permisos de exportación

  La configuración de los permisos de exportación para el acceso SMB es opcional.

- Comparta los permisos
- Permisos de archivo

  Los siguientes tipos de permisos de archivo se pueden aplicar a los datos en los que el usuario desea realizar una acción:

  - NTFS
  - ACL de UNIX NFSv4
  - Bits de modo UNIX

En el caso de los datos con ACL de NFSv4 o conjuntos de bits de modo UNIX, se utilizan permisos de estilo UNIX para determinar los derechos de acceso a los archivos de los datos. El administrador de SVM debe establecer el permiso de archivo adecuado para garantizar que los usuarios tienen derechos para realizar la acción deseada.

> Los datos de un volumen de estilo de seguridad mixto pueden tener un estilo de seguridad efectivo NTFS o UNIX. Si los datos tienen un estilo de seguridad efectivo de UNIX, se utilizan los permisos de NFSv4 o bits de modo UNIX al determinar los derechos de acceso a los datos.

Acceso seguro a archivos mediante control de acceso dinámico (DAC)

Obtenga información sobre la seguridad del acceso a archivos DAC para servidores SMB de ONTAP

Puede proteger el acceso mediante el control de acceso dinámico y mediante la creación de directivas de acceso central en Active Directory y su aplicación a archivos y carpetas en las SVM mediante objetos de directiva de grupo aplicados (GPO). Puede configurar la auditoría para utilizar los eventos de configuración de directivas de acceso central para ver los efectos de los cambios en las directivas de acceso central antes de aplicarlas.

Adiciones a las credenciales CIFS

Antes del control dinámico de acceso, una credencial CIFS incluía la identidad de los principales de seguridad (el usuario) y la pertenencia al grupo Windows. Con el control dinámico de acceso, se agregan tres tipos más de información a la credencial: Identidad del dispositivo, reclamos del dispositivo y reclamos del usuario:

- Identidad del dispositivo

  El análogo de la información de identidad del usuario, excepto que es la identidad y pertenencia de grupo del dispositivo desde el que el usuario inicia sesión.

- Reclamaciones de dispositivos

  Afirmaciones acerca de una entidad de seguridad del dispositivo. Por ejemplo, una reclamación de dispositivo podría ser que es miembro de una unidad organizativa específica.

- Reclamaciones del usuario

  Afirmaciones acerca de una entidad de seguridad de usuario. Por ejemplo, una reclamación de usuario podría ser que su cuenta AD es miembro de una unidad organizativa específica.

Políticas de acceso central

Las políticas de acceso central para archivos permiten a las organizaciones implementar y administrar de forma centralizada políticas de autorización que incluyen expresiones condicionales mediante grupos de usuarios, reclamaciones de usuarios, reclamaciones de dispositivos y propiedades de recursos.

Por ejemplo, para acceder a datos de alto impacto empresarial, un usuario necesita ser un empleado a tiempo completo y solo tener acceso a los datos desde un dispositivo gestionado. Las directivas de acceso central se definen en Active Directory y se distribuyen a servidores de archivos mediante el mecanismo GPO.

Configuración de directivas de acceso central con auditoría avanzada

Las políticas centrales de acceso pueden ser «más favorables», en cuyo caso se evalúan de forma «qué sucede si» durante los controles de acceso a los archivos. Los resultados de lo que habría ocurrido si la directiva estaba en vigor y cómo difiere de lo que está configurado actualmente se registran como un evento de auditoría. De esta forma, los administradores pueden utilizar registros de eventos de auditoría para estudiar el impacto de un cambio de directiva de acceso antes de poner la directiva en juego. Tras evaluar el impacto de un cambio de política de acceso, la política se puede implementar a través de GPO en las SVM deseadas.

Información relacionada

- Obtenga más información sobre los GPO compatibles
- Obtenga información sobre cómo aplicar objetos de directiva de grupo a servidores SMB
- Habilitar o deshabilitar la compatibilidad con GPO en los servidores
- Mostrar información acerca de las configuraciones de GPO
- Muestra información sobre las políticas de acceso central
- Muestra información acerca de las reglas de la política de acceso central
- Configurar políticas de acceso central para proteger los datos en los servidores
- Mostrar información sobre la seguridad de los servidores
- "Seguimiento de seguridad y auditoría de SMB y NFS"

Funcionalidad DAC compatible con servidores SMB de ONTAP

Si desea utilizar el control de acceso dinámico (DAC) en un servidor CIFS, debe comprender cómo ONTAP admite la funcionalidad de control de acceso dinámico en entornos Active Directory.

Compatible con el control de acceso dinámico

ONTAP admite la siguiente funcionalidad cuando está habilitado el control de acceso dinámico en el servidor CIFS:

Funcionalidad	Comentarios
Reclamaciones en el sistema de archivos	Las reclamaciones son pares simples de nombre y valor que indican cierta verdad acerca de un usuario. Las credenciales de usuario contienen información de reclamación y los descriptores de seguridad de los archivos pueden realizar comprobaciones de acceso que incluyen comprobaciones de reclamaciones. De este modo, los administradores disponen de un mayor nivel de control sobre quién puede acceder a los archivos.
Expresiones condicionales para comprobaciones de acceso a archivos	Al modificar los parámetros de seguridad de un archivo, los usuarios pueden agregar expresiones condicionales arbitrariamente complejas al descriptor de seguridad del archivo. La expresión condicional puede incluir comprobaciones para las reclamaciones.
Control centralizado de acceso a ficheros mediante directivas de acceso central	Las directivas de acceso central son un tipo de ACL almacenadas en Active Directory que se pueden etiquetar a un archivo. El acceso al archivo sólo se concede si el acceso comprueba tanto el descriptor de seguridad del disco como la directiva de acceso central etiquetada permiten el acceso.esto proporciona a los administradores la capacidad de controlar el acceso a los archivos desde una ubicación central (AD) sin tener que modificar el descriptor de seguridad del disco.
Configuración de políticas de acceso central	Agrega la capacidad de probar los cambios de seguridad sin afectar el acceso real a los archivos, mediante un «envejecimiento» de las políticas de acceso centrales y viendo el efecto del cambio en un informe de auditoría.
Soporte para mostrar información sobre la seguridad de las políticas de acceso central mediante la interfaz de línea de comandos de ONTAP	Amplía el `vserver security file-directory show` comando para mostrar información sobre las políticas de acceso central aplicadas.

Funcionalidad	Comentarios
Seguimiento de la seguridad que incluye políticas de acceso central	Amplía `vserver security trace` la familia de comandos para mostrar los resultados que incluyen información sobre las políticas de acceso central aplicadas.

No compatible con el control de acceso dinámico

ONTAP no admite la siguiente funcionalidad cuando el control de acceso dinámico está habilitado en el servidor CIFS:

Funcionalidad	Comentarios
Clasificación automática de objetos del sistema de archivos NTFS	Esta es una extensión de la infraestructura de clasificación de archivos de Windows que no se admite en ONTAP.
Auditoría avanzada que no sea la configuración de políticas de acceso central	Sólo se admite la configuración de directivas de acceso central para la auditoría avanzada.

Aprenda a usar DAC y políticas de acceso central con servidores SMB de ONTAP

Hay ciertas consideraciones que debe tener en cuenta al utilizar el control de acceso dinámico (DAC) y las políticas de acceso central para proteger los archivos y las carpetas en los servidores CIFS.

Se puede denegar el acceso NFS a la raíz si la regla de directiva se aplica al usuario de dominio\administrador

En determinadas circunstancias, puede denegarse el acceso NFS a root cuando se aplica la seguridad de la política de acceso central a los datos a los que el usuario raíz intenta acceder. El problema se produce cuando la directiva de acceso central contiene una regla que se aplica al dominio\administrador y la cuenta raíz se asigna a la cuenta de dominio\administrador.

En lugar de aplicar una regla al usuario de dominio\administrador, debe aplicar la regla a un grupo con privilegios administrativos, como el dominio\grupo de administradores. De esta forma, puede asignar root a la cuenta de dominio\administrador sin que este problema afecte a root.

El grupo BUILTIN\Administrators del servidor CIFS tiene acceso a los recursos cuando la directiva de acceso central aplicada no se encuentra en Active Directory

Es posible que los recursos contenidos en el servidor CIFS tengan políticas de acceso central aplicadas a ellos, pero cuando el servidor CIFS usa el SID de la política de acceso central para intentar recuperar información de Active Directory, el SID no coincide con ningún SID de política de acceso central existente en Active Directory. En estas circunstancias, el servidor CIFS aplica la política de recuperación predeterminada local para ese recurso.

La directiva de recuperación predeterminada local permite el acceso de grupo BUILTIN\Administrators del servidor CIFS a ese recurso.

Habilitar o deshabilitar DAC para servidores SMB de ONTAP

La opción que permite utilizar el control de acceso dinámico (DAC) para proteger objetos en el servidor CIFS está deshabilitada de forma predeterminada. Debe habilitar la opción si desea utilizar el control de acceso dinámico en el servidor CIFS. Si más adelante decide que no desea utilizar el control de acceso dinámico para proteger los objetos almacenados en el servidor CIFS, puede deshabilitar la opción.

Puede encontrar información acerca de cómo configurar el control de acceso dinámico en Active Directory en la biblioteca de Microsoft TechNet.

"Microsoft TechNet: Información general sobre el escenario de control de acceso dinámico"

Acerca de esta tarea

Una vez que el control de acceso dinámico está activado, el sistema de archivos puede contener ACL con entradas relacionadas con el control de acceso dinámico. Si el control de acceso dinámico está desactivado, se ignorarán las entradas actuales del control de acceso dinámico y no se permitirán las nuevas.

Esta opción solo está disponible en el nivel de privilegios avanzado.

Paso

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

Si desea que el control de acceso dinámico sea…	Introduzca el comando…
Activado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled true`
Deshabilitado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled false`

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

Información relacionada

Configurar políticas de acceso central para proteger los datos en los servidores

Administrar ACL que contienen ACE de DAC cuando DAC está deshabilitado en servidores SMB de ONTAP

Si tiene recursos que tienen ACL aplicados a ACE de control de acceso dinámico y deshabilita el control de acceso dinámico en la máquina virtual de almacenamiento (SVM), debe quitar las ACE de control de acceso dinámico antes de poder gestionar las ACE que no son de control de acceso dinámico en ese recurso.

Acerca de esta tarea

Una vez que el control dinámico de acceso está desactivado, no puede quitar los ACE de control de acceso no dinámico existentes ni agregar nuevos ACE de control de acceso no dinámico hasta que haya eliminado los ACE de control dinámico de acceso existentes.

Puede utilizar cualquier herramienta que utilice normalmente para administrar ACL para realizar estos pasos.

Pasos

1. Determine qué ACE de control dinámico de acceso se aplican al recurso.
2. Quite los ACE de control de acceso dinámico del recurso.
3. Agregue o quite ACE de control de acceso no dinámico según lo desee del recurso.

Configurar políticas de acceso central para proteger los datos en los servidores SMB de ONTAP

Hay varios pasos que debe dar para garantizar el acceso seguro a los datos en el servidor CIFS mediante políticas de acceso centrales, incluida la habilitación del control de acceso dinámico (DAC) en el servidor CIFS, la configuración de políticas de acceso centrales en Active Directory y la aplicación de las políticas de acceso centrales a los contenedores de Active Directory con GPO, Y habilitar los GPO en el servidor CIFS.

Antes de empezar

- Active Directory debe estar configurado para utilizar las directivas de acceso central.
- Debe tener suficiente acceso en los controladores de dominio de Active Directory para crear políticas de acceso centrales y crear y aplicar GPO a los contenedores que contienen los servidores CIFS.
- Debe tener suficiente acceso administrativo en la máquina virtual de almacenamiento (SVM) para ejecutar los comandos necesarios.

Acerca de esta tarea

Las directivas de acceso central se definen y aplican a los objetos de directiva de grupo (GPO) en Active Directory. Puede encontrar información acerca de cómo configurar las políticas de acceso central en Active Directory en la biblioteca de Microsoft TechNet.

"Microsoft TechNet: Escenario de política de acceso central"

Pasos

1. Habilite el control de acceso dinámico en la SVM si todavía no se habilita mediante `vserver cifs options modify` el comando.

   ```
   vserver cifs options modify -vserver vs1 -is-dac-enabled true
   ```

2. Habilite los objetos de política de grupo (GPO) en el servidor CIFS si aún no se han habilitado mediante `vserver cifs group-policy modify` el comando.

   ```
   vserver cifs group-policy modify -vserver vs1 -status enabled
   ```

3. Crear reglas de acceso central y políticas de acceso central en Active Directory.
4. Cree un objeto de directiva de grupo (GPO) para implementar las directivas de acceso central en Active Directory.
5. Aplique el GPO al contenedor donde se encuentra la cuenta de equipo servidor CIFS.
6. Actualice manualmente los objetos de normativa de grupo aplicados al servidor CIFS mediante `vserver cifs group-policy update` el comando.

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. Compruebe que la política de acceso central de GPO se aplica a los recursos del servidor CIFS mediante `vserver cifs group-policy show-applied` el comando.

   El siguiente ejemplo muestra que la política de dominio predeterminada tiene dos políticas de acceso centrales que se aplican al servidor CIFS:

   `vserver cifs group-policy show-applied`

```
Vserver: vs1
----------------------------
    GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
```

```
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2

    GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
2 entries were displayed.
```

Información relacionada

- Obtenga información sobre cómo aplicar objetos de directiva de grupo a servidores SMB
- Mostrar información acerca de las configuraciones de GPO
- Muestra información sobre las políticas de acceso central
- Muestra información acerca de las reglas de la política de acceso central
- Habilitar o deshabilitar DAC para servidores

Mostrar información sobre la seguridad de DAC para servidores SMB de ONTAP

Puede mostrar información acerca de la seguridad DAC (Dynamic Access Control) en volúmenes NTFS y en datos con seguridad efectiva NTFS en volúmenes mixtos de estilo de seguridad. Esto incluye información sobre ACE condicionales, ACE de recursos y ACE de políticas de acceso central. Puede utilizar los resultados para validar la configuración de seguridad o solucionar problemas de acceso a archivos.

Acerca de esta tarea

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los datos cuya información de seguridad de archivo o carpeta desee mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

Paso

1. Mostrar la configuración de seguridad de archivos y directorios con el nivel de detalle deseado:

Si desea mostrar información…	Introduzca el siguiente comando…
En forma de resumen	`vserver security file-directory show -vserver vserver_name -path path`
Con detalle ampliado	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
Donde se muestra la salida con los SID de grupo y usuario	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
Acerca de la seguridad de archivos y directorios para archivos y directorios en los que la máscara de bits hexadecimal se traduce al formato de texto	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

Ejemplos

En el siguiente ejemplo, se muestra información de seguridad de Control de acceso dinámico sobre la ruta de `/vol1` SVM VS1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                           Vserver: vs1
                         File Path: /vol1
                File Inode Number: 112
                   Security Style: mixed
                  Effective Style: ntfs
                   DOS Attributes: 10
           DOS Attributes in Text: ----D---
           Expanded Dos Attribute: -
                     Unix User Id: 0
                    Unix Group Id: 1
                   Unix Mode Bits: 777
           Unix Mode Bits in Text: rwxrwxrwx
                             ACLs: NTFS Security Descriptor
                                   Control:0xbf14
                                   Owner:CIFS1\Administrator
                                   Group:CIFS1\Domain Admins
                                   SACL - ACEs
                                      ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                      RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                      POLICY ID-All resources - No Write-
0x0-OI|CI
                                   DACL - ACEs
                                      ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                      ALLOW-Everyone-0x1f01ff-OI|CI
                                      ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

Información relacionada

- Mostrar información acerca de las configuraciones de GPO
- Muestra información sobre las políticas de acceso central
- Muestra información acerca de las reglas de la política de acceso central

Consideraciones de reversión para DAC en servidores SMB de ONTAP

Debe ser consciente de lo que sucede al volver a una versión de ONTAP que no admite el control de acceso dinámico (DAC) y lo que debe hacer antes y después de revertir.

Si desea revertir el clúster a una versión de ONTAP que no admite el control de acceso dinámico y que el

control de acceso dinámico está habilitado en una o varias máquinas virtuales de almacenamiento (SVM), debe hacer lo siguiente antes de revertir:

- Debe deshabilitar el control de acceso dinámico en todas las SVM que tengan habilitado en el clúster.
- Debe modificar cualquier configuración de auditoría del clúster que contenga el `cap-staging` tipo de evento para utilizar solo el `file-op` tipo de evento.

Debe comprender y actuar sobre algunas consideraciones importantes de reversión para archivos y carpetas con los ACE de control de acceso dinámico:

- Si se revierte el clúster, los ACE existentes de Dynamic Access Control no se eliminan; sin embargo, se ignorarán en las comprobaciones de acceso a archivos.
- Dado que los ACE de control de acceso dinámico se ignoran después de la nueva versión, el acceso a los archivos cambiará en archivos con ACE de control de acceso dinámico.

  Esto podría permitir a los usuarios acceder a los archivos que no podían obtener anteriormente o no tener acceso a los que podían acceder anteriormente.

- Debería aplicar ACE de control de acceso no dinámico a los archivos afectados para restaurar su nivel anterior de seguridad.

  Esto puede hacerse antes de revertir o inmediatamente después de que finaliza la reversión.

> Puesto que los ACE de control dinámico de acceso se ignoran después de volver a verlos, no es necesario eliminarlos cuando se aplican los ACE de control de acceso no dinámico a los archivos afectados. Sin embargo, si lo desea, puede eliminarlos manualmente.

Acceso seguro a SMB mediante políticas de exportación

Aprenda a usar políticas de exportación con el acceso SMB de ONTAP

Si se habilitan las políticas de exportación para el acceso de SMB en el servidor SMB, se utilizan las políticas de exportación cuando se controla el acceso a los volúmenes de SVM mediante clientes SMB. Para acceder a los datos, puede crear una política de exportación que permita el acceso a SMB y, a continuación, asociar la política con los volúmenes que contienen recursos compartidos de SMB.

Una política de exportación tiene una o varias reglas que se le aplican para especificar qué clientes pueden acceder a los datos y qué protocolos de autenticación son compatibles con el acceso de solo lectura y de lectura y escritura. Puede configurar directivas de exportación para permitir el acceso a través de SMB a todos los clientes, a una subred de clientes o a un cliente específico y para permitir la autenticación mediante autenticación Kerberos, autenticación NTLM o autenticación Kerberos y NTLM al determinar el acceso de sólo lectura y escritura a los datos.

Tras procesar todas las reglas de exportación aplicadas a la política de exportación, ONTAP puede determinar si el cliente obtiene acceso y qué nivel de acceso se concede. Las reglas de exportación se aplican a los equipos cliente, no a los usuarios y grupos de Windows. Las reglas de exportación no reemplazan la autenticación y autorización basada en usuarios y grupos de Windows. Las reglas de exportación proporcionan otra capa de seguridad de acceso, además de permisos de uso compartido y acceso a archivos.

Se asocia exactamente una política de exportación a cada volumen para configurar el acceso de los clientes al volumen. Cada SVM puede contener varias políticas de exportación. Esto le permite hacer lo siguiente para

las SVM con varios volúmenes:

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

Cada SVM tiene, como mínimo, una política de exportación denominada «default», que no contiene reglas. No puede eliminar esta política de exportación, pero puede cambiarla ni cambiar el nombre. Cada volumen de la SVM está asociado de forma predeterminada con la política de exportación predeterminada. Si en la SVM se deshabilitan las políticas de exportación de acceso SMB, la política de exportación «predeterminado» no tendrá efecto en el acceso de las pymes.

Puede configurar reglas que proporcionen acceso a los hosts NFS y SMB y asociarlos con una política de exportación, que se puede asociar al volumen que contiene datos a los que necesitan acceder los hosts NFS y SMB. De forma alternativa, si hay algunos volúmenes en los que solo los clientes SMB necesitan acceso, puede configurar una directiva de exportación con reglas que solo permitan el acceso mediante el protocolo SMB y que sólo utilice Kerberos o NTLM (o ambos) para la autenticación de solo lectura y acceso de escritura. La política de exportación se asocia entonces a los volúmenes en los que solo se desea acceso a SMB.

Si se habilitan las políticas de exportación de SMB y un cliente realiza una solicitud de acceso que no permite la política de exportación correspondiente, la solicitud genera un mensaje de permiso denegado. Si un cliente no coincide con ninguna regla de la política de exportación del volumen, se deniega el acceso. Si una política de exportación está vacía, se deniegan implícitamente todos los accesos. Esto es cierto incluso si los permisos de recurso compartido y archivo de lo contrario permitirían el acceso. Esto significa que debe configurar la política de exportación para permitir, como mínimo, el siguiente valor en los volúmenes que contengan recursos compartidos de SMB:

- Permitir el acceso a todos los clientes o al subconjunto apropiado de clientes
- Permitir el acceso a través de SMB
- Permitir el acceso de sólo lectura y escritura adecuado mediante autenticación Kerberos o NTLM (o ambos)

Obtenga más información "configuración y gestión de políticas de exportación"sobre .

Conozca las reglas de exportación de SMB de ONTAP

Las reglas de exportación son los elementos funcionales de una política de exportación. Las reglas de exportación coinciden con las solicitudes de acceso de los clientes a un volumen con los parámetros específicos que se configuran para determinar cómo se manejan las solicitudes de acceso de los clientes.

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

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

- El protocolo de acceso a archivos que utiliza el cliente para enviar la solicitud, por ejemplo, NFSv4 o SMB.

- Un identificador de cliente, por ejemplo, un nombre de host o una dirección IP.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

autentica con AUTH_SYS.

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

Ejemplos de normas de política de exportación de ONTAP que restringen o permiten el acceso a través de SMB

Los ejemplos muestran cómo crear reglas de política de exportación que restringen o permiten el acceso a través de SMB en una SVM que tiene habilitadas políticas de exportación para el acceso a SMB.

Las políticas de exportación para acceso a SMB están deshabilitadas de forma predeterminada. Debe configurar reglas de políticas de exportación que restrinjan o permitan el acceso mediante SMB solo si ha habilitado políticas de exportación para el acceso a SMB.

Regla de exportación solo para acceso SMB

El siguiente comando crea una regla de exportación en la SVM denominada "'vs1'" que tiene la siguiente configuración:

- Nombre de la directiva: Cifs1
- Número de índice: 1
- Coincidencia de cliente: Sólo coincide con los clientes de la red 192.168.1.0/24
- Protocol: Solo habilita el acceso SMB
- Acceso de sólo lectura: A clientes que utilizan autenticación NTLM o Kerberos
- Acceso de lectura y escritura: A clientes que utilizan autenticación Kerberos

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

Regla de exportación para el acceso a SMB y NFS

El siguiente comando crea una regla de exportación en el SVM denominado»' vs1'» que tiene la siguiente configuración:

- Nombre de la directiva: Cifsssnfs1
- Número de índice: 2
- Coincidencia de cliente: Coincide con todos los clientes
- Protocolo: Acceso SMB y NFS
- Acceso de sólo lectura: A todos los clientes
- Acceso de lectura y escritura: A clientes que utilizan Kerberos (NFS y SMB) o autenticación NTLM (SMB)
- Asignación para el ID de usuario de UNIX 0 (cero): Se asigna al ID de usuario 65534 (que normalmente

asigna al nombre de usuario nobody)

- Acceso suid y sgid: Permite

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule any
-rwrule krb5,ntlm -anon 65534 -allow-suid true
```

Regla de exportación para acceso SMB únicamente mediante NTLM

El siguiente comando crea una regla de exportación en la SVM denominada "'vs1'" que tiene la siguiente configuración:

- Nombre de la política: Ntlm1
- Número de índice: 1
- Coincidencia de cliente: Coincide con todos los clientes
- Protocol: Solo habilita el acceso SMB
- Acceso de sólo lectura: Sólo para clientes que utilizan NTLM
- Acceso de lectura y escritura: Sólo para clientes que utilizan NTLM

> Si configura la opción de sólo lectura o la opción de lectura y escritura para el acceso NTLM, debe utilizar las entradas basadas en dirección IP en la opción de coincidencia de cliente. De lo contrario, recibirá `access denied` errores. Esto se debe a que ONTAP utiliza los nombres principales de servicios (SPN) de Kerberos al utilizar un nombre de host para comprobar los derechos de acceso del cliente. La autenticación NTLM no admite nombres SPN.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

Habilitar o deshabilitar las políticas de exportación de ONTAP para el acceso SMB

Puede habilitar o deshabilitar las políticas de exportación para acceso de SMB en máquinas virtuales de almacenamiento (SVM). El uso de políticas de exportación para controlar el acceso de SMB a los recursos es opcional.

Antes de empezar

A continuación, se muestran los requisitos para habilitar las políticas de exportación para SMB:

- El cliente debe tener un registro PTR en DNS antes de crear las reglas de exportación para ese cliente.
- Si la SVM proporciona acceso A los clientes NFS, se requiere un conjunto adicional de registros «A» y «PTR» para los nombres de host y el nombre de host que desea utilizar para el acceso NFS es diferente del nombre del servidor CIFS.

Acerca de esta tarea

Al configurar un nuevo servidor CIFS en la SVM, el uso de políticas de exportación para acceso de SMB está deshabilitado de forma predeterminada. Puede habilitar las políticas de exportación para el acceso de SMB si

desea controlar el acceso en función del protocolo de autenticación o en direcciones IP de cliente o nombres de host. Es posible habilitar o deshabilitar las políticas de exportación para el acceso de SMB en cualquier momento.

> Al habilitar políticas de exportación para CIFS/SMB en una SVM habilitada para NFS, un cliente Linux puede usar `showmount -e` el comando en la SVM para ver las rutas de unión de todos los volúmenes SMB con reglas de políticas de exportación asociadas.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Habilite o deshabilite políticas de exportación:
   - Habilite políticas de exportación: `vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled true`
   - Desactivar políticas de exportación: `vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled false`
3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Ejemplo

El siguiente ejemplo permite el uso de políticas de exportación para controlar el acceso de clientes SMB a los recursos en SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

Acceso seguro a archivos mediante Storage-Level Access Guard

Obtenga información sobre el acceso seguro a archivos SMB de ONTAP mediante Storage-Level Access Guard

Además de proteger el acceso mediante el uso nativo a nivel de archivo y la seguridad de exportación y uso compartido, puede configurar la protección de acceso a nivel de almacenamiento, una tercera capa de seguridad aplicada por ONTAP a nivel de volumen. El servicio de protección de acceso a nivel de almacenamiento se aplica para acceder desde todos los protocolos NAS al objeto de almacenamiento al que se aplica.

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

Comportamiento de protección del acceso al nivel de almacenamiento

- Storage-Level Access Guard se aplica a todos los archivos o todos los directorios de un objeto de almacenamiento.

  Puesto que todos los archivos o directorios de un volumen están sujetos a la configuración de Storage-Level Access Guard, no se requiere la herencia a través de la propagación.

- Puede configurar Storage-Level Access Guard para que se aplique sólo a archivos, sólo a directorios o a los archivos y directorios de un volumen.
  - Seguridad de archivos y directorios

    Se aplica a todos los directorios y archivos del objeto de almacenamiento. Esta es la configuración predeterminada.

  - Seguridad de archivos

    Se aplica a cada archivo dentro del objeto de almacenamiento. Aplicar esta seguridad no afecta al acceso a los directorios o a la auditoría de ellos.

  - Seguridad del directorio

    Se aplica a cada directorio dentro del objeto de almacenamiento. Aplicar esta seguridad no afecta al acceso a los archivos ni a la auditoría de ellos.

- Se utiliza Storage-Level Access Guard para restringir los permisos.

  Nunca dará permisos de acceso adicionales.

- Si ve la configuración de seguridad en un archivo o un directorio desde un cliente NFS o SMB, no verá la seguridad de Access Guard a nivel de almacenamiento.

  Se aplica en el nivel de objeto de almacenamiento y se almacena en los metadatos que se usan para determinar la efectividad de los permisos.

- La seguridad a nivel de almacenamiento no puede ser revocada desde un cliente, incluso por un administrador de sistema (Windows o UNIX)

  Está diseñado para que lo modifiquen únicamente administradores del almacenamiento.

- Se puede aplicar Access Guard en el nivel de almacenamiento a volúmenes con un estilo de seguridad NTFS o mixto.
- Es posible aplicar una protección de acceso al nivel de almacenamiento a los volúmenes con estilo de seguridad UNIX siempre que la SVM que contiene el volumen tenga configurado un servidor CIFS.
- Cuando los volúmenes se montan en una ruta de unión de volúmenes y, si existe la función Storage-Level Access Guard en esa ruta, no se propagará a los volúmenes montados bajo ella.
- El descriptor de seguridad de Storage-Level Access Guard se replica con la replicación de datos de SnapMirror y con la replicación de SVM.
- Hay una dispensación especial para los escáneres de virus.

  Estos servidores pueden acceder de forma excepcional a los archivos y directorios de pantalla, incluso si Storage-Level Access Guard deniega el acceso al objeto.

- Las notificaciones de FPolicy no se envían si se deniega el acceso debido a la protección de acceso al nivel de almacenamiento.

Orden de las comprobaciones de acceso

El acceso a un archivo o directorio se determina por el efecto combinado de los permisos de exportación o uso compartido, los permisos de Storage-Level Access Guard configurados en volúmenes y los permisos de archivo nativos aplicados a archivos y/o directorios. Se evalúan todos los niveles de seguridad para determinar los permisos efectivos que tiene un archivo o directorio. Las comprobaciones de acceso de seguridad se realizan en el siguiente orden:

1. Permisos a nivel de exportación de SMB o NFS
2. Protección de acceso al nivel de almacenamiento
3. Listas de control de acceso a carpetas/archivos NTFS (ACL), ACL de NFSv4 o bits de modo UNIX

Casos de uso para usar Storage-Level Access Guard

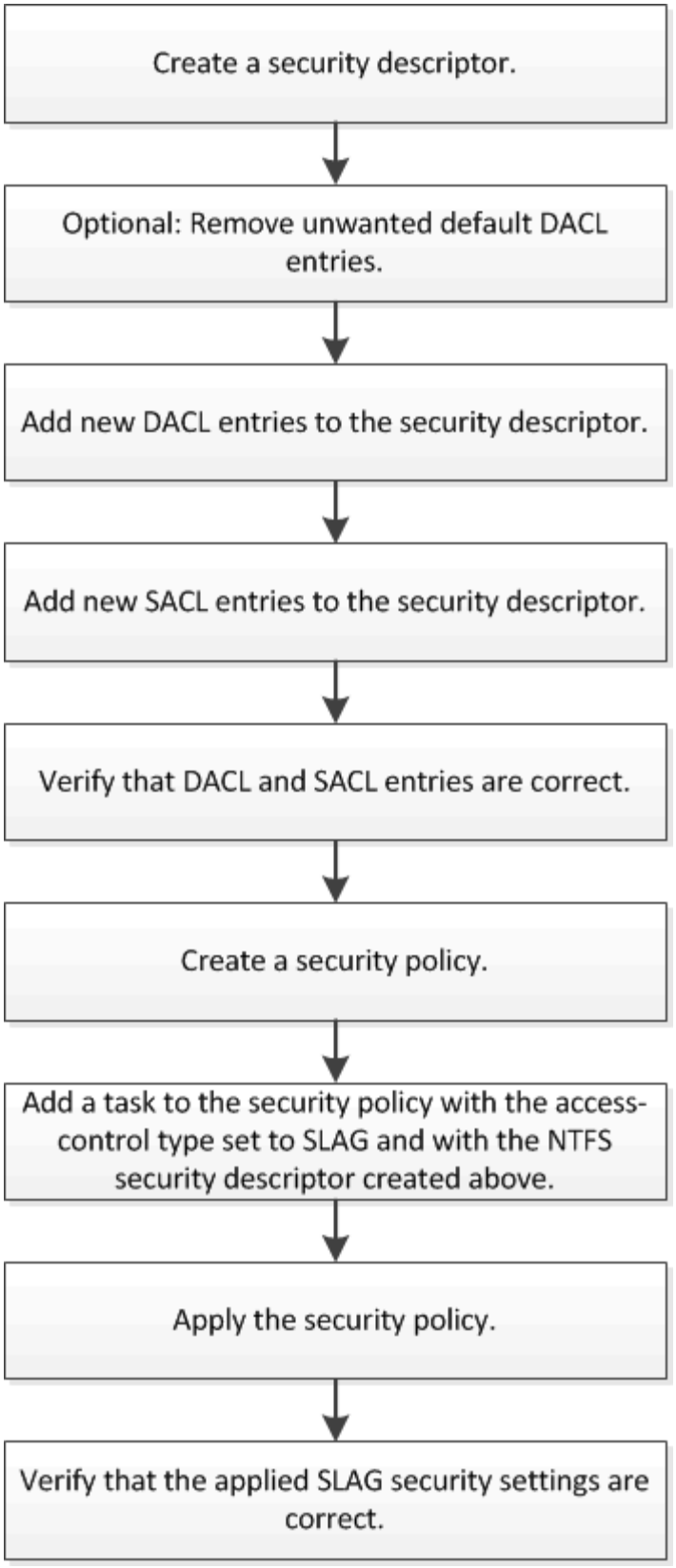
El servicio de protección de acceso a nivel de almacenamiento proporciona una seguridad adicional a nivel de almacenamiento, que no puede verse en el lado del cliente; por lo tanto, no puede ser revocado por ninguno de los usuarios o administradores de sus escritorios. Existen determinados casos de uso en los que es conveniente la capacidad de controlar el acceso en el nivel de almacenamiento.

Los casos de uso típicos de esta función incluyen las siguientes situaciones:

- Protección de la propiedad intelectual mediante la auditoría y el control del acceso de todos los usuarios a nivel de almacenamiento
- Almacenamiento para empresas de servicios financieros, incluidos grupos bancarios y comerciales
- Servicios gubernamentales con almacenamiento de ficheros independiente para departamentos individuales
- Universidades que protegen todos los archivos de los estudiantes

Flujo de trabajo de configuración para Storage-Level Access Guard en servidores SMB de ONTAP

El flujo de trabajo para configurar la protección de acceso al nivel de almacenamiento (SSLAG) utiliza los mismos comandos de la CLI de ONTAP que utiliza para configurar permisos de archivos NTFS y directivas de auditoría. En lugar de configurar el acceso a archivos y directorios en un destino designado, debe configurar SLAG en el volumen de máquina virtual de almacenamiento designado.



Información relacionada

Configurar la protección de acceso a nivel de almacenamiento en los servidores

Configurar Storage-Level Access Guard en servidores SMB de ONTAP

Hay una serie de pasos que se deben seguir para configurar la protección del acceso al nivel de almacenamiento en un volumen o un qtree. El protector de acceso al nivel de almacenamiento ofrece un nivel de seguridad de acceso que se establece en el nivel de almacenamiento. Proporciona seguridad que se aplica a todos los accesos desde todos los protocolos NAS al objeto de almacenamiento al que se ha aplicado.

Pasos

1. Cree un descriptor de seguridad con `vserver security file-directory ntfs create` el comando.

   `vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1 vserver security file-directory ntfs show -vserver vs1`

   ```
   Vserver: vs1

      NTFS Security    Owner Name
      Descriptor Name
      ------------     --------------
      sd1              -
   ```

   Se crea un descriptor de seguridad con las siguientes cuatro entradas predeterminadas de control de acceso de DACL (ACE):

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       BUILTIN\Administrators
                        allow    full-control   this-folder, sub-folders,
   files
       BUILTIN\Users    allow    full-control   this-folder, sub-folders,
   files
       CREATOR OWNER    allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   Si no desea utilizar las entradas predeterminadas al configurar Storage-Level Access Guard, puede eliminarlas antes de crear y agregar sus propias ACE al descriptor de seguridad.

2. Quite cualquiera de los ACE de DACL predeterminados del descriptor de seguridad que no desea

configurar con la seguridad Storage-Level Access Guard:

a. Elimine todas las ACE DACL no deseadas con el `vserver security file-directory ntfs dacl remove` comando.

   En este ejemplo, se quitan tres ACE de DACL predeterminados del descriptor de seguridad: BUILTIN\Administrators, BUILTIN\Users y CREATOR OWNER.

   ```
   vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
   -access-type allow -account builtin\users vserver security file-directory
   ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
   builtin\administrators vserver security file-directory ntfs dacl remove
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
   ```

b. Compruebe que las ACL DACL que no desea utilizar para la seguridad de Access Guard de nivel de almacenamiento se hayan eliminado del descriptor de seguridad mediante `vserver security file-directory ntfs dacl show` el comando.

   En este ejemplo, la salida del comando verifica que se han eliminado tres ACE de DACL predeterminados del descriptor de seguridad, dejando sólo la entrada de ACE de DACL predeterminada de NT AUTHORITY\SYSTEM:

   ```
   vserver security file-directory ntfs dacl show -vserver vs1
   ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

3. Añada una o varias entradas DACL a un descriptor de seguridad mediante `vserver security file-directory ntfs dacl add` el comando.

   En este ejemplo, se agregan dos ACE de DACL al descriptor de seguridad:

   ```
   vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
   -access-type allow -account example\engineering -rights full-control -apply-to
   this-folder,sub-folders,files vserver security file-directory ntfs dacl add
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
   -rights read -apply-to this-folder,sub-folders,files
   ```

4. Añada una o varias entradas de SACL a un descriptor de seguridad mediante `vserver security file-directory ntfs sacl add` el comando.

   En este ejemplo, se agregan dos ACE de SACL al descriptor de seguridad:

   ```
   vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
   ```

```
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. Verifique que las ACE DACL y SACL estén configuradas correctamente mediante los `vserver security file-directory ntfs dacl show` `vserver security file-directory ntfs sacl show` comandos y, respectivamente.

   En este ejemplo, el siguiente comando muestra información sobre las entradas de DACL para el descriptor de seguridad “D1”:

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   ```

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        allow    read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   En este ejemplo, el siguiente comando muestra información sobre las entradas de SACL para el descriptor de seguridad “D1”:

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    EXAMPLE\Domain Users
                     failure  read           this-folder, sub-folders,
files
    EXAMPLE\engineering
                     success  full-control   this-folder, sub-folders,
files
```

6. Cree una política de seguridad mediante `vserver security file-directory policy create` el comando.

   En el siguiente ejemplo se crea una directiva denominada «'póliza 1'»:

   ```
   vserver security file-directory policy create -vserver vs1 -policy-name
   policy1
   ```

7. Compruebe que la política se ha configurado correctamente mediante `vserver security file-directory policy show` el comando.

   ```
   vserver security file-directory policy show
   ```

   ```
      Vserver          Policy Name
      ------------     --------------
      vs1              policy1
   ```

8. Agregue una tarea con un descriptor de seguridad asociado a la política de seguridad mediante el `vserver security file-directory policy task add` comando con el `-access-control` parámetro definido en `slag`.

   Aunque una directiva puede contener más de una tarea de Storage-Level Access Guard, no puede configurar una directiva para que contenga tareas de directorio de archivos y de Storage-Level Access Guard. Una política debe contener todas las tareas de Storage-Level Access Guard o todas las tareas de directorio de archivos.

   En este ejemplo, se agrega una tarea a la política denominada "'poly1'", que se asigna al descriptor de seguridad "sD1". Se asigna a la `/datavol1` ruta con el tipo de control de acceso establecido en “Slag”.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode
   propagate -ntfs-sd sd1
   ```

9. Compruebe que la tarea está configurada correctamente mediante `vserver security file-directory policy task show` el comando.

```
vserver security file-directory policy task show -vserver vs1 -policy-name
policy1
```

```
 Vserver: vs1
  Policy: policy1

   Index  File/Folder  Access           Security  NTFS       NTFS
Security
          Path         Control          Type      Mode       Descriptor
Name
   -----  -----------  ---------------  --------  ----------
---------------
   1      /datavol1    slag             ntfs      propagate  sd1
```

10. Aplique la política de seguridad Access Guard de nivel de almacenamiento mediante `vserver security file-directory apply` el comando.

    ```
    vserver security file-directory apply -vserver vs1 -policy-name policy1
    ```

    El trabajo que se va a aplicar la directiva de seguridad está programado.

11. Verifique que la configuración de seguridad de Access Guard de nivel de almacenamiento aplicada sea correcta mediante el `vserver security file-directory show` comando.

    En este ejemplo, la salida del comando muestra que la seguridad de Storage-Level Access Guard se ha aplicado al volumen NTFS `/datavol1` . Aunque el DACL predeterminado que permite el control total para todos permanece, la seguridad de Storage-Level Access Guard restringe (y audita) el acceso a los grupos definidos en la configuración de Storage-Level Access Guard.

    ```
    vserver security file-directory show -vserver vs1 -path /datavol1
    ```

```
                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Información relacionada

- Comandos para administrar la seguridad de archivos NTFS, las políticas de auditoría de NTFS y la protección de acceso a nivel de almacenamiento
- Flujo de trabajo de configuración para Storage-Level Access Guard en servidores
- Mostrar información sobre la protección de acceso a nivel de almacenamiento en los servidores
- Eliminar la protección de acceso a nivel de almacenamiento en los servidores

Matriz SLAG eficaz en servidores SMB de ONTAP

Puede configurar SLAG en un volumen, un qtree o ambos. La matriz SLAG define en qué volumen o qtree se aplica la configuración SLAG en los distintos escenarios que se indican en la tabla.

	Volumen SLAG en un AFS	ASIGNACIÓN DE volumen en una instantánea	Qtree SLAG en un AFS	ELIMINACIÓN DE qtree en una copia snapshot
Acceso de volumen en un sistema de archivos de acceso (AFS)	SÍ	NO	N / A	N / A
Acceso del volumen en una copia de Snapshot	SÍ	NO	N / A	N / A
Acceso a Qtree en un AFS (cuando SLAG está presente en el qtree)	NO	NO	SÍ	NO
Acceso a Qtree en un AFS (cuando SLAG no está presente en qtree)	SÍ	NO	NO	NO
Acceso a Qtree en una copia de Snapshot (cuando hay UN SUFIJO en el AFS para qtree)	NO	NO	SÍ	NO
Acceso a Qtree en una copia de Snapshot (cuando no está presente LA función SLAG en el AFS para qtree)	SÍ	NO	NO	NO

Mostrar información sobre Storage-Level Access Guard en servidores SMB de ONTAP

El servicio de protección del acceso a nivel de almacenamiento es una tercera capa de seguridad aplicada en un volumen o un qtree. La configuración de Storage-Level Access Guard no se puede ver mediante la ventana Propiedades de Windows. Es necesario usar la interfaz de línea de comandos de ONTAP para ver información sobre la seguridad de protección del acceso a nivel de almacenamiento, que se puede utilizar para validar la configuración o solucionar problemas de acceso a archivos.

Acerca de esta tarea

Se debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta al volumen o qtree cuya información de seguridad de protección de acceso de nivel de almacenamiento desea mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

Paso

1. Mostrar la configuración de seguridad de protección de acceso a nivel de almacenamiento con el nivel de detalle deseado:

Si desea mostrar información…	Introduzca el siguiente comando…
En forma de resumen	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Con detalle ampliado	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Ejemplos

En el siguiente ejemplo, se muestra información de seguridad de Access Guard de nivel de almacenamiento para el volumen de estilo de seguridad NTFS con la ruta `/datavol1` en SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

En el siguiente ejemplo, se muestra información de Access Guard al nivel de almacenamiento acerca del volumen mixto de estilo de seguridad en la ruta de `/datavol5` SVM VS1. El nivel superior de este volumen tiene una seguridad efectiva para UNIX. El volumen tiene seguridad de protección de acceso en el nivel de almacenamiento.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Eliminar la protección de acceso a nivel de almacenamiento en servidores SMB de ONTAP

Puede quitar la protección de acceso al nivel de almacenamiento en un volumen o qtree si ya no desea establecer la seguridad de acceso en el nivel de almacenamiento. La eliminación de la protección de acceso a nivel de almacenamiento no modifica ni quita la seguridad normal de archivos NTFS y directorios.

Pasos

1. Compruebe que el volumen o qtree tiene la protección de acceso a nivel de almacenamiento configurada mediante `vserver security file-directory show` el comando.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

                         Storage-Level Access Guard security
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

2. Quite la protección de acceso al nivel de almacenamiento mediante `vserver security file-directory remove-slag` el comando.

   ```
   vserver security file-directory remove-slag -vserver vs1 -path /datavol2
   ```

3. Compruebe que la protección de acceso al nivel de almacenamiento se haya eliminado del volumen o qtree mediante `vserver security file-directory show` el comando.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```

Gestione el acceso a archivos mediante SMB

Utilice usuarios y grupos locales para autenticación y autorización

Cómo utiliza ONTAP usuarios y grupos locales

Obtenga información sobre los usuarios y grupos locales de ONTAP SMB

Debe saber cuáles son los usuarios y grupos locales, así como alguna información básica sobre ellos, antes de determinar si configurar y utilizar usuarios y grupos locales en su entorno.

- **Usuario local**

  Una cuenta de usuario con un identificador de seguridad único (SID) que solo tiene visibilidad en la máquina virtual de almacenamiento (SVM) donde se crea. Las cuentas de usuario local tienen un conjunto de atributos, incluidos el nombre de usuario y el SID. Una cuenta de usuario local autentica de forma local en el servidor CIFS mediante la autenticación NTLM.

  Las cuentas de usuario tienen varios usos:

  - Se utiliza para otorgar privilegios *User Rights Management* a un usuario.
  - Se usa para controlar el acceso a nivel de recurso compartido y de archivo a los recursos de archivos y carpetas que posee la SVM.

- **Grupo local**

  Un grupo con un SID exclusivo tiene visibilidad solo en la SVM donde se crea. Los grupos contienen un conjunto de miembros. Los miembros pueden ser usuarios locales, usuarios de dominio, grupos de dominio y cuentas de equipos de dominio. Los grupos se pueden crear, modificar o eliminar.

  Los grupos tienen varios usos:

  - Se utiliza para otorgar privilegios *User Rights Management* a sus miembros.
  - Se usa para controlar el acceso a nivel de recurso compartido y de archivo a los recursos de archivos y carpetas que posee la SVM.
- **Dominio local**

  Un dominio que tiene un alcance local, delimitado por la SVM. El nombre del dominio local es el nombre del servidor CIFS. Los usuarios y grupos locales se encuentran dentro del dominio local.

- **Identificador de seguridad (SID)**

  Un SID es un valor numérico de longitud variable que identifica los principios de seguridad de estilo Windows. Por ejemplo, un SID típico toma la siguiente forma: S-1-5-21-3139654847-1303905135-2517279418-123456.

- **Autenticación NTLM**

  Un método de seguridad de Microsoft Windows que se utiliza para autenticar usuarios en un servidor CIFS.

- **Base de datos replicada en cluster (RDB)**

  Base de datos replicada con una instancia en cada nodo de un clúster. Los objetos de usuario local y de grupo se almacenan en el RDB.

Razones para crear usuarios y grupos locales de ONTAP SMB

Hay varias razones para crear usuarios locales y grupos locales en la máquina virtual de almacenamiento (SVM). Por ejemplo, puede tener acceso a un servidor SMB utilizando una cuenta de usuario local si los controladores de dominio (DC) no están disponibles, es posible que desee utilizar grupos locales para asignar privilegios o que el servidor SMB esté en un grupo de trabajo.

Es posible crear una o varias cuentas de usuario locales por los siguientes motivos:

- El servidor SMB está en un grupo de trabajo y los usuarios del dominio no están disponibles.

  Los usuarios locales son necesarios en configuraciones de grupos de trabajo.

- Puede autenticar e iniciar sesión en el servidor SMB si las controladoras de dominio no están disponibles.

  Los usuarios locales pueden autenticarse con el servidor SMB mediante la autenticación NTLM cuando el controlador de dominio está inactivo o cuando los problemas de red impiden que el servidor SMB se ponga en contacto con el controlador de dominio.

- Desea asignar privilegios *User Rights Management* a un usuario local.

User Rights Management es la capacidad de un administrador de servidor SMB para controlar los derechos que tienen los usuarios y los grupos en la SVM. Puede asignar privilegios a un usuario asignando los privilegios a la cuenta del usuario o haciendo que el usuario sea miembro de un grupo local que tenga esos privilegios.

Se pueden crear uno o varios grupos locales por los siguientes motivos:

- El servidor SMB está en un grupo de trabajo y los grupos de dominio no están disponibles.

  Los grupos locales no son necesarios en las configuraciones de grupos de trabajo, pero pueden ser útiles para administrar privilegios de acceso para los usuarios de grupos de trabajo locales.

- Desea controlar el acceso a los recursos de archivos y carpetas mediante grupos locales para controlar el uso compartido y el acceso a archivos.
- Desea crear grupos locales con privilegios *User Rights Management* personalizados.

  Algunos grupos de usuarios integrados tienen privilegios predefinidos. Para asignar un conjunto personalizado de privilegios, puede crear un grupo local y asignar los privilegios necesarios a ese grupo. A continuación, puede agregar usuarios locales, usuarios de dominio y grupos de dominio al grupo local.

Información relacionada

- Obtenga más información sobre la autenticación de usuarios locales
- Lista de privilegios compatibles

Obtenga información sobre la autenticación de usuarios SMB de ONTAP local

Para que un usuario local pueda acceder a los datos en un servidor CIFS, el usuario debe crear una sesión autenticada.

Debido a que el bloque de mensajes del servidor se basa en sesiones, la identidad del usuario se puede determinar una sola vez cuando se configura la sesión por primera vez. El servidor CIFS utiliza autenticación basada en NTLM al autenticar usuarios locales. Son compatibles tanto NTLMv1 como NTLMv2.

ONTAP utiliza autenticación local en tres casos de uso. Cada caso de uso depende de si la parte del dominio del nombre de usuario (con el formato de DOMINIO\usuario) coincide con el nombre de dominio local del servidor CIFS (el nombre del servidor CIFS):

- La parte del dominio coincide

  Los usuarios que proporcionan credenciales de usuario local al solicitar acceso a los datos se autentican localmente en el servidor CIFS.

- La parte del dominio no coincide

  ONTAP intenta utilizar la autenticación NTLM con un controlador de dominio del dominio al que pertenece el servidor CIFS. Si la autenticación se realiza correctamente, se completa el inicio de sesión. Si no se realiza correctamente, lo que sucede a continuación depende de por qué la autenticación no se ha realizado correctamente.

  Por ejemplo, si el usuario existe en Active Directory pero la contraseña no es válida o ha caducado, ONTAP no intenta utilizar la cuenta de usuario local correspondiente en el servidor CIFS. En su lugar, la autenticación genera errores. Hay otros casos en los que ONTAP utiliza la cuenta local correspondiente en el servidor CIFS, si existe, para la autenticación, aunque los nombres de dominio NetBIOS no coincidan.

Por ejemplo, si existe una cuenta de dominio coincidente pero está deshabilitada, ONTAP utiliza la cuenta local correspondiente en el servidor CIFS para la autenticación.

- No se ha especificado la parte del dominio

  ONTAP intenta primero la autenticación como usuario local. Si la autenticación como usuario local falla, ONTAP autentica al usuario con una controladora de dominio en el dominio al que pertenece el servidor CIFS.

Una vez que la autenticación de usuario local o de dominio se ha completado correctamente, ONTAP crea un token de acceso de usuario completo, que tiene en cuenta la pertenencia a grupos locales y los privilegios.

Para obtener más información acerca de la autenticación NTLM para usuarios locales, consulte la documentación de Microsoft Windows.

Información relacionada

Habilitar o deshabilitar la autenticación de usuarios locales en los servidores

Obtenga más información sobre los tokens de acceso de usuario SMB de ONTAP

Cuando un usuario asigna un recurso compartido, se establece una sesión SMB autenticada y se crea un token de acceso de usuario que contiene información acerca del usuario, la pertenencia al grupo del usuario y los privilegios acumulativos, así como el usuario UNIX asignado.

A menos que la funcionalidad esté deshabilitada, la información de grupo y de usuario local también se agrega al token de acceso de usuario. La forma en que se crean los tokens de acceso depende de si el inicio de sesión es para un usuario local o un usuario de dominio de Active Directory:

- Inicio de sesión de usuario local

  Aunque los usuarios locales pueden ser miembros de diferentes grupos locales, los grupos locales no pueden ser miembros de otros grupos locales. El token de acceso de usuario local se compone de una unión de todos los privilegios asignados a grupos a los que pertenece un usuario local determinado.

- Inicio de sesión de usuario de dominio

  Cuando un usuario de dominio inicia sesión, ONTAP obtiene un token de acceso de usuario que contiene el SID y SID de usuario para todos los grupos de dominio a los que pertenece el usuario. ONTAP utiliza la unión del token de acceso de usuario de dominio con el token de acceso proporcionado por las membresías locales de los grupos de dominio del usuario (si los hay), así como todos los privilegios directos asignados al usuario de dominio o cualquiera de sus pertenencias a grupos de dominio.

Tanto para el inicio de sesión local como para el usuario de dominio, el RID de grupo principal también está configurado para el token de acceso de usuario. El RID predeterminado es `Domain Users` (RID 513). No puede cambiar el valor predeterminado.

El proceso de asignación de nombres de Windows a UNIX y UNIX a Windows sigue las mismas reglas para las cuentas locales y de dominio.

> No hay ningún mapeo implícito y automático de un usuario UNIX a una cuenta local. Si es necesario, se debe especificar una regla de asignación explícita mediante los comandos de asignación de nombres existentes.

Obtenga información sobre el uso de SnapMirror en SVM SMB de ONTAP que contienen grupos locales

Debe tener en cuenta las directrices al configurar SnapMirror en los volúmenes que son propiedad de las SVM que contienen grupos locales.

No se pueden utilizar grupos locales en ACE aplicados a archivos, directorios o recursos compartidos replicados por SnapMirror en otra SVM. Si utiliza la función SnapMirror para crear un reflejo de recuperación ante desastres en un volumen en otra SVM y el volumen tiene una ACE para un grupo local, la ACE no es válida en el reflejo. Si los datos se replican en una SVM diferente, estos se cruzan realmente en un dominio local diferente. Los permisos concedidos a los usuarios y grupos locales solo son válidos dentro del ámbito de la SVM en la que se crearon originalmente.

Conozca los efectos de eliminar servidores SMB de ONTAP en usuarios y grupos

El conjunto predeterminado de usuarios y grupos locales se crea cuando se crea un servidor CIFS y está asociado con las máquinas virtuales de almacenamiento (SVM) que alojan el servidor CIFS. Los administradores de SVM pueden crear usuarios y grupos locales en cualquier momento. Debe saber qué sucede con los usuarios locales y los grupos al eliminar el servidor CIFS.

Los usuarios y grupos locales están asociados a las SVM; por lo tanto, no se eliminan cuando los servidores CIFS se eliminan debido a consideraciones de seguridad. Aunque los usuarios y grupos locales no se eliminan al eliminar el servidor CIFS, sí se ocultan. No se pueden ver ni gestionar usuarios y grupos locales hasta que se vuelva a crear un servidor CIFS en la SVM.

El estado administrativo del servidor CIFS no afecta a la visibilidad de los grupos o usuarios locales.

Aprenda a usar Microsoft Management Console con usuarios y grupos locales de ONTAP SMB

Puede ver información acerca de los usuarios y grupos locales desde la Consola de administración de Microsoft. Con esta versión de ONTAP, no puede realizar otras tareas de administración para usuarios y grupos locales desde la Consola de administración de Microsoft.

Obtenga información sobre cómo revertir clústeres SMB de ONTAP

Si piensa revertir el clúster a una versión de ONTAP que no da soporte a usuarios y grupos locales y se están utilizando grupos y usuarios locales para gestionar los derechos de usuario o el acceso a los archivos, debe tener en cuenta ciertas consideraciones.

- Debido a motivos de seguridad, no se elimina la información sobre usuarios locales, grupos y privilegios configurados cuando ONTAP se revierte a una versión que no admite la funcionalidad de usuarios y grupos locales.
- Al volver a una versión principal anterior de ONTAP, ONTAP no utiliza usuarios ni grupos locales durante la autenticación ni la creación de credenciales.
- Los usuarios y grupos locales no se quitan de las ACL de archivos y carpetas.
- Se deniegan las solicitudes de acceso a archivos que dependen de que se conceda el acceso debido a los permisos concedidos a los usuarios o grupos locales.

Para permitir el acceso, debe volver a configurar los permisos de archivo para permitir el acceso basado en objetos de dominio en lugar de objetos de usuario local y de grupo.

Qué privilegios locales son

Lista de privilegios SMB de ONTAP admitidos

ONTAP tiene un conjunto predefinido de privilegios admitidos. Algunos grupos locales predefinidos tienen algunos de estos privilegios añadidos de forma predeterminada. También puede agregar o quitar privilegios de los grupos predefinidos o crear nuevos usuarios o grupos locales y agregar privilegios a los grupos que creó o a los usuarios y grupos de dominio existentes.

En la siguiente tabla se enumeran los privilegios admitidos en la máquina virtual de almacenamiento (SVM) y se proporciona una lista de los grupos BUILTIN con privilegios asignados:

Nombre del privilegio	Configuración de seguridad predeterminada	Descripción
`SeTcbPrivilege`	Ninguno	Actuar como parte del sistema operativo
`SeBackupPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Realice copias de seguridad de archivos y directorios, anulando cualquier ACL
`SeRestorePrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Restaurar archivos y directorios, anulando cualquier ACL establecer cualquier SID de usuario o grupo válido como propietario del archivo
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	Tomar posesión de archivos u otros objetos
`SeSecurityPrivilege`	`BUILTIN\Administrators`	Gestionar auditoría Esto incluye ver, volcar y borrar el registro de seguridad.
`SeChangeNotifyPrivilege`	`BUILTIN\Administrators`, , , , `BUILTIN\Backup Operators` `BUILTIN\Power Users` `BUILTIN\Users` , `Everyone`	Comprobación de desvío transversal No es necesario que los usuarios con este privilegio tengan permisos de desplazamiento (x) para recorrer carpetas, vínculos simbólicos o uniones.

Información relacionada

- Obtenga información sobre la asignación de privilegios

- Obtenga información sobre cómo configurar la comprobación de recorrido de derivación

Obtenga información sobre la asignación de privilegios SMB de ONTAP

Es posible asignar privilegios directamente a usuarios locales o a usuarios de dominio. También puede asignar usuarios a grupos locales cuyos privilegios asignados coincidan con las capacidades que desea que tengan esos usuarios.

- Puede asignar un conjunto de privilegios a un grupo que cree.

  A continuación, agregue un usuario al grupo que tenga los privilegios que desea que tenga ese usuario.

- También puede asignar usuarios locales y usuarios de dominio a grupos predefinidos cuyos privilegios predeterminados coincidan con los privilegios que desea conceder a esos usuarios.

Información relacionada

- Añada privilegios a usuarios o grupos locales o de dominio
- Quitar privilegios de usuarios o grupos locales o de dominio
- Restablecer privilegios para usuarios y grupos locales o de dominio
- Obtenga información sobre cómo configurar la comprobación de recorrido de derivación

Obtenga información sobre los grupos BUILTIN y las cuentas de administrador local en los servidores SMB de ONTAP

Hay ciertas pautas que debe tener en cuenta cuando utilice los grupos BUILTIN y la cuenta de administrador local. Por ejemplo, puede cambiar el nombre de la cuenta de administrador local, pero no puede eliminar esta cuenta.

- Se puede cambiar el nombre de la cuenta Administrador, pero no se puede eliminar.
- La cuenta de administrador no se puede quitar del grupo BUILTIN\Administrators.
- Se puede cambiar el nombre de los grupos INTEGRADOS, pero no se pueden eliminar.

  Después de cambiar el nombre del grupo BUILTIN, se puede crear otro objeto local con el nombre bien conocido; sin embargo, al objeto se le asigna UN NUEVO RID.

- No hay una cuenta de invitado local.

Información relacionada

Grupos BUILTIN predefinidos y privilegios predeterminados

Requisitos para las contraseñas de usuarios locales de ONTAP SMB

De manera predeterminada, las contraseñas de usuario local deben cumplir con los requisitos complejos. Los requisitos de complejidad de la contraseña son similares a los que se definen en la directiva de seguridad local de Microsoft Windows.

La contraseña debe cumplir los siguientes criterios:

- Debe tener al menos seis caracteres de longitud
- No se debe contener el nombre de cuenta de usuario

- Debe contener caracteres de al menos tres de las siguientes cuatro categorías:
  - Caracteres en mayúsculas (De La A a la Z)
  - Caracteres en minúscula (de la a a la z)
  - Base de 10 dígitos (de 0 a 9)
  - Caracteres especiales:

```
~ ! @ # $ % {caret} & * _ - + = ` \ | ( ) [ ] : ; " ' < > , . ? /
```

Información relacionada

- Configurar la complejidad de la contraseña para usuarios locales
- Mostrar información sobre la configuración de seguridad del servidor
- Cambiar las contraseñas de la cuenta de usuario local

Grupos BUILTIN predefinidos y privilegios SMB de ONTAP predeterminados

Puede asignar la pertenencia de un usuario local o un usuario de dominio a un conjunto predefinido de grupos BUILTIN proporcionados por ONTAP. Los grupos predefinidos tienen privilegios predefinidos asignados.

En la siguiente tabla se describen los grupos predefinidos:

Grupo BUILTIN predefinido	Privilegios predeterminados
`BUILTIN\Administrators`RID 544 Cuando se crea por primera vez, la `Administrator` cuenta local, con un RID de 500, se convierte automáticamente en miembro de este grupo. Cuando la máquina virtual de almacenamiento (SVM) se une a un dominio, `domain\Domain Admins` el grupo se añade al grupo. Si la SVM abandona el dominio, `domain\Domain Admins` el grupo se eliminará del grupo.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Power Users`RID 547 Cuando se crea por primera vez, este grupo no tiene miembros. Los miembros de este grupo tienen las siguientes características: • Puede crear y administrar usuarios y grupos locales. • No se pueden agregar ellos mismos ni ningún otro objeto al `BUILTIN\Administrators` grupo.	`SeChangeNotifyPrivilege`

Grupo BUILTIN predefinido	Privilegios predeterminados
`BUILTIN\Backup Operators`RID 551 Cuando se crea por primera vez, este grupo no tiene miembros. Los miembros de este grupo pueden anular los permisos de lectura y escritura en archivos o carpetas si se abren con la intención de copia de seguridad.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Users`RID 545 Cuando se crea por primera vez, este grupo no tiene ningún miembro (además del `Authenticated Users` grupo especial implícito). Cuando la SVM se une a un dominio, el `domain\Domain Users` grupo se añade a este grupo. Si la SVM abandona el dominio, `domain\Domain Users` el grupo se eliminará de este grupo.	`SeChangeNotifyPrivilege`
`Everyone`SID S-1-1-0 Este grupo incluye a todos los usuarios, incluidos invitados (pero no usuarios anónimos). Este es un grupo implícito con una membresía implícita.	`SeChangeNotifyPrivilege`

Información relacionada

- Obtenga información sobre los grupos BUILTIN y las cuentas de administrador local en los servidores
- Lista de privilegios compatibles
- Obtenga información sobre cómo configurar la comprobación de recorrido de derivación

Habilite o deshabilite la funcionalidad de grupos y usuarios locales

Obtenga información sobre la funcionalidad de los usuarios y grupos SMB locales de ONTAP

Antes de poder utilizar usuarios y grupos locales para controlar el acceso a los datos del estilo de seguridad NTFS, se debe habilitar la funcionalidad de usuario local y grupo. Además, si desea utilizar usuarios locales para la autenticación SMB, se debe habilitar la funcionalidad de autenticación de usuarios locales.

La funcionalidad de grupos y usuarios locales y la autenticación de usuarios locales están habilitadas de forma predeterminada. Si no están habilitadas, debe habilitarlas para poder configurar y utilizar usuarios y grupos locales. La funcionalidad de grupos y usuarios locales se puede deshabilitar en cualquier momento.

Además de deshabilitar explícitamente la funcionalidad de grupo y usuario local, ONTAP deshabilita la funcionalidad de grupo y usuario local si algún nodo del clúster se revierte a una versión de ONTAP que no admite la funcionalidad. La funcionalidad de usuario local y de grupo no está habilitada hasta que todos los nodos del clúster ejecuten una versión de ONTAP que la admita.

Información relacionada

- Modifique las cuentas de usuario local
- Modificar grupos locales
- Añada privilegios a usuarios o grupos locales o de dominio

Habilitar o deshabilitar usuarios y grupos locales en servidores SMB de ONTAP

Puede habilitar o deshabilitar usuarios y grupos locales para el acceso SMB en máquinas virtuales de almacenamiento (SVM). La funcionalidad de grupos y usuarios locales está activada de forma predeterminada.

Acerca de esta tarea

Puede usar usuarios y grupos locales al configurar los permisos de archivos NTFS y compartidos de SMB, y puede usar, opcionalmente, usuarios locales para la autenticación al crear una conexión SMB. Para usar usuarios locales para la autenticación, también debe habilitar la opción de autenticación de grupos y usuarios locales.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

Si desea que los grupos y usuarios locales sean…	Introduzca el comando…
Activado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled true`
Deshabilitado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled false`

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

Ejemplo

El siguiente ejemplo habilita la funcionalidad de grupos y usuarios locales en SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

Información relacionada

- Habilitar o deshabilitar la autenticación de usuarios locales en los servidores
- Habilite o deshabilite cuentas de usuario locales

Habilitar o deshabilitar la autenticación de usuarios locales en los servidores SMB de ONTAP

Puede habilitar o deshabilitar la autenticación de usuario local para el acceso SMB en máquinas virtuales de almacenamiento (SVM). El valor predeterminado es permitir la autenticación de usuario local, que resulta útil cuando la SVM no puede ponerse en contacto con un controlador de dominio o si decide no utilizar controles de acceso a nivel de dominio.

Antes de empezar

La funcionalidad de grupos y usuarios locales debe estar habilitada en el servidor CIFS.

Acerca de esta tarea

Es posible habilitar o deshabilitar la autenticación de usuario local en cualquier momento. Si desea usar usuarios locales para la autenticación al crear una conexión SMB, también debe habilitar la opción de grupos y usuarios locales del servidor CIFS.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

Si desea que la autenticación local sea…	Introduzca el comando…
Activado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled true`
Deshabilitado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled false`

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

Ejemplo

El siguiente ejemplo habilita la autenticación de usuario local en SVM vs1:

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

Información relacionada

- Obtenga más información sobre la autenticación de usuarios locales
- Habilitar o deshabilitar usuarios y grupos locales en servidores

Permite gestionar cuentas de usuario local

Modificar cuentas de usuario SMB locales de ONTAP

Puede modificar una cuenta de usuario local si desea cambiar el nombre completo o la descripción de un usuario existente y si desea habilitar o deshabilitar la cuenta de usuario. También puede cambiar el nombre de una cuenta de usuario local si el nombre del usuario está en peligro o si se necesita un cambio de nombre con fines administrativos.

Si desea…	Introduzca el comando…
Modifique el nombre completo del usuario local	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user -name` *`user_name`* `-full-name text` Si el nombre completo contiene un espacio, debe estar entre comillas dobles.
Modifique la descripción del usuario local	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user -name` *`user_name`* `-description text` Si la descripción contiene un espacio, debe estar entre comillas dobles.
Habilite o deshabilite la cuenta de usuario local	`vserver cifs users-and-groups local-user modify -vserver` *vserver_name* `-user-name` *user_name* `-is -account-disabled {true`
false}`	Cambie el nombre de la cuenta de usuario local

Ejemplo

En el siguiente ejemplo, se cambia el nombre del usuario local «'CIFS_SERVER\sue'» a «'CIFS_SERVER\sue_new» en la máquina virtual de almacenamiento (SVM, antes conocida como Vserver)

vs1:

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

Habilitar o deshabilitar cuentas de usuario SMB de ONTAP locales

Es posible habilitar una cuenta de usuario local si desea que el usuario pueda acceder a los datos contenidos en la máquina virtual de almacenamiento (SVM) a través de una conexión de SMB. También puede deshabilitar una cuenta de usuario local si no desea que ese usuario acceda a los datos de SVM mediante SMB.

Acerca de esta tarea

Para habilitar un usuario local, debe modificar la cuenta de usuario.

Paso

1. Ejecute la acción adecuada:

Si desea…	Introduzca el comando…
Habilite la cuenta de usuario	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account -disabled false`
Desactive la cuenta de usuario	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account -disabled true`

Cambiar las contraseñas de las cuentas de usuario locales de ONTAP SMB

Es posible cambiar la contraseña de la cuenta de un usuario local. Esto puede ser útil si la contraseña del usuario está en peligro o si el usuario ha olvidado la contraseña.

Paso

1. Cambie la contraseña realizando la acción adecuada: `vserver cifs users-and-groups local-user set-password -vserver` *`vserver_name`* `-user-name` *`user_name`*

Ejemplo

En el siguiente ejemplo, se establece la contraseña del usuario local "'CIFS_SERVER\sue'" asociada con la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

Información relacionada

Configurar la complejidad de la contraseña para usuarios locales

Mostrar información sobre la configuración de seguridad del servidor

Mostrar información sobre los usuarios locales de ONTAP SMB

Puede mostrar una lista de todos los usuarios locales en un formulario de resumen. Si desea determinar qué configuración de cuenta está configurada para un usuario específico, puede mostrar información detallada de la cuenta para ese usuario, así como la información de la cuenta para varios usuarios. Esta información puede ayudarle a determinar si necesita modificar la configuración de un usuario y también a resolver problemas de autenticación o acceso a archivos.

Acerca de esta tarea

Nunca se muestra información sobre la contraseña de un usuario.

Paso

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el comando…
Mostrar información sobre todos los usuarios de la máquina virtual de almacenamiento (SVM)	`vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
Muestra información detallada de la cuenta de un usuario	`vserver cifs users-and-groups local-user show -instance -vserver` *`vserver_name`* `-user-name` *`user_name`*

   Hay otros parámetros opcionales que puede elegir cuando ejecuta el comando. Obtenga más información sobre `vserver cifs` en el "Referencia de comandos del ONTAP".

Ejemplo

El siguiente ejemplo muestra información sobre todos los usuarios locales en la SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name     Description
-------- -------------------------- ------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith   Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones
```

Mostrar información sobre las membresías del grupo SMB de ONTAP para usuarios locales

Puede mostrar información sobre los grupos locales a los que pertenece un usuario local. Puede utilizar esta información para determinar qué acceso debe tener el usuario a los archivos y carpetas. Esta información puede ser útil para determinar qué derechos de acceso debe tener el usuario a los archivos y carpetas o al solucionar problemas de acceso a archivos.

Acerca de esta tarea

Puede personalizar el comando para que muestre solo la información que desea ver.

Paso

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el comando…
Muestra información de pertenencia de usuario local para un usuario local específico	`vserver cifs users-and-groups local-user show-membership -user-name` *user_name*
Mostrar información de pertenencia al usuario local para el grupo local del que forma parte este usuario local	`vserver cifs users-and-groups local-user show-membership -membership` *group_name*
Mostrar información de pertenencia al usuario para los usuarios locales que están asociados a una máquina virtual de almacenamiento (SVM) especificada	`vserver cifs users-and-groups local-user show-membership -vserver` *vserver_name*
Mostrar información detallada para todos los usuarios locales en una SVM especificada	`vserver cifs users-and-groups local-user show-membership -instance -vserver` *vserver_name*

Ejemplo

En el siguiente ejemplo se muestra la información de pertenencia de todos los usuarios locales de SVM vs1; el usuario «'CIFS_SERVER\Administrator'» es miembro del grupo «'BUILTIN\Administrators'» y «'CIFS_SERVER\sue'» es miembro del grupo «'CIFS_SERVER\g1'»:

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                     Membership
---------- ----------------------------- ------------------------
vs1        CIFS_SERVER\Administrator     BUILTIN\Administrators
           CIFS_SERVER\sue               CIFS_SERVER\g1
```

Eliminar cuentas de usuario SMB de ONTAP locales

Es posible eliminar cuentas de usuario locales de la máquina virtual de almacenamiento (SVM) si ya no son necesarias para la autenticación local de SMB en el servidor CIFS o para determinar los derechos de acceso a los datos incluidos en la SVM.

Acerca de esta tarea

Tenga en cuenta lo siguiente al eliminar usuarios locales:

- El sistema de archivos no se ha modificado.

  Los descriptores de seguridad de Windows de los archivos y directorios que hacen referencia a este usuario no están ajustados.

- Todas las referencias a los usuarios locales se eliminan de las bases de datos de pertenencia y privilegios.
- No se pueden eliminar los usuarios estándar conocidos, como el Administrador.

Pasos

1. Determine el nombre de la cuenta de usuario local que desea eliminar: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
2. Elimine el usuario local: `vserver cifs users-and-groups local-user delete -vserver` *`vserver_name`* `-user-name` *`username_name`*
3. Compruebe que se ha eliminado la cuenta de usuario: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Ejemplo

En el siguiente ejemplo se elimina el usuario local "'CIFS_SERVER\sue'" asociado con SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                    Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
```

Administrar grupos locales

Modificar grupos SMB locales de ONTAP

Puede modificar los grupos locales existentes cambiando la descripción de un grupo local existente o cambiando el nombre del grupo.

Si desea…	Usar el comando…
Modifique la descripción del grupo local	`vserver cifs users-and-groups local-group modify -vserver` *`vserver_name`* `-group-name` *`group_name`* `-description text` Si la descripción contiene un espacio, debe estar entre comillas dobles.
Cambie el nombre del grupo local	`vserver cifs users-and-groups local-group rename -vserver` *`vserver_name`* `-group-name` *`group_name`* `-new-group-name` *`new_group_name`*

Ejemplos

En el ejemplo siguiente se cambia el nombre del grupo local "'CIFS_SERVER\engineering'" a "'CIFS_SERVER\engineering_new'":

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

En el siguiente ejemplo se modifica la descripción del grupo local "'CIFS_SERVER\engineering'":

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

Mostrar información sobre los grupos locales de SMB de ONTAP

Es posible mostrar una lista de todos los grupos locales configurados en el clúster o en una máquina virtual de almacenamiento (SVM) específica. Esta información puede ser útil para solucionar problemas de acceso a los archivos en la SVM o problemas de derechos de usuario (privilegios) en la SVM.

Paso

1. Ejecute una de las siguientes acciones:

Si desea información acerca de…	Introduzca el comando…
Todos los grupos locales del clúster	`vserver cifs users-and-groups local-group show`
Todos los grupos locales en la SVM	`vserver cifs users-and-groups local-group show -vserver` *`vserver_name`*

Hay otros parámetros opcionales que puede elegir cuando ejecuta este comando. Obtenga más información sobre `vserver cifs` en el "Referencia de comandos del ONTAP".

Ejemplo

En el siguiente ejemplo, se muestra información sobre todos los grupos locales en la SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                  Description
-------- --------------------------- ----------------------------
vs1      BUILTIN\Administrators      Built-in Administrators group
vs1      BUILTIN\Backup Operators    Backup Operators group
vs1      BUILTIN\Power Users         Restricted administrative privileges
vs1      BUILTIN\Users               All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

Gestionar la pertenencia a un grupo SMB de ONTAP local

Puede administrar la pertenencia a grupos locales agregando y eliminando usuarios locales o de dominio, o agregando y eliminando grupos de dominios. Esto resulta útil si desea controlar el acceso a los datos basándose en los controles de acceso colocados en el grupo o si desea que los usuarios tengan privilegios asociados a ese grupo.

Acerca de esta tarea

Directrices para agregar miembros a un grupo local:

- No puede agregar usuarios al grupo especial *Everyone*.
- El grupo local debe existir antes de poder añadir un usuario.
- El usuario debe existir antes de poder agregar el usuario a un grupo local.
- No puede agregar un grupo local a otro grupo local.
- Para agregar un usuario o grupo de dominio a un grupo local, Data ONTAP debe poder resolver el nombre a un SID.

Directrices para eliminar miembros de un grupo local:

- No puede eliminar miembros del grupo especial *Everyone*.
- El grupo del que desea quitar un miembro debe existir.
- ONTAP debe poder resolver los nombres de los miembros que desea quitar del grupo a un SID correspondiente.

Paso

1. Agregar o quitar un miembro de un grupo.

Si desea…	A continuación, se usa el comando…
Agregar un miembro a un grupo	`vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` Puede especificar una lista delimitada por comas de usuarios locales, usuarios de dominio o grupos de dominios para agregarlos al grupo local especificado.
Quitar un miembro de un grupo	`vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` Puede especificar una lista delimitada por comas de usuarios locales, usuarios de dominio o grupos de dominios para eliminarlos del grupo local especificado.

En el siguiente ejemplo, se agrega un usuario local "MB_SERVER\sue" y un grupo de dominios "'AD_DOM\dom_eng'" al grupo local "MB_SERVER\engineering" en SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

En el siguiente ejemplo se eliminan los usuarios locales «MB_SERVER\sue» y «MB_SERVER\james» del

grupo local «MB_SERVER\engineering» de SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Información relacionada

Muestra información acerca de los miembros de los grupos locales

Mostrar información de ONTAP SMB sobre los miembros de los grupos locales

Es posible mostrar una lista de todos los miembros de grupos locales configurados en el clúster o en una máquina virtual de almacenamiento (SVM) especificada. Esta información puede ser útil para solucionar problemas de acceso a archivos o problemas de derechos de usuario (privilegios).

Paso

1. Ejecute una de las siguientes acciones:

Si desea mostrar información acerca de…	Introduzca el comando…
Miembros de todos los grupos locales del cluster	`vserver cifs users-and-groups local-group show-members`
Miembros de todos los grupos locales en la SVM	`vserver cifs users-and-groups local-group show-members -vserver` *`vserver_name`*

Ejemplo

En el siguiente ejemplo, se muestra información acerca de los miembros de todos los grupos locales en la SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                    Members
--------- ----------------------------- ------------------------
vs1       BUILTIN\Administrators        CIFS_SERVER\Administrator
                                        AD_DOMAIN\Domain Admins
                                        AD_DOMAIN\dom_grp1
          BUILTIN\Users                 AD_DOMAIN\Domain Users
                                        AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering       CIFS_SERVER\james
```

Eliminar grupos SMB locales de ONTAP

Es posible eliminar un grupo local de la máquina virtual de almacenamiento (SVM) si ya no es necesario para determinar los derechos de acceso a los datos asociados con esa SVM o si ya no es necesario para asignar los derechos de usuario (privilegios) de SVM a los miembros del grupo.

Acerca de esta tarea

Tenga en cuenta lo siguiente al eliminar grupos locales:

- El sistema de archivos no se ha modificado.

  Los descriptores de seguridad de Windows de los archivos y directorios que hacen referencia a este grupo no se ajustan.

- Si el grupo no existe, se devuelve un error.
- El grupo especial *Everyone* no se puede eliminar.
- Los grupos integrados como *BUILTIN\Administrators BUILTIN\Users* no se pueden eliminar.

Pasos

1. Determine el nombre del grupo local que desea eliminar. Para ello, muestre la lista de grupos locales en la SVM: `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. Elimine el grupo local: `vserver cifs users-and-groups local-group delete -vserver` *`vserver_name`* `-group-name` *`group_name`*
3. Compruebe que el grupo se ha suprimido: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Ejemplo

En el siguiente ejemplo se elimina el grupo local "'CIFS_SERVER\sales'" asociado con SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
```

Actualizar los nombres de usuarios y grupos del dominio SMB de ONTAP en las bases de datos locales

Puede agregar usuarios y grupos de dominio a los grupos locales de un servidor CIFS. Estos objetos de dominio se registran en bases de datos locales en el clúster. Si se cambia el nombre de un objeto de dominio, las bases de datos locales deben actualizarse manualmente.

Acerca de esta tarea

Debe especificar el nombre de la máquina virtual de almacenamiento (SVM) en la que desea actualizar los nombres de dominio.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Ejecute la acción adecuada:

Si desea actualizar usuarios y grupos de dominio y…	Se usa este comando…
Muestra usuarios y grupos de dominio que se han actualizado correctamente y que no se han podido actualizar	`vserver cifs users-and-groups update-names -vserver` *vserver_name*

Si desea actualizar usuarios y grupos de dominio y…	Se usa este comando…
Muestra los usuarios y grupos de dominio que se han actualizado correctamente	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false`
Muestra sólo los usuarios y grupos de dominio que no se pueden actualizar	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true`
Suprimir toda la información de estado acerca de las actualizaciones	`vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true`

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

Ejemplo

En el siguiente ejemplo se actualizan los nombres de los usuarios y grupos de dominio asociados con la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1. Para la última actualización, hay una cadena de nombres dependiente que se debe actualizar:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin
```

Gestione los privilegios locales

Agregar privilegios a usuarios o grupos locales o de dominio de ONTAP SMB

Puede administrar los derechos de usuario para usuarios o grupos locales o de dominio mediante la adición de privilegios. Los privilegios agregados anulan los privilegios predeterminados asignados a cualquiera de estos objetos. Esto proporciona una seguridad mejorada al permitirle personalizar qué privilegios tiene un usuario o grupo.

Antes de empezar

Debe haber ya el usuario o grupo local o de dominio al que se añadirán privilegios.

Acerca de esta tarea

Al agregar un privilegio a un objeto se reemplazan los privilegios predeterminados para ese usuario o grupo. Al añadir un privilegio, no se quitan los privilegios añadidos anteriormente.

Debe tener en cuenta lo siguiente al agregar privilegios a usuarios o grupos locales o de dominio:

- Puede añadir uno o varios privilegios.
- Al agregar privilegios a un usuario o grupo de dominio, ONTAP puede validar el usuario o grupo de dominio poniéndose en contacto con el controlador de dominio.

  Es posible que se produzca un error en el comando si ONTAP no puede comunicarse con la controladora de dominio.

Pasos

1. Añada una o más Privileges a un usuario o grupo local o de dominio: `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. Compruebe que se aplican los Privileges deseados al objeto: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Ejemplo

En el siguiente ejemplo, se añaden los privilegios «ShebPrivilege» y «SeeTakeOwnershipPrivilege» al usuario «'CIFS_SERVER\sue» en la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege
```

Eliminar privilegios de usuarios o grupos locales o de dominio de ONTAP SMB

Puede administrar derechos de usuario para usuarios o grupos locales o de dominio eliminando privilegios. Esto proporciona una seguridad mejorada al permitirle

personalizar los privilegios máximos que tienen los usuarios y los grupos.

Antes de empezar

Debe haber ya el usuario o grupo local o de dominio del que se eliminarán los privilegios.

Acerca de esta tarea

Al quitar privilegios de usuarios o grupos locales o de dominio, debe tener en cuenta lo siguiente:

- Puede eliminar uno o varios privilegios.
- Al eliminar privilegios de un usuario o grupo de dominio, ONTAP puede validar el usuario o grupo de dominio poniéndose en contacto con el controlador de dominio.

  Es posible que se produzca un error en el comando si ONTAP no puede comunicarse con la controladora de dominio.

Pasos

1. Quite una o más Privileges de un usuario o grupo local o de dominio: `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. Verifique que el Privileges deseado se haya eliminado del objeto: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Ejemplo

En el siguiente ejemplo se eliminan los privilegios «DeeTcbPrivilege» y «SeeTakeOwnershipPrivilege» del usuario «'CIFS_SERVER\sue» en la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ------------------
vs1       CIFS_SERVER\sue      -
```

Restablecer privilegios para usuarios y grupos locales o de dominio de ONTAP SMB

Es posible restablecer privilegios para los grupos y usuarios locales o de dominio. Esto puede ser útil si ha realizado modificaciones a los privilegios de un usuario o grupo local o de dominio y esas modificaciones ya no se desean ni se necesitan.

Acerca de esta tarea

Al restablecer los privilegios de un usuario o grupo local o de dominio, se quitan todas las entradas de privilegios de ese objeto.

Pasos

1. Restablezca la Privileges en un usuario o grupo local o de dominio: `vserver cifs users-and-groups privilege reset-privilege -vserver vserver_name -user-or-group-name name`
2. Compruebe que los Privileges se han restablecido en el objeto: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Ejemplos

En el siguiente ejemplo, se restablecen los privilegios para el usuario «'CIFS_SERVER\sue'» en la máquina virtual de almacenamiento (SVM, anteriormente conocida como Vserver) vs1. De forma predeterminada, los usuarios normales no tienen privilegios asociados a sus cuentas:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

En el ejemplo siguiente se restablecen los privilegios para el grupo "'BUILTIN\Administrators'", eliminando de forma efectiva la entrada de privilegios:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ------------------------ --------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Mostrar información sobre las anulaciones de privilegios SMB de ONTAP

Puede mostrar información acerca de los privilegios personalizados asignados a cuentas o grupos de usuarios locales o de dominio. Esta información le ayuda a determinar si se aplican los derechos de usuario deseados.

Paso

1. Ejecute una de las siguientes acciones:

Si desea mostrar información acerca de…	Introduzca este comando…
Privilegios personalizados para todos los grupos y usuarios locales y de dominio en la máquina virtual de almacenamiento (SVM)	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`*
Privilegios personalizados para un dominio o un grupo y usuario local específicos de la SVM	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Hay otros parámetros opcionales que puede elegir cuando ejecuta este comando. Obtenga más información sobre `vserver cifs users-and-groups privilege show` en el "Referencia de comandos del ONTAP".

Ejemplo

El siguiente comando muestra todos los privilegios asociados explícitamente con los usuarios y grupos locales o de dominio para SVM vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
---------- ---------------------  ---------------
vs1        BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                   SeRestorePrivilege
vs1        CIFS_SERVER\sue         SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

Configurar la comprobación de recorrido de derivación

Obtenga información sobre cómo configurar la comprobación de travesía de derivación de SMB de ONTAP

La comprobación de recorrido de omisión es un derecho de usuario (también conocido como *Privilege*) que determina si un usuario puede recorrer todos los directorios de la ruta de acceso a un archivo incluso si el usuario no tiene permisos en el directorio de recorrido. Debe comprender lo que sucede al permitir o dejar de permitir la comprobación de recorrido por omisión, y cómo configurar la comprobación de recorrido por omisión para los usuarios en máquinas virtuales de almacenamiento (SVM).

Qué sucede cuando se permite o se despermite la comprobación de recorrido de derivación

- Si se permite, cuando un usuario intenta acceder a un archivo, ONTAP no comprueba el permiso Traverse para los directorios intermedios al determinar si se concede o deniega el acceso al archivo.
- Si no se permite, ONTAP comprueba el permiso recorrer (ejecutar) para todos los directorios de la ruta de acceso al archivo.

  Si alguno de los directorios intermedios no tiene el "'X'" (permiso de desplazamiento), ONTAP niega el acceso al archivo.

Configurar la comprobación de recorrido de derivación

Puede configurar la comprobación de recorrido de desvío mediante la interfaz de línea de comandos de ONTAP o mediante la configuración de directivas de grupo de Active Directory con este derecho de usuario.

```
`SeChangeNotifyPrivilege`El privilegio controla si los usuarios pueden
omitir la comprobación transversal.
```

- Si se la agrega a los usuarios o grupos SMB locales en la SVM o a usuarios o grupos de dominio, permite omitir el control transversal.
- Si lo elimina de usuarios o grupos SMB locales en la SVM o de usuarios o grupos de dominio, no permite omitir la comprobación cruzada.

De forma predeterminada, los siguientes grupos BUILTIN de la SVM tienen derecho a omitir la comprobación de recorrido:

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`
- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

Si no desea permitir a los miembros de uno de estos grupos omitir la comprobación de recorrido, debe quitar este privilegio del grupo.

Debe tener en cuenta lo siguiente al configurar la comprobación de derivación cruzada de usuarios y grupos de SMB locales en la SVM mediante la CLI:

- Si desea permitir que los miembros de un grupo local o de dominio personalizado omitan la comprobación transversal, debe agregar el `SeChangeNotifyPrivilege` privilegio a ese grupo.
- Si desea permitir que un usuario local o de dominio individual omita la comprobación transversal y que ese usuario no sea miembro de un grupo con ese privilegio, puede agregar el `SeChangeNotifyPrivilege` privilegio a esa cuenta de usuario.
- Puede desactivar la comprobación transversal de omisión para usuarios o grupos locales o de dominio eliminando el `SeChangeNotifyPrivilege` privilegio en cualquier momento.

Para desactivar la comprobación de bypass travers para usuarios o grupos locales o de dominio especificados, también debe eliminar el `SeChangeNotifyPrivilege` privilegio del `Everyone` grupo.

Información relacionada

- Permitir a los usuarios o grupos omitir la comprobación de recorrido del directorio
- No permitir a los usuarios o grupos omitir la comprobación de recorrido del directorio
- Configurar la asignación de caracteres para la traducción de nombres de archivos en volúmenes
- Crear listas de control de acceso a recursos compartidos
- Acceso seguro a archivos mediante Storage-Level Access Guard
- Lista de privilegios compatibles
- Añada privilegios a usuarios o grupos locales o de dominio

Permitir que los usuarios o grupos omitan la verificación del recorrido del directorio SMB de ONTAP

Si desea que un usuario pueda recorrer todos los directorios de la ruta a un archivo, aunque el usuario no tenga permisos en un directorio cruzado, puede añadir el `SeChangeNotifyPrivilege` privilegio a grupos o usuarios locales de SMB en máquinas virtuales de almacenamiento (SVM). De forma predeterminada, los usuarios pueden omitir la comprobación de recorrido del directorio.

Antes de empezar

- Debe haber un servidor SMB en la SVM.
- Debe habilitarse la opción del servidor SMB para los usuarios locales y los grupos.
- El usuario o grupo local o de dominio al que se `SeChangeNotifyPrivilege` agregará el privilegio debe existir ya.

Acerca de esta tarea

Al agregar privilegios a un usuario o grupo de dominio, ONTAP puede validar el usuario o grupo de dominio poniéndose en contacto con el controlador de dominio. Es posible que se produzca un error en el comando si ONTAP no puede comunicarse con la controladora de dominio.

Pasos

1. Active la comprobación de desvío mediante la adición `SeChangeNotifyPrivilege` del privilegio a un usuario o grupo local o de dominio: `vserver cifs users-and-groups privilege add-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`* `-privileges SeChangeNotifyPrivilege`

   El valor del `-user-or-group-name` parámetro es un usuario o un grupo local, o un usuario o un grupo de dominio.

2. Compruebe que el usuario o grupo especificado tiene activada la comprobación de desvío de desvío: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Ejemplo

El siguiente comando permite a los usuarios que pertenecen al grupo «`EJEMPLO\eng`» omitir la comprobación

de desplazamiento de directorios agregando el `SeChangeNotifyPrivilege` privilegio al grupo:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       EXAMPLE\eng          SeChangeNotifyPrivilege
```

Información relacionada

No permitir a los usuarios o grupos omitir la comprobación de recorrido del directorio

No permitir que usuarios o grupos omitan la comprobación del recorrido del directorio SMB de ONTAP

Si no desea que un usuario recorra todos los directorios de la ruta a un archivo porque el usuario no tiene permisos en el directorio cruzado, puede quitar el `SeChangeNotifyPrivilege` privilegio de los usuarios o grupos locales de SMB en las máquinas virtuales de almacenamiento (SVM).

Antes de empezar

Debe haber ya el usuario o grupo local o de dominio del que se eliminarán los privilegios.

Acerca de esta tarea

Al eliminar privilegios de un usuario o grupo de dominio, ONTAP puede validar el usuario o grupo de dominio poniéndose en contacto con el controlador de dominio. Es posible que se produzca un error en el comando si ONTAP no puede comunicarse con la controladora de dominio.

Pasos

1. No permitir la comprobación de desvío: `vserver cifs users-and-groups privilege remove-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`* `-privileges SeChangeNotifyPrivilege`

   El comando quita `SeChangeNotifyPrivilege` el privilegio del usuario o grupo local o de dominio que se especifique con el valor del `-user-or-group-name` *`name`* parámetro.

2. Compruebe que el usuario o grupo especificado tiene desactivada la comprobación de desvío: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Ejemplo

El siguiente comando evita que los usuarios que pertenecen al grupo "'EXAMPLE\eng'" pasen por alto la comprobación de recorrido del directorio:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ----------------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ----------------------
vs1       EXAMPLE\eng           -
```

Información relacionada

Permitir a los usuarios o grupos omitir la comprobación de recorrido del directorio

Muestra información acerca de las políticas de auditoría y seguridad de archivos

Obtenga información sobre cómo visualizar las políticas de seguridad y auditoría de archivos SMB de ONTAP

Puede mostrar información sobre la seguridad de los archivos y directorios contenidos en volúmenes en máquinas virtuales de almacenamiento (SVM). Puede mostrar información sobre las políticas de auditoría en los volúmenes de FlexVol. Si se configura, se puede mostrar información acerca de las opciones de seguridad Protección del acceso a nivel de almacenamiento y Control de acceso dinámico en volúmenes de FlexVol.

Mostrar información acerca de la seguridad de archivos

Puede visualizar la información sobre la seguridad de los archivos aplicada a los datos contenidos en volúmenes y qtrees (para volúmenes FlexVol) con los siguientes estilos de seguridad:

- NTFS
- UNIX
- Mixto

Visualización de información acerca de las directivas de auditoría

Puede mostrar información sobre las políticas de auditoría para auditar eventos de acceso en los volúmenes FlexVol mediante los siguientes protocolos NAS:

- SMB (todas las versiones)
- NFSv4.x

Mostrar información acerca de la seguridad de la protección de acceso a nivel de almacenamiento (SLAG)

La seguridad de protección de acceso a nivel de almacenamiento se puede aplicar en volúmenes de FlexVol y objetos de qtree con los siguientes estilos de seguridad:

- NTFS
- Mixto
- UNIX (si se configura un servidor CIFS en la SVM que contiene el volumen)

Mostrar información acerca de la seguridad del control de acceso dinámico (DAC)

La seguridad de control de acceso dinámico se puede aplicar a un objeto dentro de un volumen FlexVol con los siguientes estilos de seguridad:

- NTFS
- Mixto (si el objeto tiene seguridad efectiva NTFS)

Información relacionada

- Obtenga información sobre el acceso seguro a archivos mediante Storage-Level Access Guard
- Mostrar información sobre la protección de acceso a nivel de almacenamiento en los servidores

Mostrar información sobre la seguridad de archivos SMB de ONTAP en volúmenes de estilo de seguridad NTFS

Puede mostrar información acerca de la seguridad de archivos y directorios en volúmenes de estilo de seguridad NTFS, incluidos el estilo de seguridad y los estilos de seguridad efectivos, los permisos que se aplican e información acerca de los atributos dos. Puede utilizar los resultados para validar la configuración de seguridad o solucionar problemas de acceso a archivos.

Acerca de esta tarea

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los datos cuya información de seguridad de archivo o carpeta desee mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

- Debido a que los volúmenes y qtrees de estilo de seguridad NTFS utilizan sólo permisos de archivo NTFS y usuarios y grupos de Windows al determinar los derechos de acceso a archivos, los campos de salida relacionados con UNIX contienen información de permisos de archivo UNIX de sólo visualización.
- Se muestra la salida de ACL para archivos y carpetas con seguridad NTFS.
- Como la seguridad de Access Guard a nivel de almacenamiento se puede configurar en el volumen raíz o en el qtree, la salida de un volumen o una ruta de qtree en la que se configure la protección de acceso a nivel de almacenamiento puede mostrar tanto ACL de archivos normales como ACL de Storage-Level Access Guard.
- El resultado también muestra información acerca de los ACE de control de acceso dinámico si el Control de acceso dinámico está configurado para la ruta de acceso de archivo o directorio indicada.

Paso

1. Mostrar la configuración de seguridad de archivos y directorios con el nivel de detalle deseado:

Si desea mostrar información…	Introduzca el siguiente comando…
En forma de resumen	`vserver security file-directory show -vserver vserver_name -path path`
Con detalle ampliado	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Ejemplos

En el ejemplo siguiente se muestra información de seguridad sobre la ruta de `/vol4` SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                Vserver: vs1
                              File Path: /vol4
                      File Inode Number: 64
                         Security Style: ntfs
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                          Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                          ALLOW-Everyone-0x1f01ff
                                          ALLOW-Everyone-0x10000000-
OI|CI|IO
```

En el siguiente ejemplo, se muestra la información de seguridad con máscaras expandidas sobre la ruta de `/data/engineering` SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

               Vserver: vs1
             File Path: /data/engineering
     File Inode Number: 5544
```

```
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
          Unix User Id: 0
         Unix Group Id: 0
        Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
                             ...0 .... .... .... .... .... .... .... =
```

```
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
```

```
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
                              .... .... .... ..0. .... .... .... .... =
Read Control
                              .... .... .... ...0 .... .... .... .... =
Delete
                              .... .... .... .... .... ...0 .... .... =
Write Attributes
                              .... .... .... .... .... .... 0... .... =
Read Attributes
                              .... .... .... .... .... .... .0.. .... =
Delete Child
                              .... .... .... .... .... .... ..0. .... =
Execute
                              .... .... .... .... .... .... ...0 .... =
Write EA
                              .... .... .... .... .... .... .... 0... =
Read EA
                              .... .... .... .... .... .... .... .0.. =
Append
                              .... .... .... .... .... .... .... ..0. =
Write
                              .... .... .... .... .... .... .... ...0 =
Read
```

En el siguiente ejemplo, se muestra información de seguridad, incluida la información de seguridad de Storage-Level Access Guard, del volumen con la ruta `/datavol1` en SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Información relacionada

- Muestra información sobre la seguridad de archivos en volúmenes mixtos de estilo de seguridad
- Muestra información sobre la seguridad de archivos en volúmenes de estilo de seguridad UNIX

Mostrar información sobre la seguridad de los archivos SMB de ONTAP en volúmenes de estilo de seguridad mixto

Puede mostrar información acerca de la seguridad de archivos y directorios en volúmenes mixtos de estilo de seguridad, incluidos el estilo de seguridad y los estilos de seguridad efectivos, los permisos que se aplican y la información acerca de los propietarios y grupos de UNIX. Puede utilizar los resultados para validar la configuración de seguridad o solucionar problemas de acceso a archivos.

Acerca de esta tarea

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los datos cuya información de seguridad de archivo o carpeta desee mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

- Los volúmenes y qtrees de estilo de seguridad mixtos pueden contener archivos y carpetas que utilizan permisos de archivo de UNIX, bits de modo o ACL de NFSv4 y algunos archivos y directorios que utilizan permisos de archivo NTFS.
- El nivel superior de un volumen mixto de estilo de seguridad puede tener una seguridad efectiva de UNIX o NTFS.
- La salida de ACL se muestra solo para archivos y carpetas con seguridad NTFS o NFSv4.

  Este campo está vacío para archivos y directorios que utilizan la seguridad de UNIX que solo tienen aplicados permisos de bit de modo (sin ACL de NFSv4).

- Los campos de salida de propietario y grupo de la salida ACL se aplican sólo en el caso de los descriptores de seguridad NTFS.
- Debido a que la seguridad de Access Guard a nivel de almacenamiento se puede configurar en un volumen o qtree de estilo de seguridad mixto incluso si el estilo de seguridad efectivo del volumen raíz o qtree es UNIX, La salida de un volumen o una ruta de qtree en la que se configure Storage-Level Access Guard podría mostrar tanto los permisos de archivos UNIX como las ACL de Storage-Level Access Guard.
- Si la ruta de acceso introducida en el comando es a datos con seguridad efectiva de NTFS, el resultado también muestra información acerca de ACE de Control de acceso dinámico si Control de acceso dinámico está configurado para el archivo o la ruta de acceso de directorio dada.

Paso

1. Mostrar la configuración de seguridad de archivos y directorios con el nivel de detalle deseado:

Si desea mostrar información…	Introduzca el siguiente comando…
En forma de resumen	`vserver security file-directory show -vserver vserver_name -path path`
Con detalle ampliado	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Ejemplos

El siguiente ejemplo muestra la información de seguridad sobre la ruta de `/projects` SVM VS1 en formato de máscara expandida. Esta ruta mixta de estilo de seguridad tiene una seguridad efectiva de UNIX.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

               Vserver: vs1
             File Path: /projects
      File Inode Number: 78
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
          Unix User Id: 0
         Unix Group Id: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

En el ejemplo siguiente se muestra información de seguridad sobre la ruta de `/data` SVM VS1. Esta ruta mixta de estilo de seguridad tiene una seguridad NTFS efectiva.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

                                Vserver: vs1
                              File Path: /data
                      File Inode Number: 544
                         Security Style: mixed
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                            ALLOW-Everyone-0x1f01ff
                                            ALLOW-Everyone-0x10000000-
OI|CI|IO
```

En el ejemplo siguiente se muestra información de seguridad sobre el volumen en la ruta de `/datavol5` SVM VS1. El nivel superior de este volumen mixto de estilo de seguridad ofrece una seguridad efectiva para UNIX. El volumen tiene seguridad de protección de acceso en el nivel de almacenamiento.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
```

Información relacionada

- Muestra información sobre la seguridad de archivos en volúmenes de estilo de seguridad NTFS
- Muestra información sobre la seguridad de archivos en volúmenes de estilo de seguridad UNIX

Mostrar información sobre la seguridad de archivos SMB de ONTAP en volúmenes de estilo de seguridad UNIX

Puede mostrar información acerca de la seguridad de archivos y directorios en los volúmenes de estilo de seguridad de UNIX, incluidos los estilos de seguridad y los estilos

de seguridad efectivos, los permisos que se aplican y la información acerca de los propietarios y grupos de UNIX. Puede utilizar los resultados para validar la configuración de seguridad o solucionar problemas de acceso a archivos.

Acerca de esta tarea

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los datos cuyo archivo o información de seguridad de directorio desee mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

- Los volúmenes y qtrees de estilo de seguridad de UNIX solo utilizan permisos de archivos UNIX, ya sea bits de modo o ACL de NFSv4 al determinar los derechos de acceso a los archivos.
- La salida de ACL se muestra solo para los archivos y las carpetas con seguridad de NFSv4.

  Este campo está vacío para archivos y directorios que utilizan la seguridad de UNIX que solo tienen aplicados permisos de bit de modo (sin ACL de NFSv4).

- Los campos de salida de propietario y grupo de la salida de ACL no se aplican en el caso de los descriptores de seguridad de NFSv4.

  Sólo son significativos para los descriptores de seguridad NTFS.

- Como la seguridad de Access Guard en el nivel de almacenamiento se admite en un volumen UNIX o qtree si hay un servidor CIFS configurado en la SVM, el resultado puede contener información sobre la seguridad de Access Guard en el nivel de almacenamiento aplicada al volumen o qtree especificados en el `-path` parámetro.

Paso

1. Mostrar la configuración de seguridad de archivos y directorios con el nivel de detalle deseado:

Si desea mostrar información…	Introduzca el siguiente comando…
En forma de resumen	`vserver security file-directory show -vserver` *vserver_name* `-path` *path*
Con detalle ampliado	`vserver security file-directory show -vserver` *vserver_name* `-path` *path* `-expand-mask true`

Ejemplos

En el ejemplo siguiente se muestra información de seguridad sobre la ruta de `/home` SVM VS1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

El siguiente ejemplo muestra la información de seguridad sobre la ruta de `/home` SVM VS1 en formato de máscara expandida:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: 0x10
                    ...0 .... .... .... = Offline
                    .... ..0. .... .... = Sparse
                    .... .... 0... .... = Normal
                    .... .... ..0. .... = Archive
                    .... .... ...1 .... = Directory
                    .... .... .... .0.. = System
                    .... .... .... ..0. = Hidden
                    .... .... .... ...0 = Read Only
                           Unix User Id: 0
                          Unix Group Id: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

Información relacionada

- Mostrar información sobre la seguridad de los archivos en volúmenes de estilo de seguridad
- Muestra información sobre la seguridad de archivos en volúmenes mixtos de estilo de seguridad

Comandos de ONTAP para mostrar información sobre las políticas de auditoría de NTFS en volúmenes SMB FlexVol

Puede mostrar información acerca de las directivas de auditoría NTFS en los volúmenes FlexVol, incluidos los estilos de seguridad y los estilos de seguridad efectivos, los permisos que se aplican e información acerca de las listas de control de acceso al sistema. Puede utilizar los resultados para validar la configuración de seguridad o para solucionar problemas de auditoría.

Acerca de esta tarea

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los archivos o carpetas cuya información de auditoría desee mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

- Los volúmenes y qtrees de estilo de seguridad NTFS sólo utilizan listas de control de acceso al sistema (SACL) NTFS para las directivas de auditoría.
- Los archivos y carpetas de un volumen mixto de estilo de seguridad con seguridad efectiva NTFS pueden tener directivas de auditoría NTFS aplicadas.

  Los volúmenes y qtrees de estilo de seguridad mixtos pueden contener archivos y directorios que utilizan permisos de archivo de UNIX, bits de modo o ACL de NFSv4 y algunos archivos y directorios que utilizan permisos de archivo NTFS.

- El nivel superior de un volumen de estilo de seguridad mixto puede tener seguridad efectiva de UNIX o NTFS y puede que no contenga SACL NTFS.
- Debido a que la seguridad de Access Guard a nivel de almacenamiento se puede configurar en un volumen o qtree de estilo de seguridad mixto incluso si el estilo de seguridad efectivo del volumen raíz o qtree es UNIX, El resultado de una ruta de volumen o qtree en la que se configuró Storage-Level Access Guard puede mostrar tanto el archivo normal como la carpeta NFSv4 SACL y Storage-Level Access Guard NTFS SACL.
- Si la ruta de acceso que se introduce en el comando es para los datos con seguridad efectiva NTFS, la salida también muestra información sobre los ACE de control dinámico de acceso si el Control dinámico de acceso está configurado para la ruta de acceso del archivo o directorio dada.
- Cuando se muestra información de seguridad sobre archivos y carpetas con seguridad efectiva NTFS, los campos de salida relacionados con UNIX contienen información de permisos de archivo UNIX de sólo visualización.

  Los archivos y carpetas de estilo de seguridad NTFS utilizan sólo permisos de archivo NTFS y usuarios y grupos de Windows al determinar los derechos de acceso a archivos.

- El resultado de ACL se muestra solo para los archivos y las carpetas con seguridad NTFS o NFSv4.

  Este campo está vacío para archivos y carpetas que utilizan la seguridad de UNIX que solo tienen aplicados permisos de bit de modo (sin ACL de NFSv4).

- Los campos de salida de propietario y grupo de la salida ACL se aplican sólo en el caso de los descriptores de seguridad NTFS.

Paso

1. Mostrar la configuración de la directiva de auditoría de archivos y directorios con el nivel de detalle deseado:

Si desea mostrar información…	Introduzca el siguiente comando…
En forma de resumen	`vserver security file-directory show -vserver vserver_name -path path`
Como una lista detallada	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Ejemplos

En el siguiente ejemplo, se muestra información de política de auditoría para la ruta `/corp` en SVM VS1. La ruta de acceso tiene seguridad efectiva NTFS. El descriptor de seguridad NTFS contiene UNA entrada SACL CORRECTA y UNA entrada SACL SUCCESS/FAIL.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

En el siguiente ejemplo, se muestra información de política de auditoría para la ruta `/datavol1` en SVM VS1. La ruta de acceso contiene tanto SACL de archivo normal como de carpeta y SACL de Storage-Level Access

Guard.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Comandos de ONTAP para mostrar información sobre las políticas de auditoría de NFSv4 en volúmenes SMB FlexVol

Puede mostrar información sobre las políticas de auditoría de NFSv4 en volúmenes de FlexVol mediante la interfaz de línea de comandos de ONTAP, incluidos los estilos de seguridad y los estilos de seguridad efectivos, qué permisos se aplican e información sobre las listas de control de acceso del sistema (SACL). Puede utilizar los resultados para validar la configuración de seguridad o para solucionar problemas de auditoría.

Acerca de esta tarea

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los archivos o directorios cuya información de auditoría desea mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

- Los volúmenes y qtrees de estilo de seguridad de UNIX solo utilizan NFSv4 SACL para las políticas de auditoría.
- Los archivos y directorios de un volumen de estilo de seguridad mixto que sea de estilo de seguridad UNIX pueden hacer que se les apliquen las políticas de auditoría de NFSv4.

  Los volúmenes y qtrees de estilo de seguridad mixtos pueden contener archivos y directorios que utilizan permisos de archivo de UNIX, bits de modo o ACL de NFSv4 y algunos archivos y directorios que utilizan permisos de archivo NTFS.

- El nivel superior de un volumen con estilo de seguridad mixto puede tener seguridad efectiva de UNIX o NTFS y puede que contenga o no SACL de NFSv4.
- La salida de ACL se muestra solo para archivos y carpetas con seguridad NTFS o NFSv4.

  Este campo está vacío para archivos y carpetas que utilizan la seguridad de UNIX que solo tienen aplicados permisos de bit de modo (sin ACL de NFSv4).

- Los campos de salida de propietario y grupo de la salida ACL se aplican sólo en el caso de los descriptores de seguridad NTFS.
- Debido a que la seguridad de Access Guard a nivel de almacenamiento se puede configurar en un volumen o qtree de estilo de seguridad mixto incluso si el estilo de seguridad efectivo del volumen raíz o qtree es UNIX, Los resultados de una ruta de volumen o qtree en la que se configuró Storage-Level Access Guard pueden mostrar tanto el archivo NFSv4 normal como las SACL de directorio y las SACL de Storage-Level Access Guard.
- Como la seguridad de Access Guard en el nivel de almacenamiento se admite en un volumen UNIX o qtree si hay un servidor CIFS configurado en la SVM, el resultado puede contener información sobre la seguridad de Access Guard en el nivel de almacenamiento aplicada al volumen o qtree especificados en el `-path` parámetro.

Pasos

1. Mostrar la configuración de seguridad de archivos y directorios con el nivel de detalle deseado:

Si desea mostrar información…	Introduzca el siguiente comando…
En forma de resumen	`vserver security file-directory show -vserver vserver_name -path path`

Si desea mostrar información…	Introduzca el siguiente comando…
Con detalle ampliado	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Ejemplos

En el ejemplo siguiente se muestra información de seguridad sobre la ruta de `/lab` SVM VS1. Esta ruta de seguridad de UNIX tiene un SACL de NFSv4.

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

Aprenda a mostrar información sobre políticas de auditoría y seguridad de archivos SMB de ONTAP

Puede utilizar el carácter comodín (*) para mostrar información acerca de las directivas de auditoría y seguridad de archivos de todos los archivos y directorios de una ruta de acceso determinada o de un volumen raíz.

El carácter comodín (**) se puede utilizar como último subcomponente de una ruta de directorio dada debajo de la cual se desea mostrar información de todos los archivos y directorios. Si desea mostrar información de un archivo o directorio concreto denominado «*»**, deberá proporcionar la ruta completa dentro de comillas dobles (»'"').

Ejemplo

El siguiente comando con carácter comodín muestra la información de todos los archivos y directorios debajo de la ruta de `/1/` SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

El siguiente comando muestra la información de un archivo llamado “*” bajo la ruta de `/vol1/a` SVM VS1. La ruta está entre comillas dobles (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                Vserver: vs1
              File Path: "/vol1/a/*"
      Security Style: mixed
     Effective Style: unix
      DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
         Unix User Id: 1002
        Unix Group Id: 65533
       Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                  ACLs: NFSV4 Security Descriptor
                        Control:0x8014
                        SACL - ACEs
                          AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                        DACL - ACEs
                          ALLOW-EVERYONE@-0x1f00a9-FI|DI
                          ALLOW-OWNER@-0x1f01ff-FI|DI
                          ALLOW-GROUP@-0x1200a9-IG
```

Gestione la seguridad de archivos NTFS, políticas de auditoría NTFS y Storage-Level Access Guard mediante la CLI

Comandos ONTAP para administrar la seguridad de archivos NTFS de SMB, las políticas de auditoría de NTFS y la protección de acceso a nivel de almacenamiento

Puede gestionar la seguridad de archivos NTFS, políticas de auditoría de NTFS y Storage-Level Access Guard en máquinas virtuales de almacenamiento (SVM) mediante la interfaz de línea de comandos.

Puede gestionar las políticas de auditoría y seguridad de archivos NTFS desde clientes SMB o mediante la CLI. Sin embargo, al utilizar la interfaz de línea de comandos para configurar las políticas de seguridad de los archivos y de auditoría, no es necesario utilizar un cliente remoto para gestionar la seguridad de los archivos. El uso de la CLI puede reducir significativamente el tiempo que lleva aplicar la seguridad en muchos archivos y carpetas mediante un único comando.

Puede configurar la protección de acceso al nivel de almacenamiento, que es otra capa de seguridad aplicada por ONTAP a los volúmenes de SVM. Storage-Level Access Guard se aplica a los accesos desde todos los protocolos NAS al objeto de almacenamiento al que se aplica la protección de acceso a nivel de almacenamiento.

El protector de acceso a nivel de almacenamiento se puede configurar y gestionar solo desde la interfaz de línea de comandos de ONTAP. No se puede gestionar la configuración de Access Guard en el nivel de almacenamiento desde clientes SMB. Además, si ve la configuración de seguridad en un archivo o un directorio desde un cliente NFS o SMB, no verá la seguridad Storage-Level Access Guard. La seguridad de

protección de acceso a nivel de almacenamiento no se puede revocar de un cliente, ni siquiera por un administrador de sistema (Windows o UNIX). Por lo tanto, Storage-Level Access Guard ofrece una capa adicional de seguridad para el acceso a los datos que el administrador de almacenamiento establece y gestiona independientemente.

> Aunque solo se admiten permisos de acceso NTFS para Storage-Level Access Guard, ONTAP puede realizar comprobaciones de seguridad para acceder a través de NFS a datos en volúmenes donde se aplica Storage-Level Access Guard si el usuario UNIX se asigna a un usuario de Windows en la SVM propietaria del volumen.

Volúmenes de estilo de seguridad de NTFS

Todos los archivos y carpetas contenidos en qtrees y volúmenes de estilo de seguridad NTFS tienen una seguridad efectiva de NTFS. Puede utilizar `vserver security file-directory` la familia de comandos para implementar los siguientes tipos de seguridad en volúmenes de estilo de seguridad NTFS:

- Los permisos de archivo y las políticas de auditoría a los archivos y las carpetas que contiene el volumen
- Seguridad para proteger el acceso al nivel de almacenamiento en los volúmenes

Volúmenes mixtos de estilo de seguridad

Los volúmenes y qtrees de estilo de seguridad mixtos pueden contener algunos archivos y carpetas con seguridad efectiva de UNIX y usar permisos de archivos de UNIX, bits de modo o ACL de NFSv4.x y políticas de auditoría de NFSv4.x, y algunos archivos y carpetas que tengan seguridad efectiva de NTFS y usen permisos de archivos NTFS y políticas de auditoría. Puede utilizar `vserver security file-directory` la familia de comandos para aplicar los siguientes tipos de seguridad a los datos mixtos de estilo de seguridad:

- Permisos de archivo y políticas de auditoría para archivos y carpetas con un estilo de seguridad NTFS efectivo en el volumen o qtree mixtos
- Protección del acceso a nivel de almacenamiento para volúmenes con seguridad efectiva de NTFS y UNIX

Volúmenes de estilo de seguridad de UNIX

Los volúmenes y qtrees de estilo de seguridad de UNIX contienen archivos y carpetas que tienen una seguridad efectiva de UNIX (bits de modo o ACL de NFSv4.x). Debe tener en cuenta lo siguiente si desea utilizar `vserver security file-directory` la familia de comandos para implementar la seguridad en volúmenes de estilo de seguridad de UNIX:

- `vserver security file-directory`La familia de comandos no se puede utilizar para gestionar las políticas de auditoría y seguridad de archivos UNIX en volúmenes y qtrees de tipo de seguridad de UNIX.
- `vserver security file-directory`La familia de comandos se puede usar para configurar Storage-Level Access Guard en volúmenes de estilo de seguridad de UNIX, siempre y cuando la SVM con el volumen de destino contenga un servidor CIFS.

Información relacionada

- Obtenga información sobre cómo visualizar las políticas de seguridad y auditoría de archivos
- Crear descriptores de seguridad NTFS en servidores
- Comandos para configurar y aplicar políticas de auditoría a archivos y carpetas
- Obtenga información sobre el acceso seguro a archivos mediante Storage-Level Access Guard

Comandos ONTAP para configurar la seguridad de archivos y carpetas SMB

Dado que puede aplicar y administrar la seguridad de archivos y carpetas localmente sin la participación de un cliente remoto, puede reducir significativamente el tiempo que tarda en establecer la seguridad masiva en un gran número de archivos o carpetas.

Puede beneficiarse del uso de la CLI para establecer la seguridad de archivos y carpetas en los siguientes casos de uso:

- Almacenamiento de ficheros en entornos empresariales de gran tamaño, como el almacenamiento de ficheros en directorios iniciales
- Migración de datos
- Cambio de dominio de Windows
- Estandarización de las políticas de auditoría y seguridad de archivos en sistemas de archivos NTFS

Conozca los límites al usar comandos ONTAP para configurar la seguridad de archivos y carpetas SMB

Debe estar al tanto de determinados límites cuando utilice la CLI para establecer la seguridad de archivos y carpetas.

- `vserver security file-directory`La familia de comandos no admite la configuración de ACL NFSv4.

  Sólo puede aplicar descriptores de seguridad NTFS a archivos y carpetas NTFS.

Utilice descriptores de seguridad para aplicar la seguridad de archivos y carpetas SMB de ONTAP

Los descriptores de seguridad contienen las listas de control de acceso que determinan qué acciones puede realizar un usuario en archivos y carpetas, y qué se audita cuando un usuario accede a archivos y carpetas.

- **Permisos**

  El propietario de un objeto permite o deniega los permisos y determina qué acciones puede realizar un objeto (usuarios, grupos u objetos de equipo) en archivos o carpetas especificados.

- **Descriptores de seguridad**

  Los descriptores de seguridad son estructuras de datos que contienen información de seguridad que definen los permisos asociados a un archivo o carpeta.

- **Listas de control de acceso (ACL)**

  Las listas de control de acceso son las listas contenidas en un descriptor de seguridad que contienen información sobre las acciones que los usuarios, grupos o objetos de equipo pueden realizar en el archivo o la carpeta a la que se aplica el descriptor de seguridad. El descriptor de seguridad puede contener los siguientes dos tipos de ACL:

  - Listas de control de acceso discrecional (DACL)
  - Listas de control de acceso del sistema (SACL)
- **Listas de control de acceso discrecional (DACL)**

Las DACL contienen la lista de SIDS para los usuarios, grupos y objetos de equipo a los que se permite o deniega el acceso para realizar acciones en archivos o carpetas. Las DACL contienen entradas de control de acceso cero o más (ACE).

- **Listas de control de acceso al sistema (SACL)**

  SACL contiene la lista de SID para los usuarios, grupos y objetos de equipo para los que se registran eventos de auditoría correctos o fallidos. Las SACL contienen entradas de control de acceso cero o más (ACE).

- **Entradas de control de acceso (ACE)**

  Las ACE son entradas individuales en DACL o SACL:

  - Una entrada de control de acceso DACL especifica los derechos de acceso que se permiten o deniegan para determinados usuarios, grupos o objetos de equipo.
  - Una entrada de control de acceso SACL especifica los eventos de éxito o de error que se deben registrar al auditar acciones especificadas realizadas por usuarios, grupos o objetos de equipo específicos.

- **Herencia de permisos**

  La herencia de permisos describe cómo los permisos definidos en los descriptores de seguridad se propagan a un objeto de un objeto primario. Sólo los objetos secundarios heredan los permisos heredables. Al establecer permisos en el objeto padre, puede decidir si las carpetas, subcarpetas y archivos pueden heredarlos con «`Aplicar a this-folder`, `sub-folders` y `archivos`».

Información relacionada

- "Seguimiento de seguridad y auditoría de SMB y NFS"
- Comandos para configurar y aplicar políticas de auditoría a archivos y carpetas

Obtenga información sobre cómo aplicar políticas de directorio de archivos que utilizan usuarios o grupos SMB locales en el destino de recuperación ante desastres de ONTAP SVM

Hay ciertas directrices que debe tener en cuenta antes de aplicar políticas de directorio de archivos en el destino de recuperación ante desastres de la máquina virtual de almacenamiento (SVM) en una configuración de descarte de ID si la configuración de la política de directorio de archivos usa usuarios o grupos locales en el descriptor de seguridad, o en las entradas DACL o SACL.

Puede configurar una configuración de recuperación ante desastres para una SVM donde la SVM de origen en el clúster de origen replica los datos y la configuración desde la SVM de origen a una SVM de destino en un clúster de destino.

Puede configurar uno de los dos tipos de recuperación ante desastres de SVM:

- Se conserva la identidad

  Con esta configuración se conserva la identidad de la SVM y el servidor CIFS.

- Identidad descartada

  Con esta configuración, no se conserva la identidad de la SVM y el servidor CIFS. En esta situación, el

nombre de la SVM y el servidor CIFS en la SVM de destino es diferente de la SVM y del nombre del servidor CIFS en la SVM de origen.

Directrices para configuraciones de identidad descartadas

En una configuración de identidad descartada, en el caso de un origen de SVM que contenga configuraciones de usuarios locales, grupos y privilegios, se debe cambiar el nombre del dominio local (nombre del servidor CIFS local) para que coincida con el nombre del servidor CIFS en el destino de SVM. Por ejemplo, si el nombre de la SVM de origen es «'vs1'» y el nombre del servidor CIFS es «'CIFS1'» y el nombre de la SVM de destino es «'vs1_dst'» y el nombre del servidor CIFS es «'CIFS1_DST», el nombre de dominio local de un usuario local denominado «'CIFS1\user1' se cambia automáticamente a «CIFS1» en el destino».

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1_dst      CIFS1_DST\Administrator                 Built-in
administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

Aunque los nombres de usuario local y de grupos se modifican automáticamente en las bases de datos de usuario local y de grupos, los usuarios locales o los nombres de grupo no se modifican automáticamente en las configuraciones de las políticas de directorio de archivos (las políticas configuradas en la interfaz de línea de `vserver security file-directory` comandos mediante la familia de comandos).

Por ejemplo, para «`VS1`», si ha configurado una entrada DACL en la que el `-account` parámetro se establece en «`CIFS1\user1`», la configuración no se cambia automáticamente en la SVM de destino para reflejar el nombre del servidor CIFS del destino.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

Debe utilizar `vserver security file-directory modify` los comandos para cambiar manualmente el nombre del servidor CIFS al nombre del servidor CIFS de destino.

Componentes de configuración de directivas de directorio de archivos que contienen parámetros de cuenta

Existen tres componentes de configuración de directivas de directorio de archivos que pueden utilizar parámetros que pueden contener usuarios o grupos locales:

- Descriptor de seguridad

  Opcionalmente, puede especificar el propietario del descriptor de seguridad y el grupo primario del propietario del descriptor de seguridad. Si el descriptor de seguridad utiliza un usuario o grupo local para las entradas del propietario y del grupo primario, debe modificar el descriptor de seguridad para utilizar la SVM de destino en el nombre de cuenta. Puede usar el `vserver security file-directory ntfs modify` comando para realizar los cambios necesarios en los nombres de cuentas.

- Entradas de DACL

  Cada entrada de DACL debe estar asociada a una cuenta. Debe modificar todas las DACL que utilicen cuentas de usuario local o de grupo para usar el nombre de la SVM de destino. Debido a que no puede modificar el nombre de cuenta para las entradas DACL existentes, debe eliminar todas las entradas DACL con usuarios o grupos locales de los descriptores de seguridad, crear nuevas entradas DACL con los nombres de cuenta de destino corregidos y asociar estas nuevas entradas DACL con los descriptores de seguridad adecuados.

- Entradas de SACL

  Cada entrada de SACL debe estar asociada a una cuenta. Debe modificar todas las SACL que utilicen cuentas de usuario o de grupo local para utilizar el nombre de la SVM de destino. Debido a que no puede

modificar el nombre de cuenta para las entradas SACL existentes, debe eliminar todas las entradas SACL con usuarios o grupos locales de los descriptores de seguridad, crear nuevas entradas SACL con los nombres de cuenta de destino corregidos y asociar estas nuevas entradas SACL con los descriptores de seguridad adecuados.

Debe realizar los cambios necesarios en los usuarios o grupos locales utilizados en la configuración de la directiva de directorio de archivos antes de aplicar la directiva; de lo contrario, el trabajo de aplicación fallará.

Configurar y aplicar la seguridad de archivos en archivos y carpetas NTFS mediante la CLI

Crear descriptores de seguridad NTFS en servidores SMB de ONTAP

Crear un descriptor de seguridad NTFS (política de seguridad de archivos) es el primer paso para configurar y aplicar listas de control de acceso NTFS (ACL) a archivos y carpetas que residen en máquinas virtuales de almacenamiento (SVM). Puede asociar el descriptor de seguridad a la ruta de archivo o carpeta en una tarea de directiva.

Acerca de esta tarea

Puede crear descriptores de seguridad NTFS para archivos y carpetas que residen dentro de volúmenes de estilo de seguridad NTFS o para archivos y carpetas que residen en volúmenes de estilo de seguridad mixtos.

De forma predeterminada, cuando se crea un descriptor de seguridad, se agregan cuatro entradas de control de acceso de lista de control de acceso discrecional (DACL) a ese descriptor de seguridad. Los cuatro ACE predeterminados son los siguientes:

Objeto	Tipo de acceso	Derechos de acceso	Dónde aplicar los permisos
BUILTIN\Administrators	Permita	Control total	esta carpeta, subcarpetas, archivos
BUILTIN\Users	Permita	Control total	esta carpeta, subcarpetas, archivos
PROPIETARIO DEL CREADOR	Permita	Control total	esta carpeta, subcarpetas, archivos
NT AUTHORITY\SYSTEM	Permita	Control total	esta carpeta, subcarpetas, archivos

Es posible personalizar la configuración del descriptor de seguridad mediante los siguientes parámetros opcionales:

- Propietario del descriptor de seguridad
- Grupo principal del propietario
- Indicadores de control RAW

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Obtenga más información en el "Referencia de comandos del ONTAP".

Agregue entradas de control de acceso NTFS DACL a los descriptores de seguridad NTFS en servidores SMB de ONTAP

La adición de entradas de control de acceso (ACE) de DACL (lista de control de acceso discrecional) al descriptor de seguridad de NTFS es el segundo paso para configurar y aplicar ACL de NTFS a un archivo o carpeta. Cada entrada identifica qué objeto tiene permiso o acceso denegado, y define lo que el objeto puede o no puede hacer con los archivos o carpetas definidos en ACE.

Acerca de esta tarea

Puede añadir una o varias ACE a la DACL del descriptor de seguridad.

Si el descriptor de seguridad contiene una DACL que tiene ACE existentes, el comando agrega la nueva ACE a la DACL. Si el descriptor de seguridad no contiene una DACL, el comando crea la DACL y le agrega la nueva ACE.

Opcionalmente, puede personalizar las entradas DACL especificando qué derechos desea permitir o denegar para la cuenta especificada en el `-account` parámetro. Hay tres métodos mutuamente exclusivos para especificar los derechos:

- Derechos
- Derechos avanzados
- Derechos RAW (privilegio avanzado)

> Si no especifica derechos para la entrada DACL, el valor predeterminado es establecer los derechos en `Full Control`.

Opcionalmente, puede personalizar las entradas DACL especificando cómo aplicar herencia.

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

Pasos

1. Agregue una entrada DACL a un descriptor de seguridad: `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
   -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
   ```

2. Compruebe que la entrada DACL es correcta: `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

```
                Vserver: vs1
      Security Descriptor Name: sd1
                Allow or Deny: deny
           Account Name or SID: DOMAIN\joe
                 Access Rights: full-control
        Advanced Access Rights: -
                      Apply To: this-folder
                 Access Rights: full-control
```

Obtenga más información sobre `vserver security file-directory ntfs dacl` en el "Referencia de comandos del ONTAP".

Crear políticas de seguridad de ONTAP SMB

Crear una política de seguridad de archivos para SVM es el tercer paso a la hora de configurar y aplicar ACL a un archivo o carpeta. Una directiva actúa como contenedor para varias tareas, donde cada tarea es una entrada única que se puede aplicar a archivos o carpetas. Posteriormente, puede agregar tareas a la directiva de seguridad.

Acerca de esta tarea

Las tareas que agrega a una directiva de seguridad contienen asociaciones entre el descriptor de seguridad NTFS y las rutas de acceso de archivos o carpetas. Por lo tanto, debe asociar la política de seguridad con cada SVM (que contenga volúmenes de estilo de seguridad NTFS o volúmenes mixtos de estilo de seguridad).

Pasos

1. Cree una política de seguridad: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. Verifique la política de seguridad: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Agregar tareas a la política de seguridad de ONTAP SMB

Crear y añadir una tarea de política a una política de seguridad es el cuarto paso para configurar y aplicar ACL a archivos o carpetas en SVM. Al crear la tarea de directiva, asocie la tarea a una directiva de seguridad. Puede agregar una o más entradas de tareas a una directiva de seguridad.

Acerca de esta tarea

La política de seguridad es un contenedor para una tarea. Una tarea hace referencia a una única operación que puede realizar una directiva de seguridad para archivos o carpetas con seguridad NTFS o mixta (o a un objeto de volumen si se configura Storage-Level Access Guard).

Existen dos tipos de tareas:

- Tareas de archivo y directorio

  Se utiliza para especificar tareas que aplican descriptores de seguridad a archivos y carpetas especificados. Las ACL aplicadas mediante tareas de archivo y directorio se pueden gestionar con clientes de SMB o con la interfaz de línea de comandos de ONTAP.

- Tareas de protección de acceso al nivel de almacenamiento

  Se utiliza para especificar tareas que aplican descriptores de seguridad de Access Guard de nivel de almacenamiento a un volumen especificado. Las ACL aplicadas mediante tareas de protección de acceso al nivel de almacenamiento solo se pueden gestionar a través de la interfaz de línea de comandos de ONTAP.

Una tarea contiene definiciones para la configuración de seguridad de un archivo (o carpeta) o un conjunto de archivos (o carpetas). Cada tarea de una política se identifica de forma única por la ruta. Sólo puede haber una tarea por ruta dentro de una única política. Una directiva no puede tener entradas de tareas duplicadas.

Directrices para agregar una tarea a una directiva:

- Puede haber un máximo de 10,000 entradas de tareas por directiva.
- Una política puede contener una o más tareas.

  Aunque una directiva puede contener más de una tarea, no puede configurar una directiva para que contenga tareas de directorio de archivos y de protección de acceso a nivel de almacenamiento. Una política debe contener todas las tareas de Storage-Level Access Guard o todas las tareas de directorio de archivos.

- Se utiliza Storage-Level Access Guard para restringir los permisos.

  Nunca dará permisos de acceso adicionales.

Al agregar tareas a las directivas de seguridad, debe especificar los siguientes cuatro parámetros necesarios:

- Nombre de SVM
- Nombre de la política
- Ruta
- Descriptor de seguridad que se asociará a la ruta de acceso

Es posible personalizar la configuración del descriptor de seguridad mediante los siguientes parámetros opcionales:

- Tipo de seguridad
- Modo de propagación
- Posición de índice

- Tipo de control de acceso

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

Pasos

1. Agregue una tarea con un descriptor de seguridad asociado a la política de seguridad: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` es el valor predeterminado del `-access-control` parámetro. Es opcional especificar el tipo de control de acceso cuando se configuran las tareas de acceso a archivos y directorios.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
   ```

2. Verifique la configuración de la tarea de política: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

Obtenga más información sobre `vserver security file-directory policy task` en el "Referencia de comandos del ONTAP".

Aplicar las políticas de seguridad de ONTAP SMB

Aplicar una política de seguridad de archivos a las SVM es el último paso a la hora de crear y aplicar ACL de NTFS a archivos o carpetas.

Acerca de esta tarea

Puede aplicar la configuración de seguridad definida en la política de seguridad a archivos y carpetas NTFS que residen en volúmenes FlexVol (estilo de seguridad NTFS o mixto).

> Cuando se aplican una directiva de auditoría y SACL asociadas, se sobrescriben todas las DACL existentes. Cuando se aplica una directiva de seguridad y sus DACL asociados, se sobrescriben todas las DACL existentes. Debe revisar las directivas de seguridad existentes antes de crear y aplicar otras nuevas.

Paso

1. Aplicar una política de seguridad: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory apply -vserver vs1 -policy-name policy1`

   El trabajo de aplicación de política está programado y se devuelve el ID de trabajo.

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 –id
   53322" command to view the status of the operation
   ```

Supervisar los trabajos de políticas de seguridad de ONTAP SMB

Al aplicar la política de seguridad a máquinas virtuales de almacenamiento (SVM), puede supervisar el progreso de la tarea supervisando el trabajo de la política de seguridad. Esto es útil si desea comprobar que la aplicación de la política de seguridad ha sido satisfactoria. Esto también resulta útil si tiene un trabajo de larga ejecución en el que está aplicando seguridad masiva a un gran número de archivos y carpetas.

Acerca de esta tarea

Para mostrar información detallada sobre un trabajo de política de seguridad, debe utilizar el `-instance` parámetro.

Paso

1. Supervise el trabajo de política de seguridad: `vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Verificar la seguridad de los archivos SMB de ONTAP

Es posible verificar la configuración de seguridad de archivos para confirmar que los archivos o las carpetas de la máquina virtual de almacenamiento (SVM) a la que aplicó la política de seguridad tienen la configuración deseada.

Acerca de esta tarea

Debe suministrar el nombre de la SVM que contenga los datos y la ruta de acceso al archivo y las carpetas en los que desea verificar la configuración de seguridad. Puede utilizar el parámetro opcional `-expand-mask` para mostrar información detallada sobre la configuración de seguridad.

Paso

1. Mostrar configuración de seguridad de archivos y carpetas: `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

   `vserver security file-directory show -vserver vs1 -path /data/engineering -expand-mask true`

```
         Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
```

```
                        DACL - ACEs
                          ALLOW-Everyone-0x1f01ff
                            0... .... .... .... .... .... .... .... =
Generic Read
                            .0.. .... .... .... .... .... .... .... =
Generic Write
                            ..0. .... .... .... .... .... .... .... =
Generic Execute
                            ...0 .... .... .... .... .... .... .... =
Generic All
                            .... ...0 .... .... .... .... .... .... =
System Security
                            .... .... ...1 .... .... .... .... .... =
Synchronize
                            .... .... .... 1... .... .... .... .... =
Write Owner
                            .... .... .... .1.. .... .... .... .... =
Write DAC
                            .... .... .... ..1. .... .... .... .... =
Read Control
                            .... .... .... ...1 .... .... .... .... =
Delete
                            .... .... .... .... .... ...1 .... .... =
Write Attributes
                            .... .... .... .... .... .... 1... .... =
Read Attributes
                            .... .... .... .... .... .... .1.. .... =
Delete Child
                            .... .... .... .... .... .... ..1. .... =
Execute
                            .... .... .... .... .... .... ...1 .... =
Write EA
                            .... .... .... .... .... .... .... 1... =
Read EA
                            .... .... .... .... .... .... .... .1.. =
Append
                            .... .... .... .... .... .... .... ..1. =
Write
                            .... .... .... .... .... .... .... ...1 =
Read

                          ALLOW-Everyone-0x10000000-OI|CI|IO
                            0... .... .... .... .... .... .... .... =
Generic Read
                            .0.. .... .... .... .... .... .... .... =
Generic Write
```

```
                           ..0. .... .... .... .... .... .... .... =
Generic Execute
                           ...1 .... .... .... .... .... .... .... =
Generic All
                           .... ...0 .... .... .... .... .... .... =
System Security
                           .... .... ...0 .... .... .... .... .... =
Synchronize
                           .... .... .... 0... .... .... .... .... =
Write Owner
                           .... .... .... .0.. .... .... .... .... =
Write DAC
                           .... .... .... ..0. .... .... .... .... =
Read Control
                           .... .... .... ...0 .... .... .... .... =
Delete
                           .... .... .... .... .... ...0 .... .... =
Write Attributes
                           .... .... .... .... .... .... 0... .... =
Read Attributes
                           .... .... .... .... .... .... .0.. .... =
Delete Child
                           .... .... .... .... .... .... ..0. .... =
Execute
                           .... .... .... .... .... .... ...0 .... =
Write EA
                           .... .... .... .... .... .... .... 0... =
Read EA
                           .... .... .... .... .... .... .... .0.. =
Append
                           .... .... .... .... .... .... .... ..0. =
Write
                           .... .... .... .... .... .... .... ...0 =
Read
```

Configurar y aplicar directivas de auditoría a archivos y carpetas NTFS mediante la interfaz de línea de comandos

Comandos ONTAP para configurar y aplicar políticas de auditoría SMB a archivos y carpetas NTFS

Hay varios pasos que debe realizar para aplicar políticas de auditoría a archivos y carpetas NTFS cuando use la CLI de ONTAP. En primer lugar, debe crear un descriptor de seguridad NTFS y agregar SACL al descriptor de seguridad. A continuación, cree una directiva de seguridad y agregue tareas de directiva. Luego, debe aplicar la política de seguridad a una SVM.

Acerca de esta tarea

Después de aplicar la directiva de seguridad, puede supervisar el trabajo de directiva de seguridad y, a continuación, verificar la configuración de la directiva de auditoría aplicada.

> Cuando se aplican una directiva de auditoría y SACL asociadas, se sobrescriben todas las DACL existentes. Debe revisar las directivas de seguridad existentes antes de crear y aplicar otras nuevas.

Información relacionada

- Obtenga información sobre el acceso seguro a archivos mediante Storage-Level Access Guard
- Conozca los límites al usar comandos para configurar la seguridad de archivos y carpetas SMB
- Utilice descriptores de seguridad para aplicar seguridad a archivos y carpetas
- "Seguimiento de seguridad y auditoría de SMB y NFS"
- Crear descriptores de seguridad NTFS en servidores

Crear descriptores de seguridad NTFS en servidores SMB de ONTAP

Crear una política de auditoría de descriptor de seguridad NTFS es el primer paso para configurar y aplicar listas de control de acceso NTFS (ACL) a archivos y carpetas que residen en SVM. Asociará el descriptor de seguridad a la ruta de archivo o carpeta en una tarea de directiva.

Acerca de esta tarea

Puede crear descriptores de seguridad NTFS para archivos y carpetas que residen dentro de volúmenes de estilo de seguridad NTFS o para archivos y carpetas que residen en volúmenes de estilo de seguridad mixtos.

De forma predeterminada, cuando se crea un descriptor de seguridad, se agregan cuatro entradas de control de acceso de lista de control de acceso discrecional (DACL) a ese descriptor de seguridad. Los cuatro ACE predeterminados son los siguientes:

Objeto	Tipo de acceso	Derechos de acceso	Dónde aplicar los permisos
BUILTIN\Administrators	Permita	Control total	esta carpeta, subcarpetas, archivos
BUILTIN\Users	Permita	Control total	esta carpeta, subcarpetas, archivos
PROPIETARIO DEL CREADOR	Permita	Control total	esta carpeta, subcarpetas, archivos
NT AUTHORITY\SYSTEM	Permita	Control total	esta carpeta, subcarpetas, archivos

Es posible personalizar la configuración del descriptor de seguridad mediante los siguientes parámetros opcionales:

- Propietario del descriptor de seguridad
- Grupo principal del propietario
- Indicadores de control RAW

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

Pasos

1. Si desea utilizar los parámetros avanzados, configure el nivel de privilegio en advanced: `set -privilege advanced`
2. Cree un descriptor de seguridad: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   ```
   vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe
   ```

3. Compruebe que la configuración del descriptor de seguridad es correcta: `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

   ```
   vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
   ```

   ```
                                   Vserver: vs1
                         Security Descriptor Name: sd1
                  Owner of the Security Descriptor: DOMAIN\joe
   ```

4. Si se encuentra en el nivel de privilegio avanzado, vuelva al nivel de privilegio de administrador: `set -privilege admin`

Agregue entradas de control de acceso SACL NTFS a los descriptores de seguridad NTFS en servidores SMB de ONTAP

Añadir entradas de control de acceso (ACE) SACL (lista de control de acceso del sistema) al descriptor de seguridad NTFS es el segundo paso a la hora de crear directivas de auditoría NTFS para archivos o carpetas en SVM. Cada entrada identifica el usuario o grupo que desea auditar. La entrada SACL define si desea auditar los intentos de acceso fallidos o correctos.

Acerca de esta tarea

Puede añadir una o varias ACE a la SACL del descriptor de seguridad.

Si el descriptor de seguridad contiene una SACL que tiene ACE existentes, el comando agrega la nueva ACE a la SACL. Si el descriptor de seguridad no contiene una SACL, el comando crea la SACL y le agrega la nueva ACE.

Puede configurar entradas de SACL especificando los derechos que desea auditar para eventos de éxito o fallo de la cuenta especificada en el `-account` parámetro. Hay tres métodos mutuamente exclusivos para especificar los derechos:

- Derechos
- Derechos avanzados
- Derechos RAW (privilegio avanzado)

Si no especifica derechos para la entrada SACL, el valor por defecto es `Full Control`.

Opcionalmente, puede personalizar las entradas de SACL especificando cómo aplicar la herencia con el `apply to` parámetro. Si no especifica este parámetro, el valor predeterminado es aplicar esta entrada SACL a esta carpeta, subcarpetas y archivos.

Pasos

1. Agregue una entrada SACL a un descriptor de seguridad: `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
   failure -account domain\joe -rights full-control -apply-to this-folder
   -vserver vs1
   ```

2. Compruebe que la entrada de SACL es correcta: `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

   ```
                                Vserver: vs1
                  Security Descriptor Name: sd1
   Access type for Specified Access Rights: failure
                       Account Name or SID: DOMAIN\joe
                             Access Rights: full-control
                    Advanced Access Rights: -
                                  Apply To: this-folder
                             Access Rights: full-control
   ```

Crear políticas de seguridad de ONTAP SMB

Crear una política de auditoría para máquinas virtuales de almacenamiento (SVM) es el tercer paso a la hora de configurar y aplicar ACL a un archivo o una carpeta. Una directiva actúa como contenedor para varias tareas, donde cada tarea es una entrada única que se puede aplicar a archivos o carpetas. Posteriormente, puede agregar tareas a la directiva de seguridad.

Acerca de esta tarea

Las tareas que agrega a una directiva de seguridad contienen asociaciones entre el descriptor de seguridad NTFS y las rutas de acceso de archivos o carpetas. Por lo tanto, debe asociar la política de seguridad con cada máquina virtual de almacenamiento (SVM) (que contenga volúmenes de estilo de seguridad NTFS o

volúmenes mixtos de estilo de seguridad).

Pasos

1. Cree una política de seguridad: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. Verifique la política de seguridad: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Agregar tareas a la política de seguridad de ONTAP SMB

Crear y añadir una tarea de política a una política de seguridad es el cuarto paso para configurar y aplicar ACL a archivos o carpetas en SVM. Al crear la tarea de directiva, asocie la tarea a una directiva de seguridad. Puede agregar una o más entradas de tareas a una directiva de seguridad.

Acerca de esta tarea

La política de seguridad es un contenedor para una tarea. Una tarea hace referencia a una única operación que puede realizar una directiva de seguridad para archivos o carpetas con seguridad NTFS o mixta (o a un objeto de volumen si se configura Storage-Level Access Guard).

Existen dos tipos de tareas:

- Tareas de archivo y directorio

  Se utiliza para especificar tareas que aplican descriptores de seguridad a archivos y carpetas especificados. Las ACL aplicadas mediante tareas de archivo y directorio se pueden gestionar con clientes de SMB o con la interfaz de línea de comandos de ONTAP.

- Tareas de protección de acceso al nivel de almacenamiento

  Se utiliza para especificar tareas que aplican descriptores de seguridad de Access Guard de nivel de almacenamiento a un volumen especificado. Las ACL aplicadas mediante tareas de protección de acceso al nivel de almacenamiento solo se pueden gestionar a través de la interfaz de línea de comandos de ONTAP.

Una tarea contiene definiciones para la configuración de seguridad de un archivo (o carpeta) o un conjunto de archivos (o carpetas). Cada tarea de una política se identifica de forma única por la ruta. Sólo puede haber una tarea por ruta dentro de una única política. Una directiva no puede tener entradas de tareas duplicadas.

Directrices para agregar una tarea a una directiva:

- Puede haber un máximo de 10,000 entradas de tareas por directiva.

- Una política puede contener una o más tareas.

  Aunque una directiva puede contener más de una tarea, no puede configurar una directiva para que contenga tareas de directorio de archivos y de protección de acceso a nivel de almacenamiento. Una política debe contener todas las tareas de Storage-Level Access Guard o todas las tareas de directorio de archivos.

- Se utiliza Storage-Level Access Guard para restringir los permisos.

  Nunca dará permisos de acceso adicionales.

Es posible personalizar la configuración del descriptor de seguridad mediante los siguientes parámetros opcionales:

- Tipo de seguridad
- Modo de propagación
- Posición de índice
- Tipo de control de acceso

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

Pasos

1. Agregue una tarea con un descriptor de seguridad asociado a la política de seguridad: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` es el valor predeterminado del `-access-control` parámetro. Es opcional especificar el tipo de control de acceso cuando se configuran las tareas de acceso a archivos y directorios.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
   ```

2. Verifique la configuración de la tarea de política: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

Obtenga más información sobre `vserver security file-directory policy task` en el "Referencia de comandos del ONTAP".

Aplicar las políticas de seguridad de ONTAP SMB

Aplicar una política de auditoría a las SVM es el último paso a la hora de crear y aplicar ACL de NTFS a archivos o carpetas.

Acerca de esta tarea

Puede aplicar la configuración de seguridad definida en la política de seguridad a archivos y carpetas NTFS que residen en volúmenes FlexVol (estilo de seguridad NTFS o mixto).

> Cuando se aplican una directiva de auditoría y SACL asociadas, se sobrescriben todas las DACL existentes. Cuando se aplica una directiva de seguridad y sus DACL asociados, se sobrescriben todas las DACL existentes. Debe revisar las directivas de seguridad existentes antes de crear y aplicar otras nuevas.

Paso

1. Aplicar una política de seguridad: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory apply -vserver vs1 -policy-name policy1
   ```

   El trabajo de aplicación de política está programado y se devuelve el ID de trabajo.

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

Supervisar los trabajos de políticas de seguridad de ONTAP SMB

Al aplicar la política de seguridad a máquinas virtuales de almacenamiento (SVM), puede supervisar el progreso de la tarea supervisando el trabajo de la política de seguridad. Esto es útil si desea comprobar que la aplicación de la política de seguridad ha sido satisfactoria. Esto también resulta útil si tiene un trabajo de larga ejecución en el que está aplicando seguridad masiva a un gran número de archivos y carpetas.

Acerca de esta tarea

Para mostrar información detallada sobre un trabajo de política de seguridad, debe utilizar el `-instance` parámetro.

Paso

1. Supervise el trabajo de política de seguridad: `vserver security file-directory job show -vserver vserver_name`

   ```
   vserver security file-directory job show -vserver vs1
   ```

```
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
53322  Fsecurity Apply      vs1        node1          Success
       Description: File Directory Security Apply Job
```

Verificar las políticas de auditoría de ONTAP SMB

Puede verificar la política de auditoría para confirmar que los archivos o las carpetas de la máquina virtual de almacenamiento (SVM) a la que aplicó la política de seguridad tienen la configuración de seguridad de auditoría deseada.

Acerca de esta tarea

El `vserver security file-directory show` comando se utiliza para mostrar información sobre la política de auditoría. Debe proporcionar el nombre de la SVM que contiene los datos y la ruta a los datos cuyo archivo o carpeta de información de la política de auditoría que desea mostrar.

Paso

1. Mostrar configuración de política de auditoría: `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

Ejemplo

El siguiente comando muestra la información de la directiva de auditoría aplicada a la ruta "'/corp" en SVM vs1. La ruta de acceso tiene aplicada UNA entrada SACL DE ÉXITO y DE FALLO:

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

                Vserver: vs1
              File Path: /corp
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Obtenga información sobre cómo administrar los trabajos de políticas de seguridad de ONTAP SMB

Si existe un trabajo de política de seguridad, en determinadas circunstancias, no puede modificar dicha política de seguridad ni las tareas asignadas a dicha política. Debe entender en qué condiciones puede o no puede modificar las directivas de seguridad para que cualquier intento que realice para modificar la directiva se realice correctamente. Las modificaciones de la directiva incluyen agregar, eliminar o modificar tareas asignadas a la directiva y eliminar o modificar la directiva.

No puede modificar una política de seguridad ni una tarea asignada a esa política si existe un trabajo para esa política y ese trabajo está en los estados siguientes:

- El trabajo está en ejecución o en curso.
- El trabajo está en pausa.
- El trabajo se reanuda y se encuentra en estado en ejecución.
- Si el trabajo está esperando a conmutar al respaldo a otro nodo.

En las siguientes circunstancias, si existe un trabajo para una política de seguridad, puede modificar correctamente dicha política de seguridad o una tarea asignada a dicha directiva:

- El trabajo de política se ha detenido.
- El trabajo de directiva ha finalizado correctamente.

Comandos ONTAP para administrar descriptores de seguridad NTFS en servidores SMB

Existen comandos ONTAP específicos para administrar descriptores de seguridad. Puede crear, modificar, eliminar y mostrar información acerca de los descriptores de seguridad.

Si desea…	Se usa este comando…
Crear descriptores de seguridad NTFS	`vserver security file-directory ntfs create`
Modifique los descriptores de seguridad NTFS existentes	`vserver security file-directory ntfs modify`
Mostrar información acerca de los descriptores de seguridad NTFS existentes	`vserver security file-directory ntfs show`
Eliminar descriptores de seguridad NTFS	`vserver security file-directory ntfs delete`

Obtenga más información sobre `vserver security file-directory ntfs` en el "Referencia de comandos del ONTAP".

Comandos ONTAP para administrar entradas de control de acceso DACL NTFS en servidores SMB

Hay comandos ONTAP específicos para administrar entradas de control de acceso DACL (ACE). Puede agregar ACE a DACL NTFS en cualquier momento. También puede administrar las DACL de NTFS existentes modificando, eliminando y mostrando información acerca de las ACE en las DACL.

Si desea…	Se usa este comando…
Cree ACE y agréguelos a DACL NTFS	`vserver security file-directory ntfs dacl add`
Modifique los ACE existentes en las DACL NTFS	`vserver security file-directory ntfs dacl modify`
Mostrar información acerca de los ACE existentes en las DACL NTFS	`vserver security file-directory ntfs dacl show`
Elimine los ACE existentes de las DACL NTFS	`vserver security file-directory ntfs dacl remove`

Obtenga más información sobre `vserver security file-directory ntfs dacl` en el "Referencia de comandos del ONTAP".

Comandos ONTAP para administrar entradas de control de acceso SACL NTFS en servidores SMB

Hay comandos ONTAP específicos para administrar entradas de control de acceso SACL (ACE). Puede agregar ACE a SACL NTFS en cualquier momento. También puede administrar SACL NTFS existentes modificando, eliminando y mostrando información acerca de ACE en SACL.

Si desea…	Se usa este comando…
Cree ACE y agréguelos a SACL NTFS	`vserver security file-directory ntfs sacl add`
Modifique los ACE existentes en SACL NTFS	`vserver security file-directory ntfs sacl modify`
Muestra información acerca de los ACE existentes en SACL NTFS	`vserver security file-directory ntfs sacl show`
Elimine los ACE existentes de SACL NTFS	`vserver security file-directory ntfs sacl remove`

Obtenga más información sobre `vserver security file-directory ntfs sacl` en el "Referencia de comandos del ONTAP".

Comandos de ONTAP para administrar políticas de seguridad SMB

Existen comandos ONTAP específicos para administrar las políticas de seguridad. Puede mostrar información acerca de las políticas y eliminarla. No puede modificar una política de seguridad.

Si desea…	Se usa este comando…
Cree políticas de seguridad	`vserver security file-directory policy create`
Mostrar información acerca de las directivas de seguridad	`vserver security file-directory policy show`
Eliminar políticas de seguridad	`vserver security file-directory policy delete`

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

Comandos ONTAP para administrar tareas de políticas de seguridad SMB

Hay comandos de ONTAP para añadir, modificar, quitar y mostrar información acerca de tareas de políticas de seguridad.

Si desea…	Se usa este comando…
Agregar tareas de directiva de seguridad	`vserver security file-directory policy task add`
Modifique las tareas de las políticas de seguridad	`vserver security file-directory policy task modify`
Muestra información acerca de las tareas de directiva de seguridad	`vserver security file-directory policy task show`
Quitar tareas de directiva de seguridad	`vserver security file-directory policy task remove`

Obtenga más información sobre `vserver security file-directory policy task` en el "Referencia de comandos del ONTAP".

Comandos de ONTAP para administrar trabajos de políticas de seguridad de SMB

Hay comandos de la ONTAP para pausar, reanudar, detener y mostrar información acerca de los trabajos de políticas de seguridad.

Si desea…	Se usa este comando…
Pausar trabajos de directiva de seguridad	`vserver security file-directory job pause -vserver vserver_name -id integer`
Reanudar trabajos de directiva de seguridad	`vserver security file-directory job resume -vserver vserver_name -id integer`
Mostrar información sobre trabajos de directivas de seguridad	`vserver security file-directory job show -vserver vserver_name` Puede determinar el ID de trabajo de un trabajo mediante este comando.
Detener trabajos de directiva de seguridad	`vserver security file-directory job stop -vserver vserver_name -id integer`

Obtenga más información sobre `vserver security file-directory job` en el "Referencia de comandos del ONTAP".

Configure la caché de metadatos para los recursos compartidos de SMB

Obtenga más información sobre el almacenamiento en caché de metadatos SMB de ONTAP

El almacenamiento en caché de metadatos permite almacenar en caché atributos de archivos en clientes SMB 1.0 para proporcionar un acceso más rápido a los atributos de archivos y carpetas. Puede habilitar o deshabilitar el almacenamiento en caché de atributos por recurso compartido. También puede configurar el tiempo de espera para las entradas en caché si está activado el almacenamiento en caché de metadatos. No es necesario configurar el almacenamiento en caché de metadatos si los clientes se conectan a recursos compartidos mediante SMB 2.x o SMB 3.0.

Cuando se habilita esta opción, la caché de metadatos del SMB almacena los datos de atributos de archivos y rutas por una cantidad limitada de tiempo. Esto puede mejorar el rendimiento de SMB para los clientes de SMB 1.0 con cargas de trabajo comunes.

En determinadas tareas, SMB crea una cantidad significativa de tráfico que puede incluir varias consultas idénticas para los metadatos de archivos y rutas. Puede reducir el número de consultas redundantes y mejorar el rendimiento de clientes de SMB 1.0 utilizando el almacenamiento en caché de metadatos del SMB para recuperar información de la caché.

> Si bien es poco probable, es posible que la caché de metadatos proporcione información obsoleta a clientes SMB 1.0. Si su entorno no se puede permitir este riesgo, no debe habilitar esta función.

Habilitar la caché de metadatos SMB de ONTAP

Puede mejorar el rendimiento de SMB para los clientes de SMB 1.0 al habilitar la caché de metadatos de SMB. De manera predeterminada, el almacenamiento en caché de metadatos de SMB está deshabilitado.

Paso

1. Realice la acción deseada:

Si desea…	Introduzca el comando…
Habilite el almacenamiento en caché de metadatos de SMB cuando crea un recurso compartido	`vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties attributecache`
Habilite el almacenamiento en caché de metadatos de SMB en un recurso compartido existente	`vserver cifs share properties add -vserver` *`vserver_name`* `-share-name` *`share_name`* `-share-properties attributecache`

Información relacionada

- Configurar la duración de las entradas de caché de metadatos

- Agregar o eliminar propiedades de recursos compartidos en recursos compartidos existentes

Configurar la duración de las entradas de caché de metadatos SMB de ONTAP

Puede configurar la vida útil de las entradas de la caché de metadatos SMB para optimizar el rendimiento de la caché de metadatos de SMB en su entorno. El valor predeterminado es 10 segundos.

Antes de empezar

Debe haber habilitado la función de caché de metadatos SMB. Si el almacenamiento en caché de metadatos de SMB no está habilitado, no se utiliza la configuración TTL de la caché de SMB.

Paso

1. Realice la acción deseada:

Si desea configurar la vida útil de las entradas de la caché de metadatos SMB al…	Introduzca el comando…
Crear un recurso compartido	`vserver cifs share -create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-attribute-cache-ttl [integerh][integerm][integers]`
Modifique un recurso compartido existente	`vserver cifs share -modify -vserver` *`vserver_name`* `-share-name` *`share_name`* `-attribute-cache-ttl [integerh][integerm][integers]`

Puede especificar propiedades y opciones de configuración de recursos compartidos adicionales al crear o modificar recursos compartidos. Obtenga más información sobre `vserver cifs share` en el "Referencia de comandos del ONTAP".

Administrar bloqueos de archivos

Obtenga información sobre el bloqueo de archivos SMB de ONTAP 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, las operaciones de manipulación de archivos `rm` como , , `rmdir` y `mv`

pueden provocar el fallo de la aplicación NFS.

- Las operaciones de lectura y escritura de NFS se deniegan en los modos abiertos Deny-Read y Deny-write de SMB, respectivamente.
- Error en las operaciones de escritura de NFS cuando el rango escrito del archivo está bloqueado por un bytelock exclusivo de SMB.
- Desenlazar
  - En el caso de los sistemas de archivos NTFS, se admiten las operaciones de eliminación de SMB y CIFS.

    El archivo se eliminará después del último cierre.
  - No se admiten las operaciones de desenlace de NFS.

    No es compatible porque la semántica NTFS y SMB es necesaria, y la última operación Delete-on-Close no es compatible con NFS.
  - Para los sistemas de archivos UNIX, se admite la operación de desvinculación.

    Es compatible porque se necesitan semántica NFS y UNIX.
- Cambiar el nombre
  - Para los sistemas de archivos NTFS, si el archivo de destino se abre desde SMB o CIFS, se puede cambiar el nombre del archivo de destino.
  - No se admite el cambio de nombre de NFS.

    No es compatible porque se requieren semánticas NTFS y SMB.

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

Obtenga información sobre los bits de solo lectura de ONTAP SMB

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

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

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

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

- NFS trata cualquier archivo con el bit de solo lectura habilitado como si no tiene bits de permiso de escritura habilitados.
- Si un cliente NFS deshabilita todos los bits de permiso de escritura y al menos uno de esos bits se había

habilitado anteriormente, ONTAP habilita el bit de solo lectura para ese archivo.

- Si un cliente NFS habilita algún bit de permiso de escritura, ONTAP deshabilita el bit de solo lectura para ese archivo.
- Si se habilita el bit de solo lectura de un archivo y un cliente NFS intenta detectar permisos para el archivo, los bits de permiso del archivo no se envían al cliente NFS; en su lugar, ONTAP envía los bits de permiso al cliente NFS con los bits de permiso de escritura enmascarados.
- Si se habilita el bit de solo lectura de un archivo y un cliente SMB deshabilita el bit de solo lectura, ONTAP habilita el bit de permiso de escritura del propietario para el archivo.
- Los archivos con el bit de sólo lectura activado sólo son grabables por raíz.

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

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

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

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

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

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

Diferencias entre ONTAP y Windows en el manejo de bloqueos en 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 configuraciones de seguridad que impidan que los usuarios o aplicaciones cambien el nombre de los directorios críticos.

Mostrar información sobre los bloqueos SMB de ONTAP

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

Acerca de esta tarea

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

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

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

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

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

Paso

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

Ejemplos

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

```
cluster1::> vserver locks show

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

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

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

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

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

```
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Romper los bloqueos SMB de ONTAP

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

Acerca de esta tarea

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

Pasos

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

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

2. Establezca el nivel de privilegio en avanzado: `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`

Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

Supervise la actividad del SMB

Mostrar información de la sesión SMB de ONTAP

Puede mostrar información acerca de las sesiones SMB establecidas, incluidos la conexión SMB y el ID de sesión y la dirección IP de la estación de trabajo mediante la sesión. Es posible mostrar información sobre la versión del protocolo SMB de la sesión y el nivel de protección disponible continuamente, lo que ayuda a identificar si la sesión admite operaciones no disruptivas.

Acerca de esta tarea

Puede mostrar información de todas las sesiones de la SVM en formato de resumen. Sin embargo, en muchos casos, la cantidad de producción que se devuelve es grande. Puede personalizar la información que se muestra en el resultado especificando parámetros opcionales:

- Puede utilizar el parámetro opcional `-fields` para mostrar resultados sobre los campos seleccionados.

  Puede introducir `-fields ?` para determinar qué campos puede utilizar.

- Puede usar el `-instance` parámetro para mostrar información detallada acerca de las sesiones SMB establecidas.
- Puede usar `-fields` el parámetro o el `-instance` parámetro solo o en combinación con otros parámetros opcionales.

Paso

1. Ejecute una de las siguientes acciones:

Si desea mostrar información de la sesión SMB…	Introduzca el siguiente comando…
Para todas las sesiones del SVM en formato de resumen	`vserver cifs session show -vserver vserver_name`
En un ID de conexión especificado	`vserver cifs session show -vserver vserver_name -connection-id integer`
Desde una dirección IP de estación de trabajo especificada	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
En una dirección IP de LIF especificada	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
En un nodo especificado	`vserver cifs session show -vserver vserver_name -node {node_name`
local}`	Desde un usuario de Windows especificado

Si desea mostrar información de la sesión SMB…	Introduzca el siguiente comando…
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	Con un mecanismo de autenticación especificado
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1	NTLMv2
Kerberos	Anonymous}`
Con una versión de protocolo especificada	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1
SMB2	SMB2_1
SMB3	SMB3_1}`  [NOTE] ==== Protección de disponibilidad continua y multicanal de SMB solo están disponibles en sesiones SMB 3.0 y posteriores. Para ver su estado en todas las sesiones de calificación, debe especificar este parámetro con el valor definido en `SMB3` o posterior. ====
Con un nivel especificado de protección continua disponible	`vserver cifs session show -vserver vserver_name -continuously-available {No
Yes	Partial}`  [NOTE] ==== Si el estado de disponibilidad continua es `Partial`, significa que la sesión contiene al menos un archivo abierto continuamente disponible, pero la sesión tiene algunos archivos que no están abiertos con protección disponible continuamente. Puede usar el `vserver cifs sessions file show` comando para determinar qué archivos de la sesión establecida no están abiertos con la protección disponible continuamente. ====
Con un estado de sesión de firma SMB especificado	`vserver cifs session show -vserver vserver_name -is-session-signed {true

Ejemplos

El siguiente comando muestra información de sesión para las sesiones en SVM vs1 establecidas desde una estación de trabajo con dirección IP 10.1.1.1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2         23s
```

El siguiente comando muestra información detallada de la sesión para las sesiones con protección continuamente disponible en SVM vs1. La conexión se realizó mediante la cuenta de dominio.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                      Node: node1
                   Vserver: vs1
                Session ID: 1
              Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
             Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: Yes
          Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

El siguiente comando muestra información de sesión en una sesión mediante SMB 3.0 y SMB MultiChannel en SVM vs1. En el ejemplo, el usuario se conectó a este recurso compartido desde un cliente con capacidad para SMB 3.0 mediante la dirección IP de LIF; por lo tanto, el mecanismo de autenticación se estableció de forma predeterminada en NTLMv2. La conexión se debe realizar mediante la autenticación Kerberos para conectarse con la protección disponible continuamente.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Información relacionada

Mostrar información acerca de los archivos SMB abiertos

Mostrar información sobre archivos SMB de ONTAP abiertos

Es posible ver información sobre los archivos SMB abiertos, incluidos la conexión de SMB y el ID de sesión, el volumen de host, el nombre del recurso compartido y la ruta del recurso compartido. Es posible mostrar información acerca del nivel de protección disponible continuamente de un archivo, lo cual es útil para determinar si un archivo abierto está en un estado que admite operaciones no disruptivas.

Acerca de esta tarea

Puede ver información sobre los archivos abiertos en una sesión de SMB establecida. La información que se muestra es útil cuando necesita determinar la información de la sesión SMB para determinados archivos dentro de una sesión SMB.

Por ejemplo, si tiene una sesión SMB en la que algunos de los archivos abiertos están abiertos con protección disponible continuamente y otros no están abiertos con protección disponible continuamente (el valor `-continuously-available` del campo en `vserver cifs session show` la salida del comando es `Partial`), puede determinar qué archivos no están disponibles continuamente mediante este comando.

Puede mostrar información de todos los archivos abiertos en sesiones SMB establecidas en máquinas virtuales de almacenamiento (SVM) de forma resumida, mediante `vserver cifs session file show` el

comando sin ningún parámetro opcional.

Sin embargo, en muchos casos, la cantidad de producción devuelta es grande. Puede personalizar la información que se muestra en el resultado especificando parámetros opcionales. Esto puede resultar útil si desea ver información sólo de un pequeño subconjunto de archivos abiertos.

- Puede utilizar el parámetro opcional `-fields` para mostrar la salida en los campos seleccionados.

  Es posible usar este parámetro de forma independiente o combinada con otros parámetros opcionales.

- Puede utilizar el `-instance` parámetro para mostrar información detallada sobre los archivos SMB abiertos.

  Es posible usar este parámetro de forma independiente o combinada con otros parámetros opcionales.

Paso

1. Ejecute una de las siguientes acciones:

Si desea mostrar archivos SMB abiertos…	Introduzca el siguiente comando…
En la SVM de forma resumida	`vserver cifs session file show -vserver vserver_name`
En un nodo especificado	`vserver cifs session file show -vserver vserver_name -node {node_name`
local}`	En un ID de archivo especificado
`vserver cifs session file show -vserver vserver_name -file-id integer`	En un ID de conexión de SMB especificado
`vserver cifs session file show -vserver vserver_name -connection-id integer`	En un ID de sesión de SMB especificado
`vserver cifs session file show -vserver vserver_name -session-id integer`	En el agregado de host especificado
`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`	En el volumen especificado
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	En el recurso compartido de SMB especificado

Si desea mostrar archivos SMB abiertos…	Introduzca el siguiente comando…
`vserver cifs session file show -vserver vserver_name -share share_name`	En la ruta del bloque de mensajes del servidor especificada
`vserver cifs session file show -vserver vserver_name -path path`	Con el nivel especificado de protección continua disponible
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}`  [NOTE] ==== Si el estado de disponibilidad continua es `No`, esto significa que estos archivos abiertos no pueden recuperarse sin interrupciones de la toma de control y la devolución. Tampoco pueden recuperarse de la reubicación general de agregados entre partners en una relación de alta disponibilidad. ====
Con el estado reconectado especificado	`vserver cifs session file show -vserver vserver_name -reconnected {No

Existen parámetros opcionales adicionales que se pueden utilizar para refinar los resultados de la salida. Obtenga más información sobre `vserver cifs session file show` en el "Referencia de comandos del ONTAP".

Ejemplos

En el siguiente ejemplo, se muestra información sobre los archivos abiertos en la SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

En el siguiente ejemplo, se muestra información detallada sobre los archivos SMB abiertos con el ID de archivo 82 en la SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
             CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

Información relacionada

Mostrar información de la sesión

Determinar qué estadísticas, objetos y contadores están disponibles en los servidores SMB de ONTAP

Para poder obtener información acerca de las estadísticas de CIFS, SMB, auditoría y BranchCache hash, y supervisar el rendimiento, debe conocer los objetos y contadores disponibles desde los cuales puede obtener datos.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

Si desea determinar…	Introduzca…
Qué objetos están disponibles	`statistics catalog object show`
Objetos específicos disponibles	`statistics catalog object show -object object_name`
Qué contadores están disponibles	`statistics catalog counter show -object object_name`

Obtenga más información sobre `statistics catalog object show`, incluidos los objetos y contadores disponibles, en la "Referencia de comandos del ONTAP"sección .

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

Ejemplos

El siguiente comando muestra descripciones de los objetos de estadísticas seleccionados relacionados con CIFS y acceso SMB en el clúster tal y como se ve en el nivel de privilegio avanzado:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

El siguiente comando muestra información acerca de algunos de los contadores del `cifs` objeto como se ve

en el nivel de privilegio avanzado:

> En este ejemplo no se muestran todos los contadores disponibles para `cifs` el objeto; la salida se trunca.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
--------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                                vserver_1:10.72.205.179
    instance_uuid                                       2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

Información relacionada

- Mostrar estadísticas
- "Catálogo de estadísticas Contador Mostrar objeto"

- "Las estadísticas comienzan"

Mostrar estadísticas de ONTAP SMB

Puede mostrar varias estadísticas, incluidas estadísticas sobre CIFS y SMB, auditoría y hash de BranchCache, para supervisar el rendimiento y diagnosticar problemas.

Antes de empezar

Debe haber recogido muestras de datos mediante los `statistics start` `statistics stop` comandos y antes de poder mostrar información sobre los objetos.

Obtenga más información sobre `statistics start` y `statistics stop` en el "Referencia de comandos del ONTAP" .

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

Si desea mostrar estadísticas de…	Introduzca…
Todas las versiones de SMB	`statistics show -object cifs`
SMB 1,0	`statistics show -object smb1`
SMB 2.x y SMB 3.0	`statistics show -object smb2`
Subsistema CIFS del nodo	`statistics show -object nblade_cifs`
Auditoría multiprotocolo	`statistics show -object audit_ng`
Servicio hash de BranchCache	`statistics show -object hashd`
DNS dinámico	`statistics show -object ddns_update`

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

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

Información relacionada

- Determinar qué estadísticas, objetos y contadores están disponibles en los servidores
- Supervisar estadísticas de sesión firmada por SMB
- Muestra las estadísticas de BranchCache
- Utilice estadísticas para supervisar la actividad de referencia automática de nodos
- "Configuración de SMB para Microsoft Hyper-V y SQL Server"
- "Configuración de supervisión del rendimiento"

Ponga en marcha servicios basados en cliente de SMB

Utilice archivos sin conexión para permitir el almacenamiento en caché de archivos para su uso sin conexión

Obtenga información sobre el uso de archivos sin conexión para permitir el almacenamiento en caché de archivos SMB de ONTAP para su uso sin conexión

ONTAP es compatible con la característica Archivos sin conexión de Microsoft, o con la función de almacenamiento en caché del cliente_, que permite almacenar los archivos en caché en el host local para su uso sin conexión. Los usuarios pueden utilizar la funcionalidad de archivos sin conexión para seguir trabajando en archivos incluso cuando están desconectados de la red.

Puede especificar si los documentos y programas de usuario de Windows se almacenan automáticamente en caché en un recurso compartido o si los archivos deben seleccionarse manualmente para almacenar en caché. El almacenamiento en caché manual está habilitado de forma predeterminada para nuevos recursos compartidos. Los archivos que están disponibles sin conexión se sincronizan con el disco local del cliente de Windows. La sincronización se produce cuando se restaura la conectividad de red a un recurso compartido de sistema de almacenamiento específico.

Puesto que los archivos y carpetas sin conexión conservan los mismos permisos de acceso que la versión de los archivos y carpetas guardados en el servidor CIFS, el usuario debe tener suficientes permisos en los archivos y carpetas guardados en el servidor CIFS para realizar acciones en los archivos y carpetas sin conexión.

Cuando el usuario y otra persona de la red realizan cambios en el mismo archivo, el usuario puede guardar la versión local del archivo en la red, conservar la otra versión o guardar ambas. Si el usuario conserva ambas versiones, se guarda localmente un nuevo archivo con los cambios del usuario local y el archivo almacenado en caché se sobrescribe con cambios de la versión del archivo guardado en el servidor CIFS.

Puede configurar archivos sin conexión de forma compartida mediante las opciones de configuración de recursos compartidos. Puede elegir una de las cuatro configuraciones de carpetas sin conexión al crear o modificar recursos compartidos:

- Sin almacenamiento en caché

  Deshabilita el almacenamiento en caché en el cliente para el recurso compartido. Los archivos y carpetas no se almacenan automáticamente en caché local en clientes y los usuarios no pueden optar por almacenar en caché archivos o carpetas localmente.

- Almacenamiento en caché manual

  Permite la selección manual de archivos para almacenar en caché en el recurso compartido. Esta es la configuración predeterminada. De forma predeterminada, no se almacenan en caché archivos ni carpetas en el cliente local. Los usuarios pueden elegir los archivos y carpetas que desean almacenar en caché localmente para utilizarlos sin conexión.

- Almacenamiento automático de documentos en caché

  Permite que los documentos de usuario se almacenen automáticamente en caché en el recurso compartido. Sólo los archivos y carpetas a los que se tiene acceso se almacenan en caché localmente.

- Almacenamiento automático de programas en caché

  Permite que los programas y los documentos de usuario se almacenen automáticamente en caché en el recurso compartido. Sólo los archivos, carpetas y programas a los que se tiene acceso se almacenan en caché localmente. Además, esta configuración permite al cliente ejecutar ejecutables almacenados localmente en caché incluso cuando se conecta a la red.

Para obtener más información acerca de la configuración de archivos sin conexión en servidores y clientes de Windows, consulte la biblioteca de Microsoft TechNet.

Información relacionada

- Uso de perfiles de itinerancia para almacenar perfiles de usuario de forma centralizada en un servidor CIFS asociado con la SVM
- Aprenda a utilizar la redirección de carpetas para almacenar datos en servidores
- Obtenga información sobre cómo usar BranchCache para almacenar en caché contenido compartido en una sucursal
- "Biblioteca de Microsoft TechNet: technet.microsoft.com/en-us/library/"

Conozca los requisitos para usar archivos SMB de ONTAP sin conexión

Antes de poder utilizar la función Microsoft Offline Files con el servidor CIFS, debe conocer las versiones de ONTAP y SMB y los clientes Windows que admiten la función.

Requisitos de versión de ONTAP

Las versiones ONTAP admiten archivos sin conexión.

Requisitos de la versión del protocolo SMB

Para las máquinas virtuales de almacenamiento (SVM), ONTAP admite archivos sin conexión en todas las versiones de SMB.

Requisitos del cliente Windows

El cliente Windows debe admitir los archivos sin conexión.

Para obtener la información más reciente sobre los clientes de Windows que admiten la función Archivos sin conexión, consulte la matriz de interoperabilidad.

"mysupport.netapp.com/matrix"

Pautas para implementar archivos SMB de ONTAP sin conexión

Hay algunas directrices importantes que debe comprender al implementar archivos sin conexión en recursos compartidos del directorio principal que tienen la `showsnapshot` propiedad de recurso compartido establecida en los directorios principales.

Si la `showsnapshot` propiedad Compartir se establece en un recurso compartido de directorio principal que tiene configurados archivos sin conexión, los clientes de Windows almacenan en caché todas las instantáneas de `~snapshot` la carpeta en el directorio raíz del usuario.

Los clientes de Windows almacenan en caché todas las snapshots en el directorio inicial si se cumple alguna

de las siguientes opciones:

- El usuario hace que el directorio inicial esté disponible sin conexión desde el cliente.

  El contenido de `~snapshot` la carpeta en el directorio principal se incluye y se pone a disposición fuera de línea.

- El usuario configura el redireccionamiento de carpetas para redirigir una carpeta, como `My Documents` la raíz de un directorio inicial que reside en el recurso compartido del servidor CIFS.

  Es posible que algunos clientes de Windows hagan que la carpeta redirigida esté disponible sin conexión automáticamente. Si la carpeta se redirige a la raíz del directorio principal, la `~snapshot` carpeta se incluye en el contenido sin conexión almacenado en caché.

> `~snapshot`Se deben evitar los despliegues de archivos fuera de línea en los que la carpeta se incluya en archivos fuera de línea. Las instantáneas de `~snapshot` la carpeta contienen todos los datos del volumen en el momento en el que ONTAP creó la instantánea. Por lo tanto, la creación de una copia sin conexión de la `~snapshot` carpeta consume un almacenamiento local importante en el cliente, consume ancho de banda de red durante la sincronización de archivos sin conexión y aumenta el tiempo que se tarda en sincronizar los archivos sin conexión.

Comandos ONTAP para configurar la compatibilidad con archivos SMB sin conexión

Puede configurar la compatibilidad de archivos sin conexión mediante la interfaz de línea de comandos de ONTAP especificando una de las cuatro archivos sin conexión al crear recursos compartidos de SMB o en cualquier momento modificando los recursos compartidos de SMB existentes. La compatibilidad con archivos manuales sin conexión es la configuración predeterminada.

Acerca de esta tarea

Al configurar el soporte de archivos sin conexión, puede elegir una de las siguientes cuatro opciones de archivos sin conexión:

Ajuste	Descripción
`none`	Despermite a los clientes de Windows almacenar en caché cualquier archivo en este recurso compartido.
`manual`	Permite a los usuarios de clientes de Windows seleccionar manualmente los archivos que se van a almacenar en caché.

Ajuste	Descripción
`documents`	Permite a los clientes de Windows almacenar en caché los documentos de usuario utilizados por el usuario para el acceso sin conexión.
`programs`	Permite a los clientes de Windows almacenar en caché programas que utilizan el usuario para el acceso sin conexión. Los clientes pueden utilizar los archivos de programa almacenados en caché en modo sin conexión incluso si el recurso compartido está disponible.

Sólo puede seleccionar una configuración de archivo sin conexión. Si modifica una configuración de archivos sin conexión en un recurso compartido SMB existente, la opción nuevos archivos sin conexión reemplaza la configuración original. Las demás opciones de configuración y propiedades de uso compartido de SMB existentes no se eliminan ni se reemplazan. Permanecen vigentes hasta que se eliminan o cambian explícitamente.

Pasos

1. Ejecute la acción adecuada:

Si desea configurar archivos sin conexión en…	Introduzca el comando…
Un nuevo recurso compartido de SMB	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none
manual	documents
programs}`	Un recurso compartido de SMB existente
`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none	manual
documents	programs}`

2. Compruebe que la configuración del recurso compartido de SMB sea correcta: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Ejemplo

El siguiente comando crea un recurso compartido SMB denominado «ata1» con los archivos fuera de línea establecidos en `documents`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                Share Properties: oplocks
                                  browsable
                                  changenotify
              Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: Offline files
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: documents
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

El siguiente comando modifica un recurso compartido SMB existente llamado “ata1” cambiando la configuración de archivos fuera de línea a `manual` y agregando valores para la máscara de creación de modo de archivo y directorio:

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
          CIFS Server NetBIOS Name: VS1
                             Path: /data1
                  Share Properties: oplocks
                                    browsable
                                    changenotify
                Symlink Properties: enable
           File Mode Creation Mask: 644
      Directory Mode Creation Mask: 777
                    Share Comment: Offline files
                        Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                      Volume Name: -
                    Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Información relacionada

Agregar o eliminar propiedades de recursos compartidos en recursos compartidos existentes

Configurar la compatibilidad de archivos sin conexión en los recursos compartidos SMB de ONTAP mediante la MMC de administración del equipo

Si desea permitir a los usuarios almacenar en caché archivos localmente para su uso sin conexión, puede configurar la compatibilidad con archivos sin conexión mediante la MMC de Administración de equipos (Microsoft Management Console).

Pasos

1. Para abrir el MMC en el servidor de Windows, en el Explorador de Windows, haga clic con el botón secundario del mouse (ratón) en el icono del equipo local y, a continuación, seleccione **Administrar**.
2. En el panel izquierdo, seleccione **Administración de equipos**.
3. Seleccione **Acción** > **conectar a otro ordenador**.

   Aparece el cuadro de diálogo Seleccionar equipo.

4. Escriba el nombre del servidor CIFS o haga clic en **examinar** para buscar el servidor CIFS.

   Si el nombre del servidor CIFS es el mismo que el nombre de host de máquina virtual de almacenamiento (SVM), escriba el nombre de SVM. Si el nombre del servidor CIFS es diferente del nombre de host de la

SVM, escriba el nombre del servidor CIFS.

5. Haga clic en **OK**.
6. En el árbol de la consola, haga clic en **Herramientas del sistema** > **carpetas compartidas**.
7. Haga clic en **comparticiones**.
8. En el panel de resultados, haga clic con el botón derecho en el recurso compartido.
9. Haga clic en **Propiedades**.

   Se mostrarán las propiedades del recurso compartido seleccionado.

10. En la ficha **General**, haga clic en **Configuración sin conexión**.

    Se muestra el cuadro de diálogo Configuración sin conexión.

11. Configure las opciones de disponibilidad sin conexión según corresponda.
12. Haga clic en **OK**.

Use perfiles de itinerancia para almacenar perfiles de usuario de forma centralizada en un servidor SMB asociado con la SVM

Obtenga información sobre el uso de perfiles móviles para almacenar perfiles de usuarios de ONTAP SMB de forma centralizada

ONTAP admite el almacenamiento de perfiles de itinerancia de Windows en un servidor CIFS asociado con la máquina virtual de almacenamiento (SVM). La configuración de perfiles de itinerancia de usuario ofrece ventajas al usuario, como la disponibilidad automática de recursos, independientemente de dónde se conecte el usuario. Los perfiles de itinerancia también simplifican la administración y gestión de los perfiles de usuario.

Los perfiles de usuario móviles tienen las siguientes ventajas:

- Disponibilidad de recursos automática

  El perfil único de un usuario está automáticamente disponible cuando ese usuario inicia sesión en cualquier equipo de la red que ejecuta Windows 8, Windows 7, Windows 2000 o Windows XP. Los usuarios no necesitan crear un perfil en cada equipo que utilizan en una red.

- Sustitución simplificada del ordenador

  Dado que toda la información del perfil del usuario se mantiene por separado en la red, el perfil de un usuario se puede descargar fácilmente en un equipo nuevo y de repuesto. Cuando el usuario inicia sesión en el nuevo equipo por primera vez, la copia del servidor del perfil del usuario se copia en el nuevo equipo.

Información relacionada

- Obtenga información sobre el uso de archivos sin conexión para permitir el almacenamiento en caché de archivos para su uso sin conexión
- Aprenda a utilizar la redirección de carpetas para almacenar datos en servidores

Conozca los requisitos para usar perfiles SMB de roaming de ONTAP

Antes de poder utilizar los perfiles de itinerancia de Microsoft en su servidor CIFS, necesita saber qué versiones de ONTAP y SMB y qué clientes de Windows admiten esta función.

Requisitos de versión de ONTAP

ONTAP admite perfiles de itinerancia.

Requisitos de la versión del protocolo SMB

En el caso de máquinas virtuales de almacenamiento (SVM), ONTAP admite perfiles de itinerancia en todas las versiones de SMB.

Requisitos del cliente Windows

Para que un usuario pueda utilizar los perfiles de itinerancia, el cliente de Windows debe admitir la función.

Para obtener la información más reciente acerca de los clientes de Windows que admiten perfiles de itinerancia, consulte matriz de interoperabilidad.

"Herramienta de matriz de interoperabilidad de NetApp"

Configurar perfiles SMB de ONTAP móviles a través de la MMC Usuarios y equipos de Active Directory

Si desea que el perfil de un usuario esté disponible automáticamente cuando este inicie sesión en cualquier equipo de la red, puede configurar perfiles de itinerancia a través del complemento MMC Usuarios y equipos de Active Directory. Si está configurando perfiles de itinerancia en Windows Server, puede utilizar el Centro de administración de Active Directory.

Pasos

1. En el servidor Windows, abra el MMC de Usuarios y equipos de Active Directory (o el Centro de administración de Active Directory en servidores Windows).
2. Busque el usuario para el que desea configurar un perfil de itinerancia.
3. Haga clic con el botón derecho del ratón en el usuario y haga clic en **Propiedades**.
4. En la pestaña **Perfil**, ingresa la ruta de perfil al recurso compartido donde deseas almacenar el perfil de roaming del usuario, seguido de `%username%`.

   Por ejemplo, una ruta de acceso de perfil puede ser la siguiente `\\vs1.example.com\profiles\%username%`: . La primera vez que un usuario inicia sesión, `%username%` se sustituye por el nombre del usuario.

   > En la ruta `\\vs1.example.com\profiles\%username%`, `profiles` es el nombre compartido de un recurso compartido en una máquina virtual de almacenamiento (SVM) VS1 que tiene derechos de control total para todos.

5. Haga clic en **OK**.

Utilice la redirección de carpetas para almacenar datos en un servidor SMB

Aprenda a usar la redirección de carpetas para almacenar datos en servidores SMB de ONTAP

ONTAP admite la redirección de carpetas de Microsoft, lo que permite que los usuarios o administradores redirijan la ruta de una carpeta local a una ubicación en el servidor CIFS. Parece que si las carpetas redirigidas se almacenan en el cliente local de Windows, aunque los datos se almacenen en un recurso compartido de SMB.

La redirección de carpetas está destinada principalmente a las empresas que ya han implementado directorios iniciales y que desean mantener la compatibilidad con su entorno de directorio raíz existente.

- `Documents`, , `Desktop` y `Start Menu` son ejemplos de carpetas que puede redirigir.
- Los usuarios pueden redirigir carpetas desde su cliente Windows.
- Los administradores pueden configurar y administrar centralmente la redirección de carpetas configurando GPO en Active Directory.
- Si los administradores han configurado perfiles de itinerancia, la redirección de carpetas permite a los administradores dividir los datos de usuario de los datos de perfil.
- Los administradores pueden usar la redirección de carpetas y los archivos sin conexión juntos para redirigir el almacenamiento de datos de carpetas locales al servidor CIFS, permitiendo a los usuarios almacenar el contenido en la memoria caché localmente.

Información relacionada

- Obtenga información sobre el uso de archivos sin conexión para permitir el almacenamiento en caché de archivos para su uso sin conexión
- Uso de perfiles de itinerancia para almacenar perfiles de usuario de forma centralizada en un servidor CIFS asociado con la SVM

Conozca los requisitos para usar la redirección de carpetas SMB de ONTAP

Para poder utilizar la redirección de carpetas de Microsoft con el servidor CIFS, debe conocer las versiones de ONTAP y SMB y los clientes de Windows que admiten la función.

Requisitos de versión de ONTAP

ONTAP admite redirección de carpetas de Microsoft.

Requisitos de la versión del protocolo SMB

Para la máquina virtual de almacenamiento (SVM), ONTAP admite el redireccionamiento de carpetas de Microsoft en todas las versiones de SMB.

Requisitos del cliente Windows

Para que un usuario pueda utilizar la redirección de carpetas de Microsoft, el cliente de Windows debe admitir la función.

Para obtener la información más reciente acerca de los clientes de Windows que admiten la redirección de carpetas, consulte la matriz de interoperabilidad.

"mysupport.netapp.com/matrix"

Configurar la redirección de carpetas SMB de ONTAP mediante las Propiedades de Windows

Puede configurar la redirección de carpetas mediante la ventana Propiedades de Windows. La ventaja de utilizar este método es que el usuario de Windows puede configurar la redirección de carpetas sin la ayuda del administrador de SVM.

Pasos

1. En el Explorador de Windows, haga clic con el botón secundario en la carpeta que desea redirigir a un recurso compartido de red.
2. Haga clic en **Propiedades**.

   Se mostrarán las propiedades del recurso compartido seleccionado.

3. En la ficha **acceso directo**, haga clic en **destino** y especifique la ruta de acceso a la ubicación de red en la que desea redirigir la carpeta seleccionada.

   Por ejemplo, si desea redirigir una carpeta a la `data` carpeta en un directorio principal asignado a `Q:\`, especifique `Q:\data` como destino.

4. Haga clic en **OK**.

   Para obtener más información acerca de la configuración de carpetas sin conexión, consulte la Biblioteca de Microsoft TechNet.

Información relacionada

"Biblioteca de Microsoft TechNet: technet.microsoft.com/en-us/library/"

Obtenga información sobre cómo acceder al directorio ~snapshot de ONTAP desde clientes Windows mediante SMB 2.x

El método que utiliza para acceder al `~snapshot` directorio desde clientes de Windows con SMB 2.x es diferente del método utilizado para SMB 1,0. Es necesario entender cómo acceder al `~snapshot` directorio cuando se utilizan conexiones SMB 2.x para acceder correctamente a los datos almacenados en instantáneas.

El administrador de SVM controla si los usuarios de clientes de Windows pueden ver `~snapshot` el directorio en un recurso compartido y acceder a él; para ello, habilita o deshabilita la `showsnapshot` propiedad de recurso compartido mediante comandos de las familias de propiedades de recurso compartido cifs de Vserver.

Cuando `showsnapshot` se deshabilita la propiedad Compartir, un usuario de un cliente Windows que utiliza SMB 2.x no puede ver `~snapshot` el directorio y no puede acceder a las instantáneas dentro del `~snapshot` directorio, incluso cuando se introduce manualmente la ruta de acceso al `~snapshot` directorio o a instantáneas específicas dentro del directorio.

Cuando `showsnapshot` se habilita la propiedad de recurso compartido, un usuario en un cliente de Windows que utiliza SMB 2.x aún no puede ver `~snapshot` el directorio en la raíz del recurso compartido ni dentro de ninguna unión o directorio debajo de la raíz del recurso compartido. Sin embargo, después de conectarse a un recurso compartido, el usuario puede acceder al `~snapshot` directorio oculto anexando manualmente `\~snapshot` al final de la ruta de acceso al recurso compartido. `~snapshot`Se puede acceder al directorio

oculto desde dos puntos de entrada:

- En la raíz del recurso compartido
- En cada punto de unión del espacio compartido

> `~snapshot`No se puede acceder al directorio oculto desde subdirectorios que no son de unión dentro del recurso compartido.

Ejemplo

Con la configuración que se muestra en el siguiente ejemplo, un usuario en un cliente Windows con una conexión SMB 2.x al recurso compartido «`eng`» puede acceder al `~snapshot` directorio agregando manualmente `\~snapshot` a la ruta de acceso de recurso compartido en la raíz del recurso compartido y en cada punto de unión de la ruta. `~snapshot`Se puede acceder al directorio oculto desde las tres rutas siguientes:

- `\\vs1\eng\~snapshot`
- `\\vs1\eng\projects1\~snapshot`
- `\\vs1\eng\projects2\~snapshot`

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume       junction-path
------- ------------ ----------------------------------------
vs1     vs1_root      /
vs1     vs1_vol1      /eng
vs1     vs1_vol2      /eng/projects1
vs1     vs1_vol3      /eng/projects2

cluster1::> vserver cifs share show
Vserver  Share   Path     Properties    Comment  ACL
-------- ------  -------  ----------    -------- ----------
vs1      eng     /eng     oplocks       -        Everyone / Full Control
                          changenotify
                          browsable
                          showsnapshot
```

Recupere archivos y carpetas con versiones anteriores

Obtenga información sobre cómo recuperar archivos y carpetas SMB de ONTAP usando versiones anteriores

La posibilidad de utilizar versiones anteriores de Microsoft es aplicable a sistemas de archivos que admitan instantáneas de algún tipo y las tienen habilitadas. La tecnología Snapshot forma parte de ONTAP. Los usuarios pueden recuperar archivos y carpetas de snapshots desde su cliente de Windows usando la función de versiones anteriores de

Microsoft.

La funcionalidad de versiones anteriores ofrece un método para que los usuarios naveguen por las instantáneas o restauren datos desde una snapshot sin intervención de un administrador de almacenamiento. Las versiones anteriores no se pueden configurar. Está siempre habilitada. Si el administrador de almacenamiento ha puesto instantáneas disponibles en un recurso compartido, el usuario puede utilizar versiones anteriores para realizar las siguientes tareas:

- Recuperar archivos eliminados accidentalmente.
- Recuperación de la sobrescritura accidental de un archivo.
- Compare las versiones del archivo mientras está trabajando.

Los datos almacenados en snapshots son de solo lectura. Los usuarios deben guardar una copia de un archivo en otra ubicación para realizar cualquier cambio en el archivo. Las instantáneas se eliminan periódicamente; por lo tanto, los usuarios necesitan crear copias de los archivos contenidos en versiones anteriores si desean conservar indefinidamente una versión anterior de un archivo.

Requisitos de ONTAP SMB para usar versiones anteriores de Microsoft

Antes de poder utilizar las versiones anteriores con el servidor CIFS, debe conocer qué versiones de ONTAP y SMB, y qué clientes de Windows, admiten. También debe conocer el requisito de configuración de la snapshot.

Requisitos de versión de ONTAP

Admite versiones anteriores.

Requisitos de la versión del protocolo SMB

Para las máquinas virtuales de almacenamiento (SVM), ONTAP admite las versiones anteriores de todas las versiones de SMB.

Requisitos del cliente Windows

Para que un usuario pueda utilizar versiones anteriores para acceder a los datos en instantáneas, el cliente Windows debe admitir la función.

Para obtener la información más reciente sobre los clientes de Windows compatibles con versiones anteriores, consulte matriz de interoperabilidad.

"Herramienta de matriz de interoperabilidad de NetApp"

Requisitos para la configuración de Snapshot

Para usar versiones anteriores para acceder a los datos de las snapshots, se debe asociar una política Snapshot habilitada al volumen que contiene los datos, los clientes deben poder acceder a los datos de las snapshots y deben existir snapshots.

Vea y administre datos de instantáneas de ONTAP SMB con la pestaña Versiones anteriores de Windows

Los usuarios de máquinas cliente Windows pueden usar la pestaña Versiones anteriores de la ventana Propiedades de Windows para restaurar los datos almacenados en

snapshots sin necesidad de involucrar al administrador de máquinas virtuales de almacenamiento (SVM).

Acerca de esta tarea

Solo puede utilizar la pestaña Versiones anteriores para ver y gestionar datos en instantáneas de datos almacenados en la SVM si el administrador ha habilitado snapshots en el volumen que contiene el recurso compartido y si el administrador configura el recurso compartido para mostrar las snapshots.

Pasos

1. En el Explorador de Windows, muestre el contenido de la unidad asignada de los datos almacenados en el servidor CIFS.
2. Haga clic con el botón derecho en el archivo o carpeta de la unidad de red asignada cuyas instantáneas desea ver o gestionar.
3. Haga clic en **Propiedades**.

   Se muestran las propiedades del archivo o carpeta seleccionado.

4. Haga clic en la ficha **versiones anteriores**.

   En el cuadro Versiones de carpeta se muestra una lista de instantáneas disponibles del archivo o carpeta seleccionado. Las copias de Snapshot enumeradas se identifican con el prefijo del nombre de la snapshot y la fecha/hora de creación.

5. En el cuadro **versiones de carpeta:**, haga clic con el botón secundario del mouse (ratón) en la copia del archivo o carpeta que desee administrar.
6. Ejecute la acción adecuada:

Si desea…	Haga lo siguiente…
Ver datos de esa instantánea	Haga clic en **Abrir**.
Cree una copia de datos a partir de esa instantánea	Haga clic en **Copiar**.

   Los datos de las copias Snapshot son de solo lectura. Si desea realizar modificaciones en los archivos y carpetas enumerados en la ficha versiones anteriores, debe guardar una copia de los archivos y carpetas que desea modificar en una ubicación editable y realizar modificaciones en las copias.

7. Cuando termine de administrar los datos de las instantáneas, cierre el cuadro de diálogo **Propiedades** haciendo clic en **Aceptar**.

   Para obtener más información sobre el uso de la pestaña Versiones anteriores para ver y administrar datos de instantáneas, consulte la biblioteca de Microsoft TechNet.

Información relacionada

"Biblioteca de Microsoft TechNet: technet.microsoft.com/en-us/library/"

Determinar si las instantáneas SMB de ONTAP están disponibles para el uso de versiones anteriores

Las snapshots se pueden ver en la pestaña Versiones anteriores solo si se aplica una política de Snapshot habilitada al volumen que contiene el recurso compartido y si la

configuración del volumen permite el acceso a las instantáneas. Determinar la disponibilidad de instantáneas es útil cuando se ayuda a un usuario con acceso a versiones anteriores.

Pasos

1. Determine si el volumen en el que residen los datos compartidos tiene snapshots automáticas habilitadas y si los clientes tienen acceso a los directorios de snapshots: `volume show -vserver vserver-name -volume volume-name -fields vserver,volume,snapdir-access,snapshot-policy,snapshot-count`

   La salida muestra qué política de instantáneas está asociada con el volumen, si el acceso al directorio de instantáneas del cliente está habilitado y el número de instantáneas disponibles.

2. Determinar si la política de snapshots asociada está habilitada: `volume snapshot policy show -policy policy-name`
3. Enumere las instantáneas disponibles: `volume snapshot show -volume volume_name`

   Para obtener más información sobre la configuración y gestión de políticas de snapshot y programaciones de snapshot, consulte "Protección de datos".

Ejemplo

El siguiente ejemplo muestra información sobre las políticas de instantáneas asociadas con el volumen denominado «ata1» que contiene los datos compartidos y las instantáneas disponibles en «ata1».

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-------- ------ -------------- --------------- --------------
vs1      data1  true           default         10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1
                   Number of Is
Policy Name        Schedules Enabled Comment
------------------ --------- ------- ---------------------------------
default                   3 true    Default policy with hourly, daily &
weekly schedules.
    Schedule         Count     Prefix                  SnapMirror Label
    ---------------- -----     ----------------------- -------------------
    hourly               6     hourly                  -
    daily                2     daily                   daily
    weekly               2     weekly                  weekly

cluster1::> volume snapshot show -volume data1
                                                                 ---Blocks---
Vserver  Volume  Snapshot                  State        Size Total% Used%
-------- ------- ------------------------- -------- -------- ------ -----
vs1      data1
                 weekly.2012-12-16_0015    valid       408KB     0%    1%
                 daily.2012-12-22_0010     valid       420KB     0%    1%
                 daily.2012-12-23_0010     valid       192KB     0%    0%
                 weekly.2012-12-23_0015    valid       360KB     0%    1%
                 hourly.2012-12-23_1405    valid       196KB     0%    0%
                 hourly.2012-12-23_1505    valid       196KB     0%    0%
                 hourly.2012-12-23_1605    valid       212KB     0%    0%
                 hourly.2012-12-23_1705    valid       136KB     0%    0%
                 hourly.2012-12-23_1805    valid       200KB     0%    0%
                 hourly.2012-12-23_1905    valid       184KB     0%    0%
```

Información relacionada

- Crear configuraciones de instantáneas para habilitar el acceso a versiones anteriores
- "Protección de datos"

Cree configuraciones de instantáneas de ONTAP SMB para habilitar el acceso a versiones anteriores

La funcionalidad de las versiones anteriores está siempre disponible, siempre que el acceso del cliente a las instantáneas esté activado y siempre que existan instantáneas. Si la configuración de Snapshot no cumple estos requisitos, puede crear una configuración de Snapshot que sí lo cumpla.

Pasos

1. Si el volumen que contiene el recurso compartido al que desea permitir el acceso a las versiones anteriores no tiene una política Snapshot asociada, asocie una política de Snapshot al volumen y habilite dicha política con el `volume modify` comando.

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

2. Permita el acceso a las instantáneas mediante `volume modify` el comando para establecer `-snap-dir` la opción en `true`.

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

3. Comprobar que las políticas de Snapshot están habilitadas y que el acceso a los directorios de snapshots está habilitado mediante `volume show` los comandos y. `volume snapshot policy show`

   Obtenga más información sobre `volume show` y `volume snapshot policy show` en el "Referencia de comandos del ONTAP".

   Para obtener más información sobre la configuración y gestión de políticas de snapshot y programaciones de snapshot, consulte "Protección de datos".

Información relacionada

"Protección de datos"

Obtenga información sobre cómo restaurar directorios de versiones anteriores que contienen uniones SMB de ONTAP

Hay ciertas directrices que debe tener en cuenta al utilizar versiones anteriores para restaurar carpetas que contienen puntos de unión.

Al utilizar versiones anteriores para restaurar carpetas que tienen carpetas secundarias que son puntos de unión, la restauración puede fallar y `Access Denied` generar un error.

Puede determinar si la carpeta que intenta restaurar contiene una unión mediante `vol show` el uso del comando con `-parent` la opción. También puede usar `vserver security trace` los comandos para crear registros detallados sobre problemas de acceso a archivos y carpetas.

Información relacionada

Crear y gestionar volúmenes de datos en espacios de nombres NAS

Ponga en marcha servicios basados en servidor de SMB

Administrar directorios iniciales

Obtenga información sobre cómo habilitar directorios de inicio dinámicos en servidores SMB de ONTAP

Los directorios iniciales de ONTAP permiten configurar un recurso compartido de SMB que se asigna a directorios diferentes en función del usuario que se conecta a él y a un conjunto de variables. En lugar de crear recursos compartidos independientes para cada usuario, puede configurar un recurso compartido con algunos parámetros del directorio

inicial para definir la relación de un usuario entre un punto de entrada (el recurso compartido) y el directorio inicial (un directorio en la SVM).

Un usuario que ha iniciado sesión como usuario invitado no tiene un directorio principal y no puede acceder a los directorios iniciales de otros usuarios. Existen cuatro variables que determinan cómo se asigna un usuario a un directorio:

- **Nombre del recurso compartido**

  Éste es el nombre del recurso compartido que se crea al que se conecta el usuario. Debe establecer la propiedad del directorio principal para este recurso compartido.

  El nombre del recurso compartido puede utilizar los siguientes nombres dinámicos:

  - `%w` (Nombre de usuario de Windows del usuario)
  - `%d` (Nombre de dominio de Windows del usuario)
  - `%u` (Nombre de usuario UNIX asignado al usuario) Para que el nombre del recurso compartido sea único en todos los directorios raíz, el nombre del recurso compartido debe contener/`%w` `%u` la variable o. El nombre del recurso compartido puede contener tanto la `%d`/`%w` variable como la variable (por ejemplo, `%d`/`%w`), o el nombre del recurso compartido puede contener una parte estática y una parte variable (por ejemplo, home_/`%w`).

- **Compartir ruta**

  Esta es la ruta relativa, que define el recurso compartido y, por lo tanto, está asociada con uno de los nombres de recurso compartido, que se anexa a cada ruta de búsqueda para generar toda la ruta de directorio inicial del usuario desde la raíz de la SVM. Puede ser estático (por ejemplo `home`,), dinámico (por ejemplo, `%w`) o una combinación de ambos (por ejemplo, `eng/%w`).

- **Rutas de búsqueda**

  Este es el conjunto de rutas absolutas desde la raíz de la SVM que especifique que dirige la búsqueda ONTAP de directorios iniciales. Puede especificar una o más rutas de búsqueda mediante `vserver cifs home-directory search-path add` el comando. Si especifica varias rutas de búsqueda, ONTAP las intenta en el orden especificado hasta que encuentre una ruta válida. Obtenga más información sobre `vserver cifs home-directory search-path add` en el "Referencia de comandos del ONTAP".

- **Directorio**

  Éste es el directorio principal del usuario que se crea para el usuario. El nombre del directorio suele ser el nombre del usuario. Debe crear el directorio principal en uno de los directorios definidos por las rutas de búsqueda.

Por ejemplo, considere la siguiente configuración:

- Usuario: John Smith
- Dominio de usuario: acme
- Nombre de usuario: Jsmith
- Nombre de SVM: vs1
- Nombre compartido del directorio inicial #1: Home_ `%w` - Ruta de acceso compartida: `%w`

- Nombre compartido del directorio inicial #2: `%w` - Ruta de acceso compartida: `%d/%w`
- Ruta de búsqueda #1: `/vol0home/home`
- Ruta de búsqueda #2: `/vol1home/home`
- Ruta de búsqueda #3: `/vol2home/home`
- Directorio inicial: `/vol1home/home/jsmith`

Escenario 1: El usuario se conecta a `\\vs1\home_jsmith`. Esto coincide con el primer nombre compartido del directorio raíz y genera la ruta de acceso relativa `jsmith` . ONTAP ahora busca un directorio llamado `jsmith` comprobando cada ruta de búsqueda en orden:

- `/vol0home/home/jsmith` no existe; pasando a la ruta de búsqueda #2.
- `/vol1home/home/jsmith` existe; por lo tanto, la ruta de búsqueda #3 no está seleccionada; el usuario está ahora conectado a su directorio principal.

Escenario 2: El usuario se conecta a `\\vs1\jsmith`. Esto coincide con el segundo nombre compartido del directorio raíz y genera la ruta de acceso relativa `acme/jsmith` . ONTAP ahora busca un directorio llamado `acme/jsmith` comprobando cada ruta de búsqueda en orden:

- `/vol0home/home/acme/jsmith` no existe; pasando a la ruta de búsqueda #2.
- `/vol1home/home/acme/jsmith` no existe; pasando a la ruta de búsqueda #3.
- `/vol2home/home/acme/jsmith` no existe; el directorio principal no existe; por lo tanto, la conexión falla.

Recursos compartidos de directorios iniciales

Agregar recursos compartidos del directorio de inicio SMB de ONTAP

Si desea utilizar la característica de directorio inicial SMB, debe agregar al menos un recurso compartido con la propiedad de directorio principal incluida en las propiedades de recurso compartido.

Acerca de esta tarea

Puede crear un recurso compartido de directorio inicial en el momento de crear el recurso compartido mediante `vserver cifs share create` el comando, o bien puede cambiar un recurso compartido existente en un recurso compartido de directorio inicial en cualquier momento con `vserver cifs share modify` el comando.

Para crear un recurso compartido de directorio inicial, debe incluir `homedirectory` el valor en `-share -properties` la opción al crear o modificar un recurso compartido. Puede especificar el nombre de recurso compartido y la ruta de acceso compartida mediante variables que se amplían dinámicamente cuando los usuarios se conectan a sus directorios iniciales. Las variables disponibles que puede utilizar en la ruta de acceso son `%w`, `%d`, y `%u`, correspondientes al nombre de usuario de Windows, dominio y nombre de usuario UNIX asignado, respectivamente.

Pasos

1. Añadir un recurso compartido de directorio principal:
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties homedirectory[,…]`

`-vserver vserver` Especifica la máquina virtual de almacenamiento (SVM) habilitada para CIFS en la que se añadirá la ruta de búsqueda.

`-share-name` *share-name* especifica el nombre del recurso compartido del directorio principal.

Además de contener una de las variables necesarias, si el nombre del recurso compartido contiene una de las cadenas literales `%w` , , `%u` o `%d`, debe preceder la cadena literal con un carácter % (porcentaje) para evitar que ONTAP trate la cadena literal como una variable (por ejemplo, `%%w`).

- El nombre del recurso compartido debe contener la `%w` `%u` variable o.
- El nombre del recurso compartido puede contener además la `%d` variable (por ejemplo, `%d/%w`) o una parte estática en el nombre del recurso compartido (por ejemplo, home1_/`%w`).
- Si los administradores utilizan el recurso compartido para conectarse a los directorios principales de otros usuarios o para permitir que los usuarios se conecten a los directorios principales de otros usuarios, el patrón de nombre de recurso compartido dinámico debe ir precedido de una tilde (~).

  El `vserver cifs home-directory modify` se utiliza para activar este acceso estableciendo `-is -home-dirs-access-for-admin-enabled` la opción en `true`) o estableciendo la opción avanzada `-is-home-dirs-access-for-public-enabled` en `true`.

`-path path` especifica la ruta relativa al directorio raíz.

`-share-properties homedirectory[,…]` especifica las propiedades de recurso compartido para ese recurso compartido. Debe especificar `homedirectory` el valor. Puede especificar propiedades de recursos compartidos adicionales mediante una lista delimitada por comas.

1. Compruebe que ha agregado correctamente el recurso compartido del directorio inicial mediante `vserver cifs share show` el comando.

Ejemplo

El siguiente comando crea un recurso compartido de directorio raíz denominado `%w`. Las `oplocks browsable changenotify` propiedades , y share se establecen además de definir la `homedirectory` propiedad share.

> Este ejemplo no muestra el resultado de todos los recursos compartidos de la SVM. La salida está truncada.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory

vs1::> vserver cifs share show -vserver vs1
Vserver    Share    Path         Properties     Comment  ACL
---------- -------- ------------ -------------- -------- -----------
vs1        %w       %w           oplocks        -        Everyone / Full
Control
                                 browsable
                                 changenotify
                                 homedirectory
```

Información relacionada

- Agregar rutas de búsqueda del directorio de inicio
- Requisitos y pautas para el uso de referencias automáticas de nodos en servidores
- Administrar la accesibilidad a los directorios personales de los usuarios

Obtenga información sobre los requisitos únicos de nombre de usuario SMB de ONTAP para recursos compartidos del directorio de inicio

Tenga cuidado de asignar nombres de usuario únicos al crear recursos compartidos de directorios principales mediante las `%w %u` variables (nombre de usuario de Windows) o (nombre de usuario de UNIX) para generar recursos compartidos de forma dinámica. El nombre del recurso compartido está asignado al nombre de usuario.

Pueden ocurrir dos problemas cuando el nombre de un recurso compartido estático y el nombre de un usuario son iguales:

- Cuando el usuario enumera los recursos compartidos en un clúster con `net view` el comando, se muestran dos recursos compartidos con el mismo nombre de usuario.
- Cuando el usuario se conecta a ese nombre de recurso compartido, el usuario siempre está conectado al recurso compartido estático y no puede acceder al recurso compartido del directorio principal con el mismo nombre.

Por ejemplo, hay un recurso compartido denominado «'Administrator'» y usted tiene un nombre de usuario «'Administrator'» de Windows. Si crea un recurso compartido de directorio principal y se conecta a dicho recurso compartido, se conecta a la unidad estática "'Administrator'", no a su directorio principal "'Administrator'".

Puede resolver el problema con nombres de recursos compartidos duplicados siguiendo cualquiera de estos pasos:

- Cambiar el nombre del recurso compartido estático para que deje de estar en conflicto con el recurso compartido del directorio principal del usuario.
- Dar al usuario un nuevo nombre de usuario para que no entre en conflicto con el nombre de recurso compartido estático.
- Crear un recurso compartido de directorio raíz CIFS con un nombre estático como «`home`» en lugar de utilizar el `%w` parámetro para evitar conflictos con los nombres del recurso compartido.

Obtenga información sobre qué sucede con los nombres de recursos compartidos del directorio de inicio SMB de ONTAP estático después de la actualización

Los nombres compartidos del directorio inicial deben contener `%w %u` la variable dinámica o la variable dinámica. Debe saber qué ocurre con los nombres de recursos compartidos de directorios iniciales estáticos existentes después de actualizar a una versión de ONTAP con el nuevo requisito.

Si la configuración del directorio raíz contiene nombres de recursos compartidos estáticos y se actualiza a ONTAP, los nombres de recursos compartidos de directorio raíz estáticos no se modifican y siguen siendo válidos. Sin embargo, no puede crear ningún recurso compartido nuevo del directorio inicial que no contenga `%w %u` la variable o.

Al requerir que se incluya una de estas variables en el nombre del recurso compartido del directorio principal

del usuario se garantiza que cada nombre de recurso compartido sea único en la configuración del directorio principal. Si lo desea, puede cambiar los nombres compartidos del directorio principal estático por nombres que contengan la `%w` `%u` variable o.

Agregar rutas de búsqueda del directorio de inicio de ONTAP SMB

Si desea utilizar directorios iniciales SMB de ONTAP, debe agregar al menos una ruta de búsqueda de directorio raíz.

Acerca de esta tarea

Puede agregar una ruta de búsqueda del directorio inicial utilizando `vserver cifs home-directory search-path add` el comando.

El `vserver cifs home-directory search-path add` comando comprueba la ruta especificada en la `-path` opción durante la ejecución del comando. Si la ruta especificada no existe, el comando genera un mensaje solicitando si desea continuar. Usted elige `y` o `n`. Si decide `y` continuar, ONTAP creará la ruta de búsqueda. Sin embargo, debe crear la estructura de directorios para poder utilizar la ruta de búsqueda en la configuración del directorio principal. Si elige no continuar, el comando falla; no se crea la ruta de búsqueda. A continuación, puede crear la estructura de directorios PATH y volver a ejecutar `vserver cifs home-directory search-path add` el comando.

Pasos

1. Agregar una ruta de búsqueda del directorio inicial: `vserver cifs home-directory search-path add -vserver vserver -path path`
2. Compruebe que ha agregado correctamente la ruta de búsqueda mediante el `vserver cifs home-directory search-path show` comando.

Ejemplo

En el siguiente ejemplo, se agrega la ruta `/home1` a la configuración del directorio inicial en la SVM VS1.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

vs1::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

En el siguiente ejemplo, se intenta añadir la ruta `/home2` a la configuración del directorio inicial en la SVM VS1. La ruta no existe. Se decide no continuar.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home2
Warning: The specified path "/home2" does not exist in the namespace
         belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

Información relacionada

Agregar recursos compartidos del directorio de inicio

Cree configuraciones de directorio de inicio SMB de ONTAP utilizando las variables %w y %d

Puede crear una configuración del directorio inicial mediante `%w` `%d` las variables y. Los usuarios pueden conectarse a su propio recurso compartido mediante recursos compartidos creados dinámicamente.

Pasos

1. Cree un qtree que contenga los directorios iniciales de usuario: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Compruebe que el qtree esté utilizando el estilo de seguridad correcto: `volume qtree show`
3. Si el qtree no está usando el estilo de seguridad deseado, cambie el estilo de seguridad con el `volume qtree security` comando.
4. Añadir un recurso compartido de directorio inicial: `vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory\[,...\]`

   `-vserver vserver` Especifica la máquina virtual de almacenamiento (SVM) habilitada para CIFS en la que se añadirá la ruta de búsqueda.

   `-share-name %w` especifica el nombre del recurso compartido del directorio principal. ONTAP crea dinámicamente el nombre del recurso compartido a medida que cada usuario se conecta a su directorio inicial. El nombre del recurso compartido tendrá el formato *Windows_USER_NAME*.

   `-path %d/%w` especifica la ruta relativa al directorio raíz. La ruta relativa se crea dinámicamente a medida que cada usuario se conecta a su directorio principal y tendrá el formato *domain/Windows_user_name*.

   `-share-properties homedirectory[,…]+` especifica las propiedades de recurso compartido para ese recurso compartido. Debe especificar `homedirectory` el valor. Puede especificar propiedades de recursos compartidos adicionales mediante una lista delimitada por comas.

5. Compruebe que el recurso compartido tiene la configuración deseada con `vserver cifs share show` el comando.
6. Agregar una ruta de búsqueda del directorio inicial: `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver` *`vserver-name`* Especifica la SVM habilitada para CIFS en la que se añadirá la ruta de búsqueda.

   `-path` *`path`* especifica la ruta de acceso absoluta del directorio a la ruta de búsqueda.

7. Compruebe que ha agregado correctamente la ruta de búsqueda mediante el `vserver cifs home-directory search-path show` comando.
8. Para los usuarios que dispongan de un directorio inicial, cree un directorio correspondiente en el qtree o en el volumen designado para que contengan directorios iniciales.

   Por ejemplo, si creó un qtree con la ruta de `/vol/vol1/users` y el nombre de usuario cuyo directorio desea crear es mydomain\user1, debe crear un directorio con la ruta de acceso siguiente `/vol/vol1/users/mydomain/user1:` .

Si creaste un volumen llamado “home1” montado en `/home1`, crearías un directorio con la siguiente ruta: `/home1/mydomain/user1`.

9. Compruebe que un usuario puede conectarse correctamente al recurso compartido principal mediante la asignación de una unidad o la conexión mediante la ruta UNC.

   Por ejemplo, si el usuario mydomain\user1 desea conectarse al directorio creado en el Paso 8 que se encuentra en la SVM VS1, user1 se conectaría mediante la ruta UNC `\\vs1\user1` .

Ejemplo

Los comandos del siguiente ejemplo crean una configuración de directorio inicial con los siguientes ajustes:

- El nombre del recurso compartido es %w.
- La ruta de acceso relativa al directorio principal es %d/%w.
- La ruta de búsqueda que se utiliza para contener los directorios raíz `/home1` , es un volumen configurado con estilo de seguridad NTFS.
- La configuración se crea en SVM vs1.

Puede utilizar este tipo de configuración de directorio inicial cuando los usuarios acceden a sus directorios iniciales desde hosts de Windows. También puede utilizar este tipo de configuración cuando los usuarios acceden a sus directorios iniciales desde hosts Windows y UNIX y el administrador del sistema de archivos utiliza usuarios y grupos basados en Windows para controlar el acceso al sistema de archivos.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %w

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %d/%w
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

Información relacionada

- Configure directorios iniciales utilizando la variable %u
- Obtenga más información sobre configuraciones adicionales del directorio de inicio
- Mostrar información sobre las rutas del directorio de inicio del usuario

Configurar los directorios de inicio de ONTAP SMB utilizando la variable %u

Puede crear una configuración de directorio inicial donde se designe el nombre del recurso compartido mediante la `%w` variable, pero se utiliza la `%u` variable para designar la ruta relativa al recurso compartido del directorio inicial. A continuación, los usuarios pueden conectarse a su recurso compartido doméstico mediante recursos compartidos dinámicamente creados con su nombre de usuario de Windows sin tener en cuenta el nombre real o la ruta de acceso del directorio principal.

Pasos

1. Cree un qtree que contenga los directorios iniciales de usuario: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Compruebe que el qtree esté utilizando el estilo de seguridad correcto: `volume qtree show`
3. Si el qtree no está usando el estilo de seguridad deseado, cambie el estilo de seguridad con el `volume qtree security` comando.
4. Añadir un recurso compartido de directorio inicial: `vserver cifs share create -vserver vserver -share-name %w -path %u -share-properties homedirectory ,...]`

   `-vserver vserver` Especifica la máquina virtual de almacenamiento (SVM) habilitada para CIFS en la que se añadirá la ruta de búsqueda.

   `-share-name %w` especifica el nombre del recurso compartido del directorio principal. El nombre del recurso compartido se crea dinámicamente a medida que cada usuario se conecta a su directorio principal y tiene el formato *Windows_USER_NAME*.

   > También puede utilizar `%u` la variable para `-share-name` la opción. Esto crea una ruta de acceso de recursos compartidos relativa que utiliza el nombre de usuario UNIX asignado.

   `-path %u` especifica la ruta relativa al directorio raíz. La ruta relativa se crea dinámicamente a medida que cada usuario se conecta a su directorio principal y tiene el formato *corated_UNIX_user_name*.

   > El valor de esta opción también puede contener elementos estáticos. Por ejemplo, `eng/%u`.

   `-share-properties homedirectory\[,...\]` especifica las propiedades de recurso compartido para ese recurso compartido. Debe especificar `homedirectory` el valor. Puede especificar propiedades de recursos compartidos adicionales mediante una lista delimitada por comas.

5. Compruebe que el recurso compartido tiene la configuración deseada con `vserver cifs share show` el comando.
6. Agregar una ruta de búsqueda del directorio inicial: `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver vserver` Especifica la SVM habilitada para CIFS en la que se añadirá la ruta de búsqueda.

   `-path path` especifica la ruta de acceso absoluta del directorio a la ruta de búsqueda.

7. Compruebe que ha agregado correctamente la ruta de búsqueda mediante el `vserver cifs home-directory search-path show` comando.
8. Si el usuario UNIX no existe, cree el usuario UNIX con el `vserver services unix-user create` comando.

   > Debe existir el nombre de usuario UNIX al que se asigna el nombre de usuario de Windows antes de asignar el usuario.

9. Cree una asignación de nombres para el usuario Windows al usuario UNIX con el siguiente comando: `vserver name-mapping create -vserver vserver_name -direction win-unix -priority integer -pattern windows_user_name -replacement unix_user_name`

Si ya existen asignaciones de nombres que asignan usuarios de Windows a usuarios UNIX, no es necesario realizar el paso de asignación.

El nombre de usuario de Windows está asignado al nombre de usuario UNIX correspondiente. Cuando el usuario de Windows se conecta a su recurso compartido de directorio principal, se conectan a un directorio raíz creado dinámicamente con un nombre de recurso compartido que corresponde a su nombre de usuario de Windows sin tener en cuenta que el nombre de directorio corresponde al nombre de usuario UNIX.

10. Para los usuarios que dispongan de un directorio inicial, cree un directorio correspondiente en el qtree o en el volumen designado para que contengan directorios iniciales.

    Por ejemplo, si creaste un qtree con la ruta de acceso de `/vol/vol1/users` y el nombre de usuario UNIX asignado del usuario cuyo directorio quieres crear es 'unixuser1', crearías un directorio con la siguiente ruta de acceso `/vol/vol1/users/unixuser1`: .

    Si creaste un volumen llamado "home1" montado en `/home1`, crearías un directorio con la siguiente ruta: `/home1/unixuser1`.

11. Compruebe que un usuario puede conectarse correctamente al recurso compartido principal mediante la asignación de una unidad o la conexión mediante la ruta UNC.

    Por ejemplo, si el usuario mydomain\user1 se asigna al usuario UNIX unixuser1 y desea conectarse al directorio creado en el Paso 10 que se encuentra en SVM VS1, user1 se conectaría mediante la ruta UNC `\\vs1\user1` .

Ejemplo

Los comandos del siguiente ejemplo crean una configuración de directorio inicial con los siguientes ajustes:

- El nombre del recurso compartido es %w.
- La ruta de acceso relativa al directorio principal es %u.
- La ruta de búsqueda que se utiliza para contener los directorios raíz `/home1` , es un volumen configurado con estilo de seguridad UNIX.
- La configuración se crea en SVM vs1.

Puede utilizar este tipo de configuración de directorio inicial cuando los usuarios acceden a sus directorios iniciales desde hosts Windows o hosts Windows y UNIX y el administrador del sistema de archivos utiliza usuarios y grupos basados en UNIX para controlar el acceso al sistema de archivos.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %u

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %u
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show -vserver vs1
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1

cluster::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1

cluster::> vserver name-mapping show -pattern user1
Vserver        Direction Position
-------------- --------- --------
vs1            win-unix  5        Pattern: user1
                               Replacement: unixuser1
```

Información relacionada

- Cree configuraciones de directorio de inicio utilizando las variables %w y %d
- Obtenga más información sobre configuraciones adicionales del directorio de inicio
- Mostrar información sobre las rutas del directorio de inicio del usuario

Obtenga más información sobre configuraciones adicionales del directorio de inicio SMB de ONTAP

Puede crear configuraciones de directorio raíz adicionales mediante las `%w` `%d` `%u` variables , y, lo que permite personalizar la configuración del directorio raíz para satisfacer sus necesidades.

Puede crear una serie de configuraciones de directorios iniciales mediante una combinación de variables y cadenas estáticas en los nombres de recursos compartidos y las rutas de búsqueda. En la siguiente tabla se muestran algunos ejemplos que ilustran cómo crear distintas configuraciones de directorio principal:

Rutas creadas cuando `/vol1/user` contiene directorios iniciales…	**Compartir comando…**
Para crear una ruta de acceso compartida `\\vs1\~win_username` que dirija al usuario a. `/vol1/user/win_username`	`vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory`
Para crear una ruta de acceso compartida `\\vs1\win_username` que dirija al usuario a. `/vol1/user/domain/win_username`	`vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory`
Para crear una ruta de acceso compartida `\\vs1\win_username` que dirija al usuario a. `/vol1/user/unix_username`	`vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory`
Para crear una ruta de acceso compartida `\\vs1\unix_username` que dirija al usuario a. `/vol1/user/unix_username`	`vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory`

Comandos ONTAP para administrar rutas de búsqueda SMB

Hay comandos ONTAP específicos para gestionar las rutas de búsqueda de las configuraciones de directorios iniciales de SMB. Por ejemplo, hay comandos para agregar, quitar y mostrar información acerca de las rutas de búsqueda. También hay un comando para cambiar el orden de la ruta de búsqueda.

Si desea…	**Se usa este comando…**
Agregue una ruta de búsqueda	`vserver cifs home-directory search-path add`
Mostrar rutas de búsqueda	`vserver cifs home-directory search-path show`

Si desea…	Se usa este comando…
Cambie el orden de la ruta de búsqueda	`vserver cifs home-directory search-path reorder`
Quitar una ruta de búsqueda	`vserver cifs home-directory search-path remove`

Obtenga más información sobre `vserver cifs home-directory search-path` en el "Referencia de comandos del ONTAP".

Mostrar información sobre las rutas del directorio de inicio del usuario SMB de ONTAP

Puede mostrar la ruta de directorio inicial de un usuario SMB en la máquina virtual de almacenamiento (SVM), que puede utilizarse si tiene varias rutas de directorio raíz CIFS configuradas y desea ver qué ruta contiene el directorio raíz del usuario.

Paso

1. Visualice la ruta del directorio inicial con `vserver cifs home-directory show-user` el comando.

```
vserver cifs home-directory show-user -vserver vs1 -username user1
```

```
Vserver      User                 Home Dir Path
-----------  -------------------  ----------------------
vs1          user1                /home/user1
```

Información relacionada

Administrar la accesibilidad a los directorios personales de los usuarios

Administrar la accesibilidad a los directorios de inicio de los usuarios de ONTAP SMB

De forma predeterminada, sólo el usuario puede acceder al directorio principal de un usuario. Para los recursos compartidos donde el nombre dinámico del recurso compartido va precedido de una tilde (~), los administradores de Windows o cualquier otro usuario (acceso público) pueden habilitar o deshabilitar el acceso a los directorios principales de los usuarios.

Antes de empezar

Los recursos compartidos de directorio inicial en la máquina virtual de almacenamiento (SVM) deben configurarse con nombres de recursos compartidos dinámicos que van precedidos por una tilde (~). En los siguientes casos se ilustran los requisitos de nomenclatura de los recursos compartidos:

Nombre del recurso compartido del directorio inicial	Ejemplo de comando para conectarse al recurso compartido
~%d~%w	`net use * \\IPaddress\~domain~user/u:credentials`
~%w	`net use * \\IPaddress\~user/u:credentials`
~abc~%w	`net use * \\IPaddress\abc~user/u:credentials`

Paso

1. Ejecute la acción adecuada:

Si desea activar o desactivar el acceso a los directorios de inicio de los usuarios a…	Introduzca lo siguiente…
Administradores de Windows	`vserver cifs home-directory modify -vserver` *`vserver_name`* `-is-home-dirs -access-for-admin-enabled {true|false}` El valor predeterminado es `true`.
Cualquier usuario (acceso público)	a. Establezca el nivel de privilegio en AVANZADO: `set -privilege advanced` b. Activar o desactivar el acceso: `vserver cifs home-directory modify -vserver` *vserver_name* -is-home-dirs-access-for-public-enabled {true

El siguiente ejemplo habilita el acceso público a los directorios principales de los usuarios:

```
set -privilege advanced +
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public
-enabled true set -privilege admin
```

Información relacionada

Mostrar información sobre las rutas del directorio de inicio del usuario

Configure el acceso del cliente SMB a los enlaces simbólicos de UNIX

Obtenga información sobre cómo proporcionar acceso de cliente SMB de ONTAP a enlaces simbólicos de UNIX

Un enlace simbólico es un archivo creado en un entorno UNIX que contiene una referencia a otro archivo o directorio. Si un cliente accede a un enlace simbólico, se redirige al cliente al archivo o directorio de destino al que hace referencia el enlace simbólico. ONTAP soporta enlaces simbólicos relativos y absolutos, incluyendo enlaces de widelinks (enlaces absolutos con destinos fuera del sistema de archivos local).

ONTAP proporciona a los clientes SMB la capacidad de seguir enlaces simbólicos UNIX configurados en la SVM. Esta función es opcional y puede configurarla por recurso compartido, utilizando la `-symlink -properties` opción del `vserver cifs share create` comando, con una de las siguientes opciones:

- Habilitada con acceso de lectura/escritura
- Habilitado con acceso de solo lectura
- Desactivado mediante la ocultación de enlaces simbólicos de clientes SMB
- Deshabilitado sin acceso a enlaces simbólicos de clientes SMB

Si habilita enlaces simbólicos en un recurso compartido, los enlaces simbólicos relativos funcionan sin más configuración.

Si activa enlaces simbólicos en un recurso compartido, los enlaces simbólicos absolutos no funcionan de inmediato. Primero debe crear una asignación entre la ruta UNIX del enlace simbólico a la ruta SMB de destino. Al crear asignaciones de vínculos simbólicos absolutos, puede especificar si se trata de un enlace local o de un *widelink*; las widelinks pueden ser enlaces a sistemas de archivos en otros dispositivos de almacenamiento o vínculos a sistemas de archivos alojados en SVM independientes en el mismo sistema ONTAP. Al crear un windelink, debe incluir la información que debe seguir el cliente; es decir, cree un punto de reanálisis para que el cliente detecte el punto de unión del directorio. Si crea un vínculo simbólico absoluto a un archivo o directorio fuera del recurso compartido local pero establece la localidad en local, ONTAP no permite el acceso al destino.

> Si un cliente intenta eliminar un enlace simbólico local (absoluto o relativo), sólo se eliminará el enlace simbólico, no el archivo o directorio de destino. Sin embargo, si un cliente intenta eliminar un widelink, podría eliminar el archivo de destino real o el directorio al que hace referencia el widelink. ONTAP no tiene control sobre esto, ya que el cliente puede abrir de forma explícita el archivo o directorio de destino fuera de la SVM y eliminarlo.

- **Puntos de análisis y servicios del sistema de archivos ONTAP**

  Un *reanálisis point* es un objeto del sistema de archivos NTFS que se puede almacenar opcionalmente en volúmenes junto con un archivo. Los puntos de análisis proporcionan a los clientes SMB la capacidad de recibir servicios del sistema de archivos mejorados o ampliados al trabajar con volúmenes de estilo NTFS. Los puntos de reanálisis constan de etiquetas estándar que identifican el tipo de punto de reanálisis y el contenido del punto de reanálisis que pueden recuperar los clientes SMB para un procesamiento posterior por parte del cliente. De los tipos de objeto disponibles para la funcionalidad ampliada del sistema de archivos, ONTAP implementa la compatibilidad con enlaces simbólicos NTFS y puntos de unión de directorios mediante etiquetas de punto de reanálisis. Los clientes SMB que no pueden comprender el contenido de un punto de análisis simplemente lo ignoran y no proporcionan el servicio de sistema de archivos ampliado que podría habilitar el punto de análisis.

- **Puntos de unión de directorios y soporte de ONTAP para enlaces simbólicos**

  Los puntos de unión de directorios son ubicaciones dentro de una estructura de directorios del sistema de archivos que pueden hacer referencia a ubicaciones alternativas en las que se almacenan los archivos, ya sea en una ruta de acceso diferente (enlaces simbólicos) o en un dispositivo de almacenamiento independiente (widelinks). Los servidores SMB de ONTAP exponen los puntos de unión de directorios a los clientes de Windows como puntos de análisis, lo que permite a los clientes con capacidad obtener contenidos de punto de análisis de ONTAP cuando se pasa un punto de unión de directorios. De este modo, pueden navegar y conectarse a diferentes rutas o dispositivos de almacenamiento, como si formaran parte del mismo sistema de archivos.

- **Activación de la compatibilidad con el uso de las opciones de punto de reanálisis**

`-is-use-junctions-as-reparse-points-enabled`La opción está habilitada de forma predeterminada en ONTAP 9. La opción para habilitar la información se puede configurar según la versión del protocolo, ya que no todos los clientes SMB admiten enlaces anchos. Esto permite a los administradores adaptar tanto a clientes SMB compatibles como a los no compatibles. Debe habilitar esta opción. `-widelink-as-reparse-point-versions` para cada protocolo de cliente que accede al recurso compartido mediante enlaces anchos; el valor predeterminado es SMB1.

Información relacionada

- "Aplicaciones de backup de Windows y symlinks de tipo Unix"
- "Documentación de Microsoft: Puntos de análisis"

Límites al configurar enlaces simbólicos de UNIX para el acceso SMB de ONTAP

Debe estar al tanto de determinados límites al configurar los enlaces simbólicos UNIX para el acceso a SMB.

Límite	Descripción
45	Longitud máxima del nombre del servidor CIFS que puede especificar al usar un FQDN para el nombre del servidor CIFS. También puede especificar el nombre del servidor CIFS como nombre NetBIOS, que está limitado a 15 caracteres.
80	La longitud máxima del nombre del recurso compartido.
256	Longitud máxima de la ruta de UNIX que puede especificar al crear un enlace simbólico o al modificar la ruta de UNIX de un enlace simbólico existente. La ruta de acceso de UNIX debe comenzar con un '/" (slash) and end with a "/'. Las barras diagonales iniciales y finales cuentan como parte del límite de 256 caracteres.
256	Longitud máxima de la ruta CIFS que puede especificar al crear un enlace simbólico o al modificar la ruta CIFS de un enlace simbólico existente. La ruta CIFS debe empezar por ' '/" (slash) and end with a " /'. Las barras diagonales iniciales y finales cuentan como parte del límite de 256 caracteres.

Información relacionada

Crear asignaciones de enlaces simbólicos para acciones

Controlar anuncios DFS automáticos en servidores SMB de ONTAP

Una opción de servidor CIFS controla cómo se anuncian las funcionalidades DFS a los clientes SMB al conectarse a recursos compartidos. Dado que ONTAP utiliza referencias DFS cuando los clientes acceden a enlaces simbólicos a través de SMB, debe ser consciente del impacto que tiene al deshabilitar o habilitar esta opción.

Una opción de servidor CIFS determina si los servidores CIFS se anuncian automáticamente que son DFS capaz de clientes SMB. De forma predeterminada, esta opción está habilitada y el servidor CIFS siempre anuncia que es DFS capaz de los clientes SMB (incluso cuando se conecta a recursos compartidos donde el acceso a enlaces simbólicos está deshabilitado). Si desea que el servidor CIFS anuncie que es compatible con DFS sólo cuando se conectan a recursos compartidos donde está habilitado el acceso a enlaces simbólicos, puede deshabilitar esta opción.

Debe tener en cuenta lo que ocurre cuando se deshabilita esta opción:

- La configuración de uso compartido de los enlaces simbólicos no cambia.
- Si el parámetro share se establece para permitir el acceso de enlace simbólico (ya sea de lectura y escritura o de sólo lectura), el servidor CIFS DFS anuncia capacidades a clientes que se conectan a ese recurso compartido.

  Las conexiones del cliente y el acceso a enlaces simbólicos se mantienen sin interrupción.

- Si el parámetro share se establece para no permitir el acceso de enlace simbólico (ya sea deshabilitando el acceso o si el valor del parámetro share es null), el servidor CIFS no anuncia capacidades DFS a clientes que se conectan a ese recurso compartido.

  Como los clientes tienen información en caché que el servidor CIFS es compatible con DFS y ya no anuncia que es, es posible que los clientes conectados a recursos compartidos donde se deshabilita el acceso a enlaces simbólicos no puedan acceder a estos recursos compartidos una vez que se deshabilita la opción de servidor CIFS. Después de deshabilitar la opción, es posible que deba reiniciar los clientes conectados a estos recursos compartidos, borrando de esta forma la información almacenada en caché.

Estos cambios no se aplican a conexiones SMB 1.0.

Configurar la compatibilidad con enlaces simbólicos de UNIX en recursos compartidos SMB de ONTAP

Puede configurar la compatibilidad de vínculos simbólicos de UNIX en recursos compartidos de SMB especificando una configuración de propiedad de recurso compartido de vínculo simbólico al crear recursos compartidos de SMB o en cualquier momento mediante la modificación de recursos compartidos de SMB existentes. La compatibilidad con el enlace simbólico de UNIX está habilitada de forma predeterminada. También puede deshabilitar la compatibilidad con enlaces simbólicos de UNIX en un recurso compartido.

Acerca de esta tarea

Al configurar la compatibilidad de enlaces simbólicos de UNIX para recursos compartidos de SMB, puede elegir una de las siguientes opciones de configuración:

Ajuste	Descripción
`enable` (ANTICUADO*)	Especifica que los enlaces simbólicos están habilitados para el acceso de lectura y escritura.
`read_only` (ANTICUADO*)	Especifica que los enlaces simbólicos están habilitados para el acceso de sólo lectura. Esta configuración no se aplica a las tintas widelinks. El acceso a Widelink siempre es de lectura y escritura.
`hide` (ANTICUADO*)	Especifica que los clientes SMB no pueden ver enlaces simbólicos.
`no-strict-security`	Especifica que los clientes siguen enlaces simbólicos fuera de los límites de recursos compartidos.
`symlinks`	Especifica que los enlaces simbólicos están habilitados localmente para el acceso de lectura y escritura. Los anuncios DFS no se generan incluso si la opción CIFS `is-advertise-dfs-enabled` está establecida en `true`. Esta es la configuración predeterminada.
`symlinks-and-widelinks`	Especifica que tanto los enlaces simbólicos locales como los widelinks para el acceso de lectura y escritura. Los anuncios DFS se generan tanto para enlaces simbólicos locales como widelinks incluso si la opción CIFS `is-advertise-dfs-enabled` está establecida en `false`.
`disable`	Especifica que los enlaces simbólicos y las tintas widelinks están desactivados. Los anuncios DFS no se generan incluso si la opción CIFS `is-advertise-dfs-enabled` está establecida en `true`.
`""` (nulo, no definido)	Deshabilita los enlaces simbólicos en el recurso compartido.
– (no configurado)	Deshabilita los enlaces simbólicos en el recurso compartido.

*Los parámetros *enable*, *ocultar* y *Read-only* están obsoletos y se pueden eliminar en una futura versión de ONTAP.

Pasos

1. Configure o deshabilite el soporte de enlaces simbólicos:

Si es…	Introduzca…
Un nuevo recurso compartido de SMB	`+vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink -properties {enable
hide	read-only
""	-
symlinks	symlinks-and-widelinks
disable},…]+`	Un recurso compartido de SMB existente
`+vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable	hide
read-only	""
-	symlinks
symlinks-and-widelinks	disable},…]+`

2. Compruebe que la configuración del recurso compartido de SMB sea correcta: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Ejemplo

El siguiente comando crea un recurso compartido SMB llamado «ata1» con la configuración de enlace simbólico de UNIX establecida en `enable`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
          CIFS Server NetBIOS Name: VS1
                             Path: /data1
                   Share Properties: oplocks
                                     browsable
                                     changenotify
                 Symlink Properties: enable
           File Mode Creation Mask: -
      Directory Mode Creation Mask: -
                    Share Comment: -
                        Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                      Volume Name: -
                    Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Información relacionada

Crear asignaciones de enlaces simbólicos para acciones

Crear asignaciones de enlaces simbólicos para recursos compartidos SMB de ONTAP

Puede crear asignaciones de enlaces simbólicos UNIX para los recursos compartidos de SMB. Puede crear un vínculo simbólico relativo, que hace referencia al archivo o la carpeta relativa a su carpeta principal, o bien puede crear un vínculo simbólico absoluto, que hace referencia al archivo o la carpeta utilizando una ruta absoluta.

Acerca de esta tarea

Los usuarios de Mac OS X no pueden acceder a Widelinks si utilizan SMB 2.x. Cuando un usuario intenta conectarse a un recurso compartido mediante widelinks desde un cliente Mac OS X, el intento falla. Sin embargo, puede utilizar widelinks con clientes Mac OS X si utiliza SMB 1.

Pasos

1. Para crear asignaciones de enlaces simbólicos para recursos compartidos de SMB: `vserver cifs symlink create -vserver virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-directory {true|false}]`

   `-vserver virtual_server_name` Especifica el nombre de la máquina virtual de almacenamiento

(SVM).

`-unix-path path` Especifica la ruta UNIX. La ruta UNIX debe empezar por una barra diagonal (`/`) y debe terminar con una barra diagonal (`/`).

`-share-name share_name` Especifica el nombre del recurso compartido de SMB que se va a asignar.

`-cifs-path path` Especifica la ruta CIFS. La ruta CIFS debe comenzar con una barra diagonal (`/`) y debe terminar con una barra diagonal (`/`).

`-cifs-server server_name` Especifica el nombre del servidor CIFS. El nombre del servidor CIFS puede especificarse como un nombre DNS (por ejemplo, mynetwork.cifs.server.com), una dirección IP o un nombre NetBIOS. El nombre de NetBIOS se puede determinar mediante el `vserver cifs show` comando. Si no se especifica este parámetro opcional, el valor predeterminado es el nombre NetBIOS del servidor CIFS local.

`-locality local|free|widelink}` especifica si se debe crear un enlace local, un enlace libre o un enlace simbólico amplio. Un enlace simbólico local se asigna al recurso compartido local de SMB. Un enlace simbólico gratuito puede asignar en cualquier parte del servidor SMB local. Un amplio enlace simbólico se asigna a cualquier recurso compartido de SMB en la red. Si no se especifica este parámetro opcional, el valor por defecto es `local`.

`-home-directory true false}` especifica si el recurso compartido de destino es un directorio raíz. Aunque este parámetro sea opcional, debe definir este parámetro en `true` cuando el recurso compartido de destino esté configurado como directorio raíz. El valor predeterminado es `false`.

Ejemplo

El siguiente comando crea una asignación de enlaces simbólicos en la SVM llamada vs1. Tiene la ruta UNIX `/src/` , el nombre compartido SMB 'SOURCE', la ruta CIFS `/mycompany/source/` y la dirección IP del servidor CIFS 123.123.123.123, y es un enlace inalámbrico.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

Información relacionada

Configurar la compatibilidad de enlaces simbólicos de UNIX en recursos compartidos

Comandos ONTAP para administrar asignaciones de enlaces simbólicos SMB

Hay comandos ONTAP específicos para gestionar las asignaciones de enlaces simbólicos.

Si desea…	Se usa este comando…
Cree una asignación de vínculos simbólicos	`vserver cifs symlink create`
Mostrar información acerca de las asignaciones de enlaces simbólicos	`vserver cifs symlink show`

Si desea…	Se usa este comando…
Modificar una asignación de vínculos simbólicos	`vserver cifs symlink modify`
Eliminar una asignación de vínculos simbólicos	`vserver cifs symlink delete`

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

Aplicaciones de copia de seguridad de Windows y enlaces simbólicos de estilo Unix en servidores SMB de ONTAP

Cuando una aplicación de copia de seguridad que se ejecuta en Windows encuentra un enlace simbólico de estilo Unix (symlink), se sigue el enlace y se realiza una copia de seguridad de los datos. A partir de ONTAP 9.15.1, tiene la opción de realizar una copia de seguridad de los symlinks en lugar de los datos. Esta función es totalmente compatible con volúmenes de ONTAP FlexGroup y FlexVols.

Descripción general

Antes de cambiar la forma en que ONTAP maneja los enlaces simbólicos durante una operación de copia de seguridad de Windows, debería estar familiarizado con las ventajas, los conceptos clave y las opciones de configuración.

Beneficios

Cuando esta función está desactivada o no disponible, se recorre cada enlace simbólico y se realiza una copia de seguridad de los datos a los que enlaza. Debido a esto, a veces se puede hacer un backup de los datos innecesarios y en ciertas situaciones la aplicación podría terminar en un bucle. En su lugar, la copia de seguridad de los enlaces simbólicos evita estos problemas. Y como los archivos symlink son muy pequeños en comparación con los datos en la mayoría de los casos, las copias de seguridad tardan menos tiempo en completarse. El rendimiento general del clúster también puede mejorar debido a la reducción de las operaciones de I/O.

Entorno de servidor Windows

Esta función es compatible con aplicaciones de backup que se ejecutan en Windows. Debe comprender los aspectos técnicos relevantes del entorno antes de utilizarlo.

Atributos ampliados

Windows admite atributos extendidos (EA) que forman colectivamente metadatos adicionales asociados opcionalmente a los archivos. Estos atributos los utilizan varias aplicaciones, como el subsistema de Windows para Linux, como se describe en "Permisos de archivo para WSL". Las aplicaciones pueden solicitar atributos ampliados para cada archivo al leer datos de ONTAP.

Los enlaces simbólicos se devuelven en los atributos extendidos cuando la función está activada. Por lo tanto, una aplicación de copia de seguridad debe proporcionar compatibilidad de EA estándar que se utiliza para almacenar los metadatos. Algunas utilidades de Windows admiten y conservan los atributos extendidos. Sin embargo, si el software de copia de seguridad no admite la copia de seguridad y la restauración de los atributos extendidos, no conservará los metadatos asociados con cada archivo y no podrá procesar los enlaces simbólicos correctamente.

Configuración de Windows

Las aplicaciones de copia de seguridad que se ejecutan en un servidor de Microsoft Windows pueden tener un privilegio especial que les permite omitir la seguridad de archivos normal. Esto se realiza normalmente agregando las aplicaciones al grupo Operadores de copia de seguridad. A continuación, las aplicaciones pueden realizar copias de seguridad y restaurar archivos según sea necesario, así como realizar otras operaciones relacionadas con el sistema. Se producen sutiles cambios en el protocolo SMB que utilizan las aplicaciones de backup que ONTAP puede detectar a medida que se leen y escriben los datos.

Requisitos

La función de copia de seguridad Symlink tiene varios requisitos, entre los que se incluyen:

- El clúster ejecuta ONTAP 9.15.1 o una versión posterior.
- Aplicación de copia de seguridad de Windows a la que se han otorgado privilegios de copia de seguridad especiales.
- La aplicación de backup también debe admitir atributos ampliados y solicitarlos durante las operaciones de backup.
- La función de backup de symlink de ONTAP está habilitada para la SVM de datos correspondiente.

Opciones de configuración

Además de la interfaz de línea de comandos de ONTAP, también es posible gestionar esta función mediante la API de REST. Consulte "Novedades de la API de REST DE ONTAP y la automatización" para obtener más información. La configuración que determina cómo ONTAP procesa los enlaces simbólicos de estilo Unix se debe realizar por separado en cada SVM.

Habilite la función de backup de symlink en ONTAP

Se introdujo una opción de configuración en un comando de la CLI existente con ONTAP 9.15.1. Puede utilizar esta opción para activar o desactivar el procesamiento de enlaces simbólicos de estilo Unix.

Antes de empezar

Revise el básico Requisitos. Además:

- Sea capaz de elevar su privilegio de CLI al nivel avanzado.
- Determine la SVM de datos que desea modificar. La SVM `vs1` se usa en el comando de ejemplo.

Pasos

1. Establezca el nivel de privilegio avanzado.

```
set privilege advanced
```

2. Active la copia de seguridad de archivos symlink.

```
vserver cifs options modify -vserver vs1 -is-backup-symlink-enabled true
```

Utilice BranchCache para almacenar en caché contenido compartido SMB en una sucursal

Obtenga información sobre el uso de BranchCache para almacenar en caché el contenido compartido de ONTAP SMB en una sucursal

BranchCache fue desarrollado por Microsoft para permitir el almacenamiento de contenido en la caché de los equipos locales de los clientes que lo soliciten. La implementación de BranchCache por parte de ONTAP puede reducir la utilización de la red de área amplia (WAN) y proporcionar un tiempo de respuesta de acceso mejorado cuando los usuarios de una sucursal acceden al contenido almacenado en máquinas virtuales de almacenamiento (SVM) mediante SMB.

Si configura BranchCache, los clientes de Windows BranchCache en primer lugar recuperan el contenido de la SVM y, a continuación, almacenan en caché el contenido de un equipo dentro de la sucursal. Si otro cliente con BranchCache habilitado en la sucursal solicita el mismo contenido, la SVM primero autentica y autoriza al usuario solicitante. A continuación, la SVM determina si el contenido en caché aún está actualizado y, si lo está, envía los metadatos del cliente sobre el contenido en caché. A continuación, el cliente utiliza los metadatos para recuperar contenido directamente desde la memoria caché basada en la ubicación local.

Información relacionada

Obtenga información sobre el uso de archivos sin conexión para permitir el almacenamiento en caché de archivos para su uso sin conexión

Requisitos y directrices

Obtenga información sobre la compatibilidad de versiones de ONTAP SMB BranchCache

Debe tener en cuenta qué versiones de BranchCache son compatibles con ONTAP.

ONTAP es compatible con BranchCache 1 y con BranchCache 2 mejorado:

- Cuando se configura BranchCache en el servidor SMB para la máquina virtual de almacenamiento (SVM), puede habilitar BranchCache 1, BranchCache 2 o todas las versiones.

  De forma predeterminada, todas las versiones están habilitadas.

- Si solo habilita BranchCache 2, los equipos cliente Windows de oficina remota deben admitir BranchCache 2.

  Solo los clientes SMB 3.0 o una versión posterior admiten BranchCache 2.

Para obtener más información sobre las versiones de BranchCache, consulte la biblioteca de Microsoft TechNet.

Información relacionada

"Biblioteca de Microsoft TechNet: technet.microsoft.com/en-us/library/"

Obtenga información sobre los requisitos de compatibilidad del protocolo de red SMB de ONTAP

Debe tener en cuenta los requisitos del protocolo de red para implementar BranchCache de ONTAP.

Puede implementar la función ONTAP BranchCache en redes IPv4 e IPv6 mediante SMB 2.1 o una versión posterior.

Todos los servidores CIFS y los equipos de oficinas remotas que participan en la implementación de BranchCache deben tener habilitado el protocolo SMB 2.1 o una versión posterior. SMB 2.1 tiene extensiones de protocolo que permiten que un cliente participe en un entorno de BranchCache. Esta es la versión mínima del protocolo SMB que ofrece compatibilidad con BranchCache. SMB 2.1 admite la versión de BranchCache, versión 1.

Si desea usar BranchCache versión 2, SMB 3.0 es la versión mínima admitida. Todos los servidores CIFS y los equipos de oficinas remotas que participan en una implementación de BranchCache 2 deben tener habilitado SMB 3.0 o una versión posterior.

Si tiene oficinas remotas en las que algunos clientes solo admiten SMB 2.1 y algunos de los clientes admiten SMB 3.0, puede implementar una configuración de BranchCache en el servidor CIFS que proporcione compatibilidad con el almacenamiento en caché tanto en BranchCache 1 como en BranchCache 2.

Aunque la función Microsoft BranchCache admite el uso de los protocolos HTTP/HTTPS y SMB como protocolos de acceso a archivos, ONTAP BranchCache solo admite el uso de SMB.

Obtenga información sobre los requisitos de las versiones de hosts de ONTAP SMB y Windows

Los hosts de ONTAP y de oficina remota deben cumplir determinados requisitos de versión para poder configurar BranchCache.

Antes de configurar BranchCache, debe asegurarse de que la versión de ONTAP en el clúster y los clientes de la sucursal participantes sean compatibles con SMB 2.1 o una versión posterior y con la función de BranchCache. Si configura el modo de caché alojada, también debe asegurarse de que utiliza un host compatible para el servidor de caché.

BranchCache 1 es compatible con las siguientes versiones de ONTAP y hosts de Windows:

- Servidor de contenido: Máquina virtual de almacenamiento (SVM) con ONTAP
- Servidor de caché: Windows Server 2008 R2 o Windows Server 2012 o posterior
- Igual o cliente: Windows 7 Enterprise, Windows 7 Ultimate, Windows 8, Windows Server 2008 R2 o Windows Server 2012 o posterior

BranchCache 2 es compatible con las siguientes versiones de ONTAP y hosts de Windows:

- Servidor de contenido: SVM con ONTAP
- Servidor de caché: Windows Server 2012 o posterior
- Igual o cliente: Windows 8 o Windows Server 2012 o posterior

Conozca las razones por las que ONTAP SMB invalida los hashes de BranchCache

Comprender los motivos por los que ONTAP invalida los hash puede ser útil a la hora de planificar la configuración de BranchCache. Puede ayudarle a decidir el modo operativo que debe configurar y a elegir en qué recursos compartidos desea habilitar BranchCache.

ONTAP debe gestionar los hash de BranchCache para garantizar que sean válidos. Si un hash no es válido,

ONTAP invalida el hash y calcula un nuevo hash la próxima vez que se solicite el contenido, suponiendo que BranchCache siga estando habilitado.

ONTAP invalida los hash por los siguientes motivos:

- Se modifica la clave de servidor.

  Si se modifica la clave del servidor, ONTAP invalida todos los hash del almacén hash.

- Un hash se vacía de la caché porque se alcanzó el tamaño máximo del almacén hash de BranchCache.

  Se trata de un parámetro ajustable y puede modificarse para satisfacer sus requisitos empresariales.

- Un archivo se modifica mediante un acceso SMB o NFS.
- Un archivo para el que hay hash calculados se restaura con `snap restore` el comando.
- Un volumen que contiene recursos compartidos de SMB que tienen habilitada para BranchCache se restaura mediante `snap restore` el comando.

Obtenga información sobre cómo elegir la ubicación del almacén de hash de ONTAP SMB

Al configurar BranchCache, elija dónde almacenar los hash y qué tamaño debe tener el almacén hash. Las directrices a la hora de elegir la ubicación y el tamaño del almacén hash pueden ayudarle a planificar la configuración de BranchCache en una SVM habilitada para CIFS.

- Debe localizar el almacén hash en un volumen en el que se permitan las actualizaciones de atime.

  El tiempo de acceso de un archivo hash se utiliza para mantener los archivos a los que se accede con más frecuencia en el almacén hash. Si las actualizaciones de atime están deshabilitadas, se utiliza la hora de creación con este fin. Es preferible utilizar atime para realizar un seguimiento de los archivos utilizados con frecuencia.

- No puede almacenar hash en sistemas de archivos de solo lectura como los destinos de SnapMirror y los volúmenes SnapLock.
- Si se alcanza el tamaño máximo del almacén hash, los hash más antiguos se vacían para crear espacio para los hash nuevos.

  Es posible aumentar el tamaño máximo del almacén hash para reducir la cantidad de hash que se vacía de la caché.

- Si el volumen en el que almacena hash no está disponible o lleno, o si hay un problema con la comunicación dentro del clúster donde el servicio BranchCache no puede recuperar información hash, los servicios de BranchCache no estarán disponibles.

  El volumen puede no estar disponible porque está sin conexión o porque el administrador de almacenamiento especificó una nueva ubicación para el almacén de hash.

  Esto no provoca problemas con el acceso a archivos. Si se ve afectado el acceso al almacén hash, ONTAP devolverá un error definido por Microsoft al cliente, que hace que el cliente solicite el archivo con la solicitud de lectura SMB normal.

Información relacionada

- Configurar BranchCache en los servidores
- Modificar las configuraciones de BranchCache en los recursos compartidos

Conozca las recomendaciones de ONTAP SMB BranchCache

Antes de configurar BranchCache, hay ciertas recomendaciones que debe tener en cuenta a la hora de decidir qué recursos compartidos de SMB desea habilitar el almacenamiento en caché de BranchCache.

Debe tener en cuenta las siguientes recomendaciones a la hora de decidir qué modo operativo usar y en qué recursos compartidos de SMB para habilitar BranchCache:

- Las ventajas de BranchCache se reducen cuando los datos que se van a almacenar en caché de forma remota cambian con frecuencia.
- Los servicios de BranchCache son beneficiosos para los recursos compartidos que contienen contenido de archivos que se vuelve a utilizar por varios clientes de oficina remota o por contenido de archivo al que un único usuario remoto accede en repetidas ocasiones.
- Considere la posibilidad de habilitar el almacenamiento en caché para contenido de solo lectura, como datos en snapshots y destinos SnapMirror.

Configure BranchCache

Obtenga más información sobre la configuración de ONTAP SMB BranchCache

Puede configurar BranchCache en el servidor SMB con los comandos de la ONTAP. Para implementar BranchCache, también debe configurar los clientes y, opcionalmente, los servidores de caché alojados en las sucursales en las que desea almacenar en caché el contenido.

Si configura BranchCache para habilitar el almacenamiento en caché de recurso compartido por recurso, debe habilitar BranchCache en los recursos compartidos SMB para los que desea proporcionar servicios de almacenamiento en caché de BranchCache.

Requisitos para configurar ONTAP SMB BranchCache

Después de cumplir algunos requisitos previos, puede configurar BranchCache.

Debe cumplir los siguientes requisitos antes de configurar BranchCache en el servidor CIFS para la SVM:

- ONTAP debe instalarse en todos los nodos del clúster.
- CIFS debe tener una licencia y se debe configurar un servidor SMB. La licencia SMB se incluye con "ONTAP One". Si no tiene ONTAP One y la licencia no está instalada, póngase en contacto con su representante de ventas.
- Se debe configurar la conectividad de red IPv4 o IPv6.
- Para BranchCache 1, se debe habilitar SMB 2.1 o una versión posterior.
- Para BranchCache 2, se debe habilitar SMB 3.0 y los clientes de Windows remotos deben admitir BranchCache 2.

Puede configurar BranchCache para proporcionar servicios de BranchCache por recurso compartido. Como alternativa, puede configurar BranchCache para habilitar automáticamente el almacenamiento en caché en todos los recursos compartidos de SMB.

Acerca de esta tarea

Puede configurar BranchCache en las SVM.

- Puede crear una configuración de BranchCache para todos los recursos compartidos si desea ofrecer servicios de almacenamiento en caché para todo el contenido en todos los recursos compartidos SMB en el servidor CIFS.
- Puede crear una configuración de BranchCache por recurso compartido si desea ofrecer servicios de almacenamiento en caché para el contenido de ciertos recursos compartidos SMB en el servidor CIFS.

Debe especificar los siguientes parámetros al configurar BranchCache:

Parámetros necesarios	Descripción
SVM name	BranchCache se configura por SVM. Debe especificar en qué SVM con la función CIFS habilitada desea configurar el servicio BranchCache.
Path to hash store	Los hash de BranchCache se almacenan en archivos normales del volumen de SVM. Debe especificar la ruta a un directorio existente en el que desea que ONTAP almacene los datos de hash.la ruta hash de BranchCache debe ser de lectura y escritura. No se admiten rutas de solo lectura, como los directorios de snapshots. Es posible almacenar datos de hash en un volumen que contiene otros datos o se puede crear un volumen independiente para almacenar datos hash. Si la SVM es un origen de recuperación ante desastres de SVM, la ruta de hash no puede estar en el volumen raíz. Esto se debe a que el volumen raíz no se replica en el destino de recuperación ante desastres. La ruta de hash puede contener espacios en blanco y cualquier carácter válido de nombre de archivo.

Opcionalmente, puede especificar los siguientes parámetros:

Parámetros opcionales	Descripción
Versiones compatibles	ONTAP admite BranchCache 1 y 2. Puede habilitar la versión 1, la versión 2 o ambas versiones. El valor predeterminado es habilitar ambas versiones.

Parámetros opcionales	Descripción
Tamaño máximo del almacén hash	Puede especificar el tamaño que se usará para el almacén de datos hash. Si los datos de hash superan este valor, ONTAP eliminará los hash más antiguos para hacer sitio a los más recientes. El tamaño predeterminado del almacén hash es 1 GB. BranchCache funciona de manera más eficiente si no se descartan los hash de una forma excesivamente agresiva. Si determina que los hash se descartan con frecuencia porque el almacén hash está lleno, puede aumentar el tamaño del almacén hash modificando la configuración de BranchCache.
Clave de servidor	Puede especificar una clave de servidor que el servicio de BranchCache utilice para evitar que los clientes suplanten el servidor de BranchCache. Si no se especifica una clave de servidor, se genera de forma aleatoria al crear la configuración de BranchCache. Puede establecer la clave de servidor como un valor específico, de modo que, si hay varios servidores que proporcionan datos de BranchCache para los mismos archivos, los clientes puedan usar hash de cualquier servidor que utilice la misma clave de servidor. Si la clave de servidor contiene espacios, debe escribirla entre comillas.
Modo de funcionamiento	El valor predeterminado es habilitar BranchCache por recurso compartido. • Para crear una configuración de BranchCache donde se habilita BranchCache por recurso compartido, no se puede especificar este parámetro opcional o se puede especificar `per-share`. • Para habilitar automáticamente BranchCache en todos los recursos compartidos, debe establecer el modo operativo en `all-shares`.

Pasos

1. Habilite SMB 2.1 y 3.0 según sea necesario:
   a. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
   b. Compruebe la configuración de SMB de SVM configurada para determinar si todas las versiones necesarias de SMB están habilitadas: `vserver cifs options show -vserver` *`vserver_name`*
   c. Si es necesario, habilite SMB 2,1: `vserver cifs options modify -vserver` *`vserver_name`* `-smb2-enabled true`

      El comando habilita SMB 2.0 y SMB 2.1.

   d. Si es necesario, habilite SMB 3,0: `vserver cifs options modify -vserver` *`vserver_name`*

```
-smb3-enabled true
```

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

2. Configurar BranchCache: `vserver cifs branchcache create -vserver vserver_name -hash -store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all] [-server-key text] -operating-mode {per-share|all-shares}`

   La ruta de almacenamiento hash especificada debe existir y debe residir en un volumen gestionado por la SVM. La ruta también debe ubicarse en un volumen de lectura y escritura. El comando falla si la ruta es de solo lectura o no existe.

   Si desea usar la misma clave de servidor para configuraciones de BranchCache adicionales, registre el valor introducido para la clave de servidor. La clave de servidor no aparece cuando se muestra información sobre la configuración de BranchCache.

3. Compruebe que la configuración de BranchCache sea correcta: `vserver cifs branchcache show -vserver vserver_name`

Ejemplos

Los siguientes comandos verifican que tanto SMB 2.1 como 3.0 están habilitadas y configuran BranchCache para permitir automáticamente el almacenamiento en caché de todos los recursos compartidos de SMB en SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true


cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares
```

Los siguientes comandos verifican que tanto SMB 2.1 como 3.0 están habilitadas, configure BranchCache para permitir el almacenamiento en caché de acuerdo con un recurso compartido en SVM vs1 y verifique la configuración de BranchCache:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Información relacionada

- Obtenga más información sobre la compatibilidad de versiones de BranchCache
- Obtenga información sobre cómo configurar BranchCache en la oficina remota
- Cree un recurso compartido de SMB habilitado con BranchCache
- Habilitar BranchCache en recursos compartidos existentes
- Modificar las configuraciones de BranchCache en los recursos compartidos
- Obtenga información sobre cómo deshabilitar BranchCache en los recursos compartidos
- Eliminar la configuración de BranchCache en los recursos compartidos

Obtenga información sobre cómo configurar BranchCache en la oficina remota en ONTAP SMB

Después de configurar BranchCache en el servidor SMB, debe instalar y configurar BranchCache en los equipos cliente y, opcionalmente, en los servidores de almacenamiento en caché de la oficina remota. Microsoft proporciona instrucciones para la configuración de BranchCache en la oficina remota.

Las instrucciones para configurar clientes de sucursal y, de manera opcional, los servidores de almacenamiento en caché que usen BranchCache se encuentran en el sitio web de Microsoft BranchCache.

"Microsoft BranchCache Docs: Novedades"

Configure los recursos compartidos SMB habilitados para BranchCache

Obtenga información sobre cómo configurar recursos compartidos SMB de ONTAP habilitados para BranchCache

Una vez que configura BranchCache en el servidor SMB y en la sucursal, puede habilitar BranchCache en recursos compartidos SMB que contienen contenido que desea permitir que los clientes de las sucursales se almacenan en caché.

El almacenamiento en caché de BranchCache puede habilitarse en todos los recursos compartidos de SMB en el servidor SMB o de recurso compartido por recurso.

- Si habilita BranchCache por recurso compartido, puede habilitar BranchCache a medida que crea el recurso compartido o modifica los recursos compartidos existentes.

  Si habilita el almacenamiento en caché en un recurso compartido de SMB existente, ONTAP comienza a enviar hashes de computación y metadatos a clientes que soliciten contenido tan pronto como habilite BranchCache en ese recurso compartido.

- Todos los clientes que tengan una conexión SMB existente a un recurso compartido no obtienen compatibilidad con BranchCache si, a continuación, se habilita BranchCache en ese recurso compartido.

  ONTAP anuncia el soporte de BranchCache para un recurso compartido en el momento de la configuración de la sesión del bloque de mensajes del servidor. Los clientes que ya han establecido sesiones cuando se habilita BranchCache deben desconectar y volver a conectarse para usar el contenido en caché para este recurso compartido.

> Si BranchCache en un recurso compartido de SMB se encuentra deshabilitado posteriormente, ONTAP deja de enviar metadatos al cliente solicitante. Un cliente que necesita datos lo recupera directamente del servidor de contenido (servidor SMB).

Crear recursos compartidos SMB de ONTAP habilitados para BranchCache

Puede habilitar BranchCache en un recurso compartido de SMB cuando se crea el recurso compartido mediante la configuración `branchcache` de la propiedad de recurso compartido.

Acerca de esta tarea

- Si se habilita BranchCache en el recurso compartido de SMB, el recurso compartido debe tener la configuración de los archivos sin conexión establecida en el almacenamiento manual en caché.

  Esta es la configuración predeterminada cuando se crea un recurso compartido.

- También puede especificar parámetros de recurso compartido opcionales al crear el recurso compartido con BranchCache habilitado.
- Es posible establecer `branchcache` la propiedad en un recurso compartido aunque BranchCache no esté configurado y habilitado en la máquina virtual de almacenamiento (SVM).

  Sin embargo, si desea que el recurso compartido ofrezca contenido en caché, debe configurar y habilitar BranchCache en la SVM.

- Dado que no hay propiedades de recurso compartido predeterminadas aplicadas al recurso compartido al utilizar el `-share-properties` parámetro, debe especificar todas las demás propiedades de recurso compartido que desee aplicar al recurso compartido además de la `branchcache` propiedad de recurso compartido mediante una lista delimitada por comas.
- Obtenga más información sobre `vserver cifs share create` en el "Referencia de comandos del ONTAP".

Paso

1. Cree un recurso compartido de SMB habilitado para BranchCache:
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties branchcache[,…]`
2. Compruebe que la propiedad BranchCache Share esté configurada en el recurso compartido de SMB mediante `vserver cifs share show` el comando.

Ejemplo

El siguiente comando crea un recurso compartido SMB habilitado para BranchCache llamado «data» con una ruta de acceso `/data` de en SVM VS1. De forma predeterminada, la configuración de archivos fuera de línea se establece en `manual`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
                      Vserver: vs1
                        Share: data
     CIFS Server NetBIOS Name: VS1
                         Path: /data
             Share Properties: branchcache
                               oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: data
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Información relacionada

Deshabilitar BranchCache en un solo recurso compartido

Habilitar BranchCache en recursos compartidos SMB de ONTAP existentes

Puede habilitar BranchCache en un recurso compartido SMB existente agregando la

`branchcache` propiedad de recurso compartido a la lista existente de propiedades de recurso compartido.

Acerca de esta tarea

- Si se habilita BranchCache en el recurso compartido de SMB, el recurso compartido debe tener la configuración de los archivos sin conexión establecida en el almacenamiento manual en caché.

  Si la opción de archivos sin conexión del recurso compartido existente no está establecida en almacenamiento en caché manual, debe configurarlo modificando el recurso compartido.

- Es posible establecer `branchcache` la propiedad en un recurso compartido aunque BranchCache no esté configurado y habilitado en la máquina virtual de almacenamiento (SVM).

  Sin embargo, si desea que el recurso compartido ofrezca contenido en caché, debe configurar y habilitar BranchCache en la SVM.

- Al agregar `branchcache` la propiedad Compartir al recurso compartido, se conservan la configuración de recurso compartido existente y las propiedades de recurso compartido.

  La propiedad share de BranchCache se agrega a la lista existente de propiedades compartidas. Obtenga más información sobre `vserver cifs share properties add` en el "Referencia de comandos del ONTAP".

Pasos

1. Si es necesario, configure el parámetro de recursos compartidos de archivos sin conexión para el almacenamiento en caché manual:
   a. Determine cuál es el valor del recurso compartido de archivos sin conexión mediante el `vserver cifs share show` comando.
   b. Si la configuración de archivos compartidos sin conexión no está establecida en manual, cámbiela al valor necesario: `vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual`
2. Habilitar BranchCache en un recurso compartido de SMB existente: `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. Compruebe que la propiedad de recurso compartido de BranchCache esté configurada en el recurso compartido de SMB: `vserver cifs share show -vserver vserver_name -share-name share_name`

Ejemplo

El siguiente comando habilita BranchCache en un recurso compartido SMB existente denominado «dATA2» con una ruta de acceso `/data2` de en SVM VS1:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              showsnapshot
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties add  -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              showsnapshot
                              changenotify
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Información relacionada

- Agregar o eliminar propiedades de recursos compartidos en recursos compartidos existentes
- Deshabilitar BranchCache en un solo recurso compartido

Gestione y supervise la configuración de BranchCache

Modificar las configuraciones de BranchCache en los recursos compartidos SMB de ONTAP

Puede modificar la configuración del servicio BranchCache en las SVM, lo que incluye el cambio de la ruta de directorio del almacén hash, el tamaño máximo del directorio del almacén hash, el modo operativo y las versiones de BranchCache que son compatibles. También puede aumentar el tamaño del volumen que contiene el almacén hash.

Pasos

1. Ejecute la acción adecuada:

Si desea…	Introduzca lo siguiente…
Modifique el tamaño del directorio del almacén hash	`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB
MB	GB
TB	PB]}`
Aumente el tamaño del volumen que contiene el almacén hash	`volume size -vserver vserver_name -volume volume_name -new-size new_size[k
m	g
t]` Si el volumen que contiene el almacén hash se llena, es posible que pueda aumentar el tamaño del volumen. Puede especificar el nuevo tamaño del volumen como número, seguido de una designación de unidad. Más información acerca de "Gestión de volúmenes de FlexVol"	Modifique la ruta del directorio del almacén hash

Si desea…	Introduzca lo siguiente…
`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true	false}` Si la SVM es un origen de recuperación ante desastres de SVM, la ruta hash no puede estar en el volumen raíz. Esto se debe a que el volumen raíz no se replica en el destino de recuperación ante desastres. La ruta de hash de BranchCache puede contener espacios en blanco y cualquier carácter válido de nombre de archivo. Si modifica la ruta de hash, `-flush-hashes` es un parámetro requerido que especifica si desea que ONTAP vacíe los hash de la ubicación del almacén hash original. Puede definir los siguientes valores para el `-flush-hashes` parámetro: **Si especifica `true`, ONTAP eliminará los hash de la ubicación original y creará nuevos hash en la nueva ubicación a medida que los clientes habilitados para BranchCache realicen nuevas solicitudes.** Si especifica `false`, los hashes no se vacían. + En este caso, puede optar por reutilizar los hash existentes más adelante cambiando la ruta del almacén hash de vuelta a la ubicación original.
Cambie el modo de funcionamiento	`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share
all-shares	disable}` Debe tener en cuenta lo siguiente al modificar el modo de funcionamiento: **ONTAP anuncia el soporte de BranchCache para un recurso compartido cuando se configura la sesión SMB.** Los clientes que ya han establecido sesiones cuando se habilita BranchCache deben desconectar y volver a conectarse para usar el contenido en caché para este recurso compartido.
Cambie la compatibilidad de la versión de BranchCache	`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable
v2-enable	enable-all}`

2. Verifique los cambios de configuración con `vserver cifs branchcache show` el comando.

Mostrar información sobre las configuraciones de BranchCache en los recursos compartidos SMB de ONTAP

Puede mostrar información sobre las configuraciones de BranchCache en máquinas virtuales de almacenamiento (SVM), que se pueden utilizar al verificar una configuración o al determinar la configuración actual antes de modificar una configuración.

Paso

1. Ejecute una de las siguientes acciones:

Si desea mostrar…	Introduzca este comando…
Información resumida sobre las configuraciones de BranchCache en todas las SVM	`vserver cifs branchcache show`
Información detallada sobre la configuración de una SVM específica	`vserver cifs branchcache show -vserver` *`vserver_name`*

Ejemplo

En el siguiente ejemplo, se muestra información sobre la configuración de BranchCache en la SVM vs1:

```
cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
           Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
           Maximum Size of the Hash Store: 20GB
  Encryption Key Used to Secure the Hashes: -
         CIFS BranchCache Operating Modes: per_share
```

Cambiar la clave del servidor ONTAP SMB BranchCache

Puede cambiar la clave de servidor de BranchCache mediante la modificación de la configuración de BranchCache en la máquina virtual de almacenamiento (SVM) y la especificación de una clave de servidor diferente.

Acerca de esta tarea

Puede establecer la clave de servidor como un valor específico, de modo que, si hay varios servidores que proporcionan datos de BranchCache para los mismos archivos, los clientes puedan usar hash de cualquier servidor que utilice la misma clave de servidor.

Cuando cambia la clave de servidor, también debe vaciar la caché hash. Después de vaciar los hash, ONTAP crea nuevos hash a medida que los clientes habilitados para BranchCache crean nuevas solicitudes.

Pasos

1. Cambie la clave de servidor mediante el siguiente comando: `vserver cifs branchcache modify -vserver vserver_name -server-key text -flush-hashes true`

Al configurar una nueva clave de servidor, también debe especificar `-flush-hashes` y definir el valor en `true`.

2. Compruebe que la configuración de BranchCache sea correcta mediante `vserver cifs branchcache show` el comando.

Ejemplo

En el ejemplo siguiente se establece una nueva clave de servidor que contiene espacios y vacía la caché hash en la SVM vs1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Información relacionada

Conozca las razones por las que ONTAP invalida los hashes de BranchCache

Calcular previamente los hashes de BranchCache en rutas SMB de ONTAP específicas

Puede configurar el servicio BranchCache para que preajuste los valores hash de computación para un único archivo, para un directorio o para todos los archivos de una estructura de directorio. Esto puede resultar útil si desea calcular hash en datos de un recurso compartido habilitado con BranchCache durante las horas fuera de servicio y no en las horas punta.

Acerca de esta tarea

Si desea recoger una muestra de datos antes de mostrar estadísticas de hash, debe usar `statistics start` `statistics stop` los comandos opcionales y.

- Debe especificar la máquina virtual de almacenamiento (SVM) y la ruta en la que desea contar con los hash de tecnología previa.
- También debe especificar si desea calcular los valores hash de forma recursiva.
- Si desea calcular los hash de forma recursiva, el servicio BranchCache atraviesa todo el árbol de directorios bajo la ruta de acceso especificada y calcula los hash de cada objeto elegible.

  Obtenga más información sobre `statistics start` y `statistics stop` en el "Referencia de comandos del ONTAP" .

Pasos

1. Hash de precomputación como desee:

Si desea contar con hash de tecnología previa…	Introduzca el comando…
Un único archivo o directorio	`vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false`
Recursivamente en todos los archivos de una estructura de directorios	`vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true`

2. Verifique que los hash se están calculando mediante `statistics` el comando:

   a. Muestre estadísticas del `hashd` objeto en la instancia SVM deseada: `statistics show -object hashd -instance vserver_name`

   b. Compruebe que el número de hash creado aumenta repitiendo el comando.

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

Ejemplos

En el siguiente ejemplo se crean hash en la ruta `/data` y en todos los archivos y subdirectorios contenidos en SVM VS1:

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       85
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       92
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -
```

Información relacionada

- "Configuración de supervisión del rendimiento"

Limpiar hashes del almacén de hashes BranchCache de ONTAP SMB SVM

Puede vaciar todos los hash almacenados en caché del almacén hash de BranchCache en la máquina virtual de almacenamiento (SVM). Esto puede ser útil si ha cambiado la configuración de BranchCache de la sucursal. Por ejemplo, si recientemente reconfiguró el modo de almacenamiento en caché desde el almacenamiento en caché distribuido al modo de almacenamiento en caché alojado, debería vaciar el almacén hash.

Acerca de esta tarea

Después de vaciar los hash, ONTAP crea nuevos hash a medida que los clientes habilitados para BranchCache crean nuevas solicitudes.

Paso

1. Vacíe los hash del almacén hash de BranchCache: `vserver cifs branchcache hash-flush -vserver` *`vserver_name`*

   ```
   vserver cifs branchcache hash-flush -vserver vs1
   ```

Mostrar estadísticas de ONTAP SMB BranchCache

Puede mostrar las estadísticas de BranchCache para, entre otras cosas, identificar el nivel de rendimiento del almacenamiento en caché, determinar si su configuración proporciona contenido en caché a los clientes y determinar si los archivos hash se eliminaron para dar cabida a los datos hash más recientes.

Acerca de esta tarea

```
`hashd`El objeto de estadística contiene contadores que proporcionan
información estadística sobre los hashes de BranchCache.  `cifs`El objeto
estadístico contiene contadores que proporcionan información estadística
sobre la actividad relacionada con BranchCache. Puede recopilar y mostrar
información acerca de estos objetos en el nivel de privilegio avanzado.
```

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`

   ```
   cluster1::> set -privilege advanced

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

2. Muestre los contadores relacionados con BranchCache mediante `statistics catalog counter show` el comando.

   ```
   cluster1::*> statistics catalog counter show -object hashd
   ```

```
Object: hashd
    Counter                       Description
    ---------------------------
-------------------------------------------
    branchcache_hash_created      Number of times a request to generate
                                  BranchCache hash for a file succeeded.
    branchcache_hash_files_replaced
                                  Number of times a BranchCache hash file
was
                                  deleted to make room for more recent
hash
                                  data. This happens if the hash store
size is
                                  exceeded.
    branchcache_hash_rejected     Number of times a request to generate
                                  BranchCache hash data failed.
    branchcache_hash_store_bytes
                                  Total number of bytes used to store hash
data.
    branchcache_hash_store_size Total space used to store BranchCache
hash
                                  data for the Vserver.
    instance_name                 Instance Name
    instance_uuid                 Instance UUID
    node_name                     System node name
    node_uuid                     System node id
9 entries were displayed.

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                       Description
    ---------------------------
-------------------------------------------
    active_searches               Number of active searches over SMB and
SMB2
    auth_reject_too_many          Authentication refused after too many
                                  requests were made in rapid succession
    avg_directory_depth           Average number of directories crossed by
SMB
                                  and SMB2 path-based commands
    avg_junction_depth            Average number of junctions crossed by
SMB
                                  and SMB2 path-based commands
    branchcache_hash_fetch_fail Total number of times a request to fetch
```

```
hash
                                data failed. These are failures when
                                attempting to read existing hash data.
It
                                does not include attempts to fetch hash
data
                                that has not yet been generated.
    branchcache_hash_fetch_ok   Total number of times a request to fetch
hash
                                data succeeded.
    branchcache_hash_sent_bytes Total number of bytes sent to clients
                                requesting hashes.
    branchcache_missing_hash_bytes
                                Total number of bytes of data that had
to be
                                read by the client because the hash for
that
                                content was not available on the server.
    ....Output truncated....
```

Obtenga más información sobre `statistics catalog counter show` en el "Referencia de comandos del ONTAP".

3. Recopile estadísticas relacionadas con BranchCache mediante `statistics start` `statistics stop` los comandos y.

```
cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11
```

Obtenga más información sobre `statistics start` y `statistics stop` en el "Referencia de comandos del ONTAP" .

4. Muestre las estadísticas de BranchCache recogidas mediante `statistics show` el comando.

```
cluster1::*> statistics show -object cifs -counter
branchcache_hash_sent_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0

cluster1::*> statistics show -object cifs -counter
branchcache_missing_hash_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
```

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

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

```
cluster1::*> set -privilege admin
```

Información relacionada

- Mostrar estadísticas
- "Configuración de supervisión del rendimiento"
- "Las estadísticas comienzan"
- "las estadísticas se detienen"

Obtenga información sobre la compatibilidad de ONTAP SMB con los objetos de política de grupo de BranchCache

BranchCache de ONTAP proporciona compatibilidad con objetos de directiva de grupo (GPO) de BranchCache, los cuales permiten una gestión centralizada para ciertos parámetros de configuración de BranchCache. Hay dos GPO utilizados para BranchCache, la publicación Hash para el GPO de BranchCache y la compatibilidad con versiones Hash para el GPO de BranchCache.

- **Publicación Hash para BranchCache GPO**

  La publicación hash para GPO de BranchCache corresponde al `-operating-mode` parámetro. Cuando se producen actualizaciones de GPO, este valor se aplica a los objetos de máquinas virtuales de almacenamiento (SVM) contenidos en la unidad organizativa (OU) a la que se aplica la directiva de grupo.

- **Compatibilidad con la versión Hash para el GPO de BranchCache**

  La compatibilidad de versiones hash para GPO de BranchCache corresponde al `-versions` parámetro. Cuando se producen actualizaciones de GPO, este valor se aplica a los objetos SVM incluidos en la unidad organizativa a la que se aplica la directiva de grupo.

Información relacionada

Obtenga información sobre cómo aplicar objetos de directiva de grupo a servidores SMB

Mostrar información sobre los objetos de directiva de grupo de ONTAP SMB BranchCache

Puede mostrar información acerca de la configuración de objeto de directiva de grupo (GPO) del servidor CIFS para determinar si se definen GPO de BranchCache para el dominio al que pertenece el servidor CIFS y, si es así, ¿cuáles son las configuraciones permitidas? También puede determinar si la configuración de GPO de BranchCache se aplica al servidor CIFS.

Acerca de esta tarea

Aunque se ha definido una configuración de GPO en el dominio al que pertenece el servidor CIFS, no se aplica necesariamente a la unidad organizativa (OU) que contiene la máquina virtual de almacenamiento (SVM) habilitada para CIFS. La configuración de GPO aplicada es el subconjunto de todos los GPO definidos que se aplican a la SVM habilitada para CIFS. La configuración de BranchCache que se aplica a través de los GPO anula la configuración aplicada a través de la CLI.

Pasos

1. Muestre la configuración de GPO de BranchCache definida para el dominio de Active Directory mediante `vserver cifs group-policy show-defined` el comando.

   Este ejemplo no muestra todos los campos de resultado disponibles para el comando. La salida está truncada.

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]
```

2. Muestre la configuración de GPO de BranchCache aplicada al servidor CIFS mediante `vserver cifs group-policy show-applied` el comando. "

> Este ejemplo no muestra todos los campos de resultado disponibles para el comando. La salida está truncada.

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
 [...]
```

Información relacionada

- Habilitar o deshabilitar la compatibilidad con GPO en los servidores
- "definido por la política de grupo cifs de vserver"
- "exposición de políticas de grupo cifs de vserver aplicada"

Deshabilite BranchCache en los recursos compartidos SMB

Obtenga información sobre cómo deshabilitar BranchCache en los recursos compartidos SMB de ONTAP

Si no desea proporcionar servicios de almacenamiento en caché de BranchCache en ciertos recursos compartidos de SMB, pero quizás desee proporcionar servicios de almacenamiento en caché en esos recursos compartidos más tarde, puede deshabilitar BranchCache en función de su recurso compartido. Si tiene BranchCache configurado para ofrecer almacenamiento en caché en todos los recursos compartidos pero desea deshabilitar temporalmente todos los servicios de almacenamiento en caché, puede modificar la configuración de BranchCache para detener el almacenamiento en caché

automático en todos los recursos compartidos.

Si BranchCache en un recurso compartido de SMB se deshabilita después de haber habilitado por primera vez, ONTAP deja de enviar metadatos al cliente que lo solicita. Un cliente que necesita datos los recupera directamente del servidor de contenido (servidor CIFS en la máquina virtual de almacenamiento (SVM)).

Información relacionada

Obtenga información sobre cómo configurar recursos compartidos habilitados para BranchCache

Deshabilitar BranchCache en un solo recurso compartido SMB de ONTAP

Si no desea ofrecer servicios de almacenamiento en caché en determinados recursos compartidos que anteriormente ofrecían contenido en caché, puede deshabilitar BranchCache en un recurso compartido de SMB existente.

Paso

1. Introduzca el siguiente comando: `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties branchcache`

   Se elimina la propiedad compartida de BranchCache. Otras propiedades de recursos compartidos aplicadas permanecen en vigor.

Ejemplo

El siguiente comando deshabilita BranchCache en un recurso compartido de SMB existente llamado «data2»:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Detener el almacenamiento en caché automático en todos los recursos compartidos SMB de ONTAP

Si la configuración de BranchCache habilita automáticamente el almacenamiento en caché en todos los recursos compartidos SMB en cada máquina virtual de almacenamiento (SVM), puede modificar la configuración de BranchCache para detener el almacenamiento en caché automático de contenido para todos los recursos compartidos SMB.

Acerca de esta tarea

Para detener el almacenamiento en caché automático en todos los recursos compartidos SMB, debe cambiar el modo operativo de BranchCache a almacenamiento en caché por recurso compartido.

Pasos

1. Configure BranchCache para detener el almacenamiento en caché automático en todos los recursos compartidos de SMB: `vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
2. Compruebe que la configuración de BranchCache sea correcta: `vserver cifs branchcache show -vserver vserver_name`

Ejemplo

El siguiente comando cambia la configuración de BranchCache en una máquina virtual de almacenamiento (SVM, antes conocida como Vserver) vs1 para detener el almacenamiento en caché automático en todos los recursos compartidos SMB:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Deshabilite o habilite BranchCache en la SVM

Descubra qué sucede cuando deshabilita o vuelve a habilitar BranchCache en servidores SMB de ONTAP

Si anteriormente configuró BranchCache pero no desea que los clientes de la sucursal utilicen contenido almacenado en caché, puede deshabilitar el almacenamiento en caché en el servidor CIFS. Debe tener en cuenta lo que sucede al deshabilitar BranchCache.

Cuando deshabilita BranchCache, ONTAP ya no calcula los hash ni envía los metadatos al cliente solicitante. Sin embargo, no se interrumpe el acceso a los archivos. A partir de entonces, cuando los clientes habilitados para BranchCache solicitan información de metadatos sobre el contenido al que desean acceder, ONTAP responde con un error definido por Microsoft, lo que hace que el cliente envíe una segunda solicitud al

contenido real. En respuesta a la solicitud de contenido, el servidor CIFS envía el contenido real almacenado en la máquina virtual de almacenamiento (SVM).

Una vez que se deshabilita BranchCache en el servidor CIFS, los recursos compartidos de SMB no anuncian las funcionalidades de BranchCache. Para acceder a los datos de nuevas conexiones SMB, los clientes realizan solicitudes de lectura SMB normales.

Puede volver a habilitar BranchCache en el servidor CIFS en cualquier momento.

- Dado que el almacén hash no se elimina cuando deshabilita BranchCache, ONTAP puede usar los hash almacenados al responder a las solicitudes hash una vez que vuelva a habilitar BranchCache, siempre y cuando el hash solicitado siga siendo válido.
- Todos los clientes que hayan establecido conexiones SMB a recursos compartidos habilitados con BranchCache durante el momento en el que se deshabilitó BranchCache no obtienen compatibilidad con BranchCache si se vuelve a habilitar BranchCache después.

  Esto se debe a que ONTAP anuncia el soporte de BranchCache para un recurso compartido en el momento de la configuración de la sesión del SMB. Los clientes que establecieron sesiones con recursos compartidos habilitados para BranchCache mientras BranchCache estaba deshabilitado necesitan desconectar y volver a conectarse para usar el contenido en caché para este recurso compartido.

> Si no desea guardar el almacén hash después de deshabilitar BranchCache en un servidor CIFS, puede eliminarlo en forma manual. Si vuelve a habilitar BranchCache, debe asegurarse de que exista el directorio de almacén hash. Una vez que se vuelve a habilitar BranchCache, los recursos compartidos con BranchCache habilitados anuncian las funcionalidades de BranchCache. ONTAP crea nuevos hash a medida que las nuevas solicitudes las realizan los clientes habilitados para BranchCache.

Deshabilitar o habilitar BranchCache en recursos compartidos SMB de ONTAP

Es posible deshabilitar BranchCache en la máquina virtual de almacenamiento (SVM) si se cambia el modo operativo de BranchCache a `disabled`. Puede habilitar BranchCache en cualquier momento cambiando el modo operativo para ofrecer servicios de BranchCache por recurso compartido o automáticamente para todos los recursos compartidos.

Pasos

1. Ejecute el comando apropiado:

Si desea…	Introduzca lo siguiente…
Deshabilite BranchCache	`vserver cifs branchcache modify -vserver vserver_name -operating-mode disable`
Habilite BranchCache por recurso compartido	`vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`

Si desea…	Introduzca lo siguiente…
Habilite BranchCache para todos los recursos compartidos	`vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares`

2. Compruebe que el modo operativo BranchCache esté configurado con la configuración deseada: `vserver cifs branchcache show -vserver vserver_name`

Ejemplo

En el siguiente ejemplo, se deshabilita BranchCache en la SVM vs1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: disable
```

Elimine la configuración de BranchCache en las SVM

Descubra qué sucede cuando elimina la configuración de BranchCache en los recursos compartidos SMB de ONTAP

Si anteriormente configuró BranchCache, pero no desea que la máquina virtual de almacenamiento (SVM) continúe proporcionando contenido en caché, puede eliminar la configuración de BranchCache en el servidor CIFS. Debe saber lo que ocurre cuando se elimina la configuración.

Cuando se elimina la configuración, ONTAP quita la información de configuración de esa SVM del clúster y detiene el servicio BranchCache. Puede decidir si ONTAP debería eliminar el almacén hash de la SVM.

La eliminación de la configuración de BranchCache no interrumpe el acceso de los clientes habilitados para BranchCache. A partir de entonces, cuando los clientes habilitados para BranchCache solicitan información de metadatos sobre las conexiones SMB existentes para determinar el contenido que ya se ha almacenado en la caché, ONTAP responde con un error definido de Microsoft, lo que hace que el cliente envíe una segunda solicitud, solicitando el contenido real. En respuesta a la solicitud de contenido, el servidor CIFS envía el contenido real almacenado en la SVM

Una vez que se elimina la configuración de BranchCache, los recursos compartidos de SMB no anuncian las funcionalidades de BranchCache. Para acceder a contenido que no se ha almacenado previamente en la caché mediante nuevas conexiones SMB, los clientes realizan solicitudes de SMB de lectura normales.

Eliminar la configuración de BranchCache en los recursos compartidos SMB de ONTAP

El comando que se usa para eliminar el servicio BranchCache en la máquina virtual de almacenamiento (SVM) varía en función de si desea eliminar o conservar los hash existentes.

Paso

1. Ejecute el comando apropiado:

Si desea…	Introduzca lo siguiente…
Elimine la configuración de BranchCache y elimine los hash existentes	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes true`
Elimine la configuración de BranchCache, pero mantenga los hash existentes	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes false`

Ejemplo

En el siguiente ejemplo, se elimina la configuración de BranchCache en la SVM vs1 y se eliminan todos los hash existentes:

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes
true
```

Descubra qué sucede con ONTAP SMB BranchCache al revertir

Es importante comprender lo que sucede al revertir ONTAP a una versión que no admite BranchCache.

- Cuando revierte a una versión de ONTAP que no admite BranchCache, los recursos compartidos SMB no anuncian capacidades de BranchCache a los clientes habilitados para BranchCache; por lo tanto, los clientes no solicitan información hash.

  En su lugar, solicitan el contenido real mediante las solicitudes de lectura SMB normales. En respuesta a la solicitud de contenido, el servidor SMB envía el contenido real almacenado en la máquina virtual de almacenamiento (SVM).

- Cuando un nodo que aloja un almacén hash se revierte a una versión que no admite BranchCache, el administrador de almacenamiento debe revertir manualmente la configuración de BranchCache mediante un comando que se imprime durante la reversión.

  Este comando elimina la configuración y los hash de BranchCache.

  Una vez finalizada la reversión, el administrador de almacenamiento puede eliminar manualmente el directorio que contenía el almacén hash, si lo desea.

Información relacionada

Eliminar la configuración de BranchCache en los recursos compartidos

Mejorar el rendimiento de las copias remotas de Microsoft

Obtenga información sobre las mejoras de rendimiento de la copia remota de Microsoft en los servidores SMB de ONTAP

La transferencia de datos descargados (ODX) de Microsoft, también conocida como *copy fload*, permite transferir datos directamente dentro o entre dispositivos de almacenamiento compatibles sin transferir los datos a través del equipo host.

ONTAP admite ODX para los protocolos SMB Y SAN. El origen puede ser un servidor CIFS o una LUN; el destino puede ser un servidor CIFS o una LUN.

En las transferencias de archivos que no son ODX, los datos se leen del origen y se transfieren a través de la red al equipo cliente. El equipo cliente transfiere los datos a través de la red al destino. En resumen, el equipo cliente lee los datos del origen y los escribe en el destino. Con las transferencias de archivos ODX, los datos se copian directamente del origen al destino.

Dado que las copias descargados de ODX se realizan directamente entre el almacenamiento de origen y destino, se obtienen importantes ventajas en el rendimiento. Las ventajas en cuanto a rendimiento incluyen unos tiempos de copia más rápidos entre el origen y el destino, una menor utilización de recursos (CPU, memoria) en el cliente y una menor utilización de ancho de banda de I/o de la red.

En los entornos SMB, esta funcionalidad solo está disponible cuando el cliente y el servidor de almacenamiento admiten SMB 3.0 y la función ODX. En entornos SAN, esta funcionalidad solo está disponible cuando el cliente y el servidor de almacenamiento admiten la función ODX. Los equipos cliente compatibles con ODX y que tengan habilitada ODX automáticamente y de forma transparente utilizan la transferencia de archivos descargados cuando se mueven o copian archivos. ODX se utiliza independientemente de si arrastra y suelta archivos a través del Explorador de Windows, o si utiliza comandos de copia de archivos de la línea de comandos, o si una aplicación cliente inicia solicitudes de copia de archivos.

Información relacionada

- Aprenda a mejorar el tiempo de respuesta del cliente al proporcionar referencias automáticas de nodos con Ubicación automática
- "Configuración de SMB para Microsoft Hyper-V y SQL Server"

Obtenga más información sobre ODX en los servidores SMB de ONTAP

La descarga de copias ODX utiliza un mecanismo basado en tokens para leer y escribir datos dentro o entre servidores CIFS habilitados para ODX. En lugar de enrutar los datos a través del host, el servidor CIFS envía al cliente un pequeño token que representa los datos. El cliente ODX presenta ese token al servidor de destino, que posteriormente puede transferir los datos que representa ese token del origen al destino.

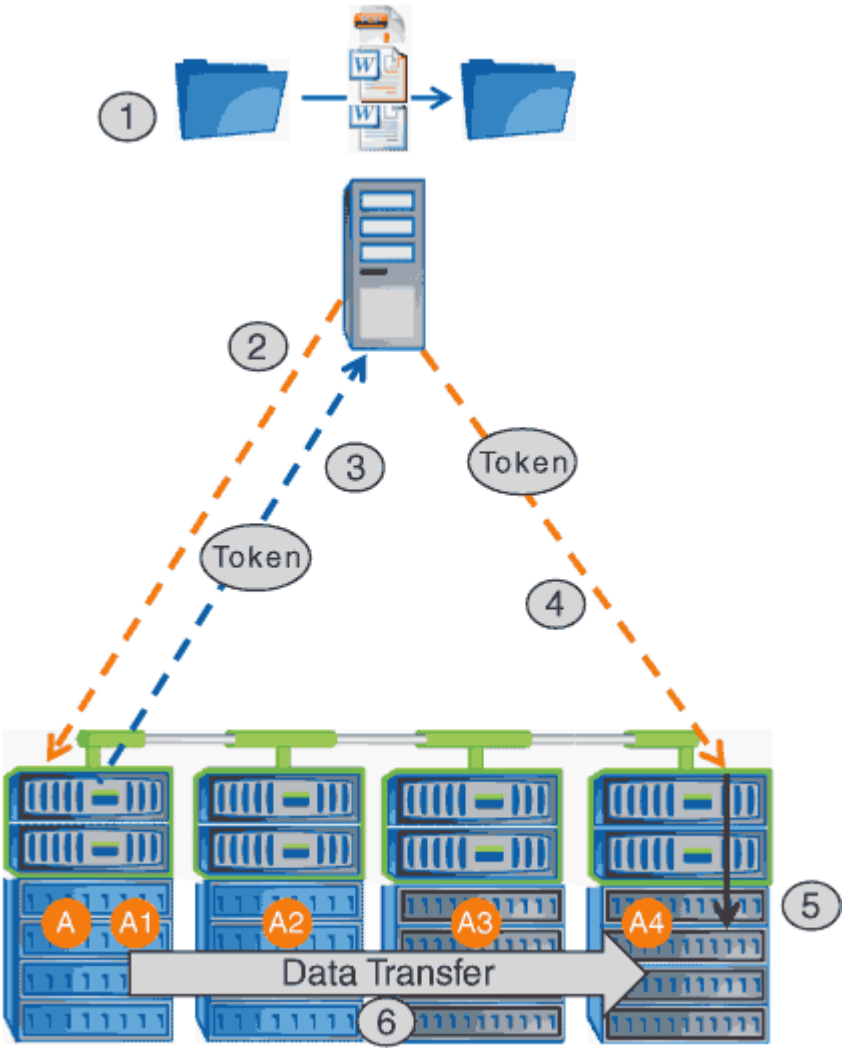
Cuando un cliente ODX descubre que el servidor CIFS es compatible con ODX, abre el archivo de origen y solicita un token del servidor CIFS. Después de abrir el archivo de destino, el cliente utiliza el token para indicar al servidor que copie los datos directamente del origen al destino.

El origen y el destino pueden estar en la misma máquina virtual de almacenamiento (SVM) o en distintas SVM, según el alcance de la operación de copia.

El token sirve como representación puntual de los datos. Por ejemplo, cuando copia datos entre ubicaciones de almacenamiento, se devuelve un token que representa un segmento de datos al cliente solicitante, que el cliente copia en el destino; de este modo, se elimina la necesidad de copiar los datos subyacentes a través del cliente.

ONTAP admite tokens que representan 8 MB de datos. Las copias ODX de más de 8 MB se realizan utilizando varios tokens, con cada token que representa 8 MB de datos.

En la siguiente figura, se explican los pasos involucrados en una operación de copia de ODX:



1. Un usuario copia o mueve un archivo mediante el Explorador de Windows, una interfaz de línea de comandos o como parte de la migración de un equipo virtual, o bien una aplicación inicia copias o traslados de archivos.
2. El cliente compatible con ODX convierte automáticamente esta solicitud de transferencia a una solicitud ODX.

   La solicitud ODX que se envía al servidor CIFS contiene una solicitud de token.
3. Si se habilita ODX en el servidor CIFS y la conexión a través de SMB 3.0, el servidor CIFS genera un token, que es una representación lógica de los datos en el origen.
4. El cliente recibe un token que representa los datos y se envía con la solicitud de escritura al servidor CIFS de destino.

Se trata de los únicos datos que se copian a través de la red desde el origen al cliente y, después, desde el cliente al destino.

5. El token se entrega al subsistema de almacenamiento.
6. La SVM realiza de forma interna la copia o el movimiento.

   Si el archivo que se copia o se mueve es de más de 8 MB, se necesitan varios tokens para realizar la copia. Pasos 2 a 6 según se requiera para completar la copia.

> Si se produce un error con la copia descargada de ODX, la operación de copia o movimiento se vuelve a leer y escribir tradicionales para la operación de copia o movimiento. Del mismo modo, si el servidor CIFS de destino no admite ODX ni ODX está deshabilitado, la operación de copia o movimiento se remonta a las lecturas y escrituras tradicionales para la operación de copia o movimiento.

Requisitos para usar ODX en servidores SMB de ONTAP

Antes de poder usar ODX para llevar a cabo descargas de copias con la máquina virtual de almacenamiento (SVM), debe conocer ciertos requisitos.

Requisitos de versión de ONTAP

ONTAP libera compatibilidad con ODX para realizar descargas de copias.

Requisitos de versión de SMB

- ONTAP es compatible con ODX mediante SMB 3.0 y versiones posteriores.
- Para poder habilitar ODX, es necesario habilitar SMB 3.0 en el servidor CIFS:
  - Si la función ODX no está habilitada, también habilita SMB 3.0.
  - Al deshabilitar SMB 3.0, también se deshabilita ODX.

Requisitos del servidor y del cliente de Windows

Antes de poder usar ODX para realizar descargas de copias, el cliente de Windows debe admitir la función.

El "Matriz de interoperabilidad de NetApp"contiene la información más reciente sobre los clientes de Windows compatibles.

Requisitos del volumen

- Los volúmenes de origen deben tener un mínimo de 1.25 GB.
- Si utiliza volúmenes comprimidos, el tipo de compresión debe ser adaptable y solo se admite el tamaño de grupo de compresión 8K.

  No se admite el tipo de compresión secundaria.

Pautas para el uso de ODX en servidores SMB de ONTAP

Antes de poder utilizar ODX para descarga de copias, debe conocer las directrices. Por ejemplo, debe saber en qué tipos de volúmenes se puede utilizar ODX y debe

comprender las consideraciones dentro del clúster y entre clústeres de ODX.

Directrices de volumen

- No se puede usar ODX para descargar la copia con las siguientes configuraciones de volumen:
  - El tamaño del volumen de origen es inferior a 1.25 GB

    El tamaño del volumen debe ser 1.25 GB o más para usar la función ODX.

  - Volúmenes de solo lectura

    ODX no se utiliza para archivos y carpetas que residen en reflejos de carga compartida o en volúmenes de destino de SnapMirror o SnapVault.

  - Si el volumen de origen no está deduplicado
- Las copias ODX solo son compatibles con las copias dentro del clúster.

  No se puede usar ODX para copiar archivos o carpetas en un volumen de otro clúster.

Otras directrices

- En los entornos SMB, para utilizar ODX para la descarga de copias, los archivos deben ser de 256 kb o más.

  Los archivos más pequeños se transfieren mediante una operación de copia tradicional.

- La descarga de copias ODX utiliza la deduplicación como parte del proceso de copia.

  Si no desea que la deduplicación se produzca en los volúmenes de SVM al copiar o mover datos, debe deshabilitar la descarga de la copia ODX en esa SVM.

- La aplicación que realiza la transferencia de datos debe escribirse para admitir ODX.

  Las operaciones de aplicaciones compatibles con ODX incluyen lo siguiente:

  - Las operaciones de gestión de Hyper-V, como la creación y conversión de discos duros virtuales (VHD), la gestión de snapshots y la copia de archivos entre máquinas virtuales
  - Operaciones del Explorador de Windows
  - Comandos de copia de Windows PowerShell
  - Comandos de copia en el símbolo del sistema de Windows

    Robocopy en el símbolo del sistema de Windows admite ODX.

    Las aplicaciones deben ejecutarse en servidores Windows o clientes que admitan ODX.

  +
  Para obtener más información acerca de las aplicaciones ODX admitidas en servidores y clientes Windows, consulte la biblioteca de Microsoft TechNet.

Información relacionada

"Biblioteca de Microsoft TechNet: technet.microsoft.com/en-us/library/"

Casos de uso de ODX en servidores SMB de ONTAP

Debe conocer los casos de uso de ODX en SVM para poder determinar en qué circunstancias le proporciona ventajas en rendimiento.

Los servidores y los clientes de Windows que admiten ODX utilizan la descarga de copias como forma predeterminada de copiar datos en servidores remotos. Si el cliente o el servidor Windows no son compatibles con ODX o se produce un error en cualquier momento, la operación de copia o movimiento vuelve a las lecturas y escrituras tradicionales para la operación de copia o movimiento.

Los siguientes casos de uso admiten el uso de copias y movimientos ODX:

- Volumen interno

  Los archivos o LUN de origen y destino están dentro del mismo volumen.

- Entre volúmenes, mismo nodo, misma SVM

  Los archivos de origen y de destino o las LUN se encuentran en distintos volúmenes ubicados en el mismo nodo. Los datos son propiedad de la misma SVM.

- Entre volúmenes, distintos nodos, misma SVM

  Los archivos de origen y de destino o las LUN se encuentran en volúmenes distintos que se encuentran en nodos diferentes. Los datos son propiedad de la misma SVM.

- Entre SVM, mismo nodo

  El archivo de origen y los LUN de destino se encuentran en distintos volúmenes ubicados en el mismo nodo. Los datos son propiedad de diferentes SVM.

- Entre SVM, diferentes nodos

  El archivo o las LUN de origen y destino se encuentran en distintos volúmenes ubicados en nodos diferentes. Los datos son propiedad de diferentes SVM.

- Entre clústeres

  Las LUN de origen y de destino se encuentran en distintos volúmenes ubicados en distintos nodos en varios clústeres. Solo se admite en SAN y no funciona para CIFS.

Existen algunos casos de uso especiales adicionales:

- Con la implementación de ODX de ONTAP, se puede utilizar ODX para copiar archivos entre recursos compartidos de SMB y unidades virtuales asociadas a FC o iSCSI.

  Puede utilizar el Explorador de Windows, la CLI de Windows o PowerShell, Hyper-V u otras aplicaciones que admiten ODX para copiar o mover archivos sin problemas mediante la descarga de la copia ODX entre recursos compartidos de SMB y LUN conectados, siempre y cuando los recursos compartidos y las LUN del SMB estén en el mismo clúster.

- Hyper-V proporciona algunos casos de uso adicionales para la descarga de copias ODX:

  - Se puede utilizar la transferencia de la copia ODX mediante Hyper-V para copiar datos dentro o a través de archivos de disco duro virtual (VHD), o bien copiar datos entre recursos compartidos de SMB

asignados y LUN iSCSI conectados dentro del mismo clúster.

Esto permite que las copias de sistemas operativos invitados pasen al almacenamiento subyacente.

- Al crear discos duros virtuales de tamaño fijo, ODX se utiliza para inicializar el disco con ceros, empleando un token de cero conocido.
- La descarga de copias ODX se utiliza para la migración de almacenamiento de máquinas virtuales si el almacenamiento de origen y destino está en el mismo clúster.

> Para aprovechar los casos de uso de un paso a través de la descarga de copias ODX mediante Hyper-V, el sistema operativo invitado debe ser compatible con ODX, mientras que los discos del sistema operativo invitado deben ser discos SCSI respaldados por almacenamiento (tanto SMB COMO SAN) que sean compatibles con ODX. Los discos IDE del sistema operativo invitado no admiten el paso a través de ODX.

Habilitar o deshabilitar ODX en servidores SMB de ONTAP

Es posible habilitar o deshabilitar ODX en máquinas virtuales de almacenamiento (SVM). El valor predeterminado es habilitar la compatibilidad con la descarga de copias ODX si también se habilita SMB 3.0.

Antes de empezar

Se debe habilitar SMB 3.0.

Acerca de esta tarea

Si deshabilita SMB 3.0, ONTAP también deshabilita SMB ODX. Si vuelve a habilitar SMB 3.0, debe volver a habilitar manualmente SMB ODX.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

Si desea que la descarga de copias de ODX sea…	Introduzca el comando…
Activado	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled true`
Deshabilitado	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled false`

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

Ejemplo

En el ejemplo siguiente se habilita la descarga de copias ODX en SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster1::*> set -privilege admin
```

Información relacionada

Opciones de servidor disponibles

Mejore el tiempo de respuesta del cliente al proporcionar referencias automáticas a nodos SMB con ubicación automática

Aprenda a mejorar el tiempo de respuesta del cliente al proporcionar referencias automáticas de nodos SMB de ONTAP con ubicación automática

Auto Location utiliza referencias de nodos automáticas de SMB para aumentar el rendimiento del cliente de SMB en máquinas virtuales de almacenamiento (SVM). Las referencias automáticas a nodos redirigen automáticamente el cliente solicitante a una LIF en la SVM de nodos que aloja el volumen en el que residen los datos, lo que puede mejorar los tiempos de respuesta del cliente.

Cuando un cliente SMB se conecta a un recurso compartido SMB alojado en la SVM, puede conectarse mediante una LIF que está en un nodo que no posee los datos solicitados. El nodo al que está conectado el cliente accede a los datos que pertenece a otro nodo mediante el uso de la red de clústeres. El cliente puede experimentar tiempos de respuesta más rápidos si la conexión SMB utiliza una LIF ubicada en el nodo que contiene los datos solicitados:

- ONTAP proporciona esta funcionalidad al utilizar referencias DFS de Microsoft para informar a los clientes SMB de que un archivo o carpeta solicitados en el espacio de nombres está alojado en otro lugar.

  Un nodo hace una referencia cuando determina que hay una LIF ANSVM en el nodo que contiene los datos.

- Las referencias automáticas de nodos son compatibles con las direcciones IP de LIF IPv4 e IPv6.
- Las referencias se realizan en función de la ubicación de la raíz del recurso compartido a través del cual está conectado el cliente.
- La referencia se produce durante la negociación SMB.

  La referencia se realiza antes de establecer la conexión. Una vez que ONTAP hace referencia al cliente SMB al nodo de destino, se establece la conexión y el cliente accede a los datos a través de la ruta LIF referida desde ese punto de encendido. Esto permite a los clientes acceder con más rapidez a los datos y evita la comunicación adicional del clúster.

Si un recurso compartido abarca varios puntos de unión y algunas uniones están en volúmenes contenidos en otros nodos, los datos del recurso compartido se distribuyen entre varios nodos. Dado que ONTAP proporciona las referencias que son locales a la raíz del recurso compartido, ONTAP debe usar la red de clúster para recuperar los datos contenidos en estos volúmenes no locales. Con este tipo de arquitectura de espacio de nombres, es posible que las referencias automáticas a nodos no ofrezcan importantes beneficios en el rendimiento.

Si el nodo que aloja los datos no tiene una LIF disponible, ONTAP establecerá la conexión mediante la LIF elegida por el cliente. Después de que un cliente SMB abre un archivo, éste continúa accediendo al archivo a través de la misma conexión referida.

Si, por algún motivo, el servidor CIFS no puede hacer una referencia, no se produce ninguna interrupción del servicio SMB. La conexión SMB se establece como si las referencias automáticas a nodos no estuvieran habilitadas.

Información relacionada

Mejora del rendimiento de las copias remotas de Microsoft

Requisitos y pautas para el uso de referencias automáticas de nodos en servidores SMB de ONTAP

Antes de poder utilizar las referencias automáticas de nodos SMB, también conocido como *autoubicación*, debe tener en cuenta ciertos requisitos, como las versiones de ONTAP que admiten esta función. También debe saber acerca de las versiones del protocolo SMB compatibles y otras directrices especiales.

Requisitos de versión y licencia de ONTAP

- Todos los nodos del clúster deben ejecutar una versión de ONTAP que admita las referencias automáticas al nodo.
- Los widgets deben estar habilitados en un recurso compartido SMB para utilizar la autolocalización.
- CIFS debe tener una licencia y el servidor SMB debe existir en las SVM. La licencia SMB se incluye con "ONTAP One". Si no tiene ONTAP One y la licencia no está instalada, póngase en contacto con su representante de ventas.

Requisitos de la versión del protocolo SMB

- Para SVM, ONTAP admite referencias de nodos automáticas en todas las versiones de SMB.

Requisitos del cliente SMB

Todos los clientes de Microsoft compatibles con ONTAP son compatibles con las referencias de nodo automáticas SMB.

La matriz de interoperabilidad contiene la información más reciente sobre los clientes Windows que admite ONTAP.

"Herramienta de matriz de interoperabilidad de NetApp"

Requisitos de LIF de datos

Si desea utilizar una LIF de datos como referencia potencial para los clientes de SMB, debe crear LIF de datos con NFS y CIFS habilitados.

Las referencias automáticas de nodos pueden fallar si el nodo de destino contiene LIF de datos que están habilitadas solo para el protocolo NFS o solo para el protocolo SMB.

Si no se cumple este requisito, el acceso a los datos no se verá afectado. El cliente de SMB asigna el recurso compartido mediante la LIF original que utilizó el cliente para conectarse a la SVM.

Requisitos de autenticación NTLM al realizar una conexión SMB a la que se hace referencia

Se debe permitir la autenticación NTLM en el dominio que contiene el servidor CIFS y en los dominios que contienen clientes que desean utilizar referencias automáticas a nodos.

Al realizar una referencia, el servidor SMB hace referencia a una dirección IP al cliente Windows. Dado que la autenticación NTLM se utiliza al realizar una conexión mediante una dirección IP, la autenticación Kerberos no se realiza para conexiones a las que se hace referencia.

Esto sucede porque el cliente Windows no puede crear el nombre principal de servicio utilizado por Kerberos (que es del formato `service/NetBIOS name` AND `service/FQDN`), lo que significa que el cliente no puede solicitar un ticket de Kerberos al servicio.

Instrucciones para el uso de referencias automáticas de nodos con la función de directorio inicial

Cuando los recursos compartidos se configuran con la propiedad del recurso compartido del directorio principal activada, puede haber una o varias rutas de búsqueda del directorio principal configuradas para una configuración de directorio principal. Las rutas de búsqueda pueden apuntar a los volúmenes contenidos en cada nodo que contiene volúmenes de SVM. Los clientes reciben una referencia y, si hay una LIF de datos local activa disponible, se conectan a través de una LIF de referencia que sea local al directorio raíz del usuario doméstico.

Existen directrices para que los clientes de SMB 1.0 accedan a directorios iniciales dinámicos con referencias de nodos automáticas habilitadas. Esto se debe a que los clientes de SMB 1.0 necesitan la referencia automática al nodo antes de que se hayan autenticado, lo que es antes de que el servidor SMB tenga el nombre del usuario. Sin embargo, el acceso al directorio raíz SMB funciona correctamente para los clientes SMB 1.0 si se cumplen las siguientes afirmaciones:

- Los directorios iniciales de SMB están configurados para usar nombres simples, como "'%w'" (nombre de usuario de Windows) o "'%u'" (nombre de usuario UNIX asignado), y no nombres de estilo de nombre de dominio, como "'%d\%w '" (nombre de dominio\nombre de usuario).
- Al crear recursos compartidos de directorios iniciales, los nombres de los recursos compartidos de directorios iniciales CIFS se configuran con variables ("'%w'" o "'%u'"), y no con nombres estáticos, como «'HOME».

Para los clientes SMB 2.x y SMB 3.0, no hay directrices especiales al acceder a directorios iniciales con referencias automáticas a nodos.

Directrices para deshabilitar las referencias automáticas de nodos en servidores CIFS con conexiones existentes referidas

Si deshabilita las referencias automáticas a nodos después de habilitar la opción, los clientes que están actualmente conectados a una LIF conocida mantienen la conexión referida. Dado que ONTAP utiliza referencias DFS como mecanismo para las referencias automáticas de nodo SMB, los clientes pueden incluso

volver a conectarse a la LIF mencionada después de deshabilitar la opción hasta que se agote el tiempo de espera de la referencia de DFS en caché del cliente para la conexión mencionada. Esto es cierto incluso si se revierte a una versión de ONTAP que no admite referencias automáticas a los nodos. Los clientes continúan utilizando referencias hasta que se agote el tiempo de espera de la referencia DFS desde la memoria caché del cliente.

La ubicación automática utiliza las referencias de nodos automáticos de SMB para aumentar el rendimiento del cliente de SMB al remitir a los clientes a la LIF en el nodo propietario del volumen de datos de una SVM. Cuando un cliente SMB se conecta a un recurso compartido SMB alojado en una SVM, puede conectarse mediante una LIF en un nodo que no posea los datos solicitados y utilice una red de interconexión de clúster para recuperar los datos. El cliente puede experimentar tiempos de respuesta más rápidos si la conexión SMB utiliza una LIF ubicada en el nodo que contiene los datos solicitados.

ONTAP proporciona esta funcionalidad al utilizar referencias del sistema de archivos distribuidos (DFS) de Microsoft para informar a los clientes SMB de que un archivo o una carpeta solicitados en el espacio de nombres se alojan en otro lugar. Un nodo hace una referencia cuando determina que hay una LIF de SVM en el nodo que contiene los datos. Las referencias se realizan en función de la ubicación de la raíz del recurso compartido a través del cual está conectado el cliente.

La referencia se produce durante la negociación SMB. La referencia se realiza antes de establecer la conexión. Una vez que ONTAP hace referencia al cliente SMB al nodo de destino, se establece la conexión y el cliente accede a los datos a través de la ruta LIF referida desde ese punto de encendido. Esto permite a los clientes acceder con más rapidez a los datos y evita la comunicación adicional del clúster.

Instrucciones para el uso de referencias automáticas a nodos con clientes Mac OS

Los clientes de Mac OS X no admiten referencias automáticas de nodos SMB, aunque Mac OS sea compatible con Microsoft Distributed File System (DFS). Los clientes de Windows realizan una solicitud de referencia DFS antes de conectarse a un recurso compartido SMB. ONTAP proporciona una referencia a una LIF de datos que se encuentra en el mismo nodo que aloja los datos solicitados, lo cual mejora los tiempos de respuesta de los clientes. Aunque Mac OS admite DFS, los clientes de Mac OS no se comportan exactamente igual que los clientes de Windows en esta área.

Información relacionada

- Obtenga información sobre cómo habilitar directorios de inicio dinámicos en servidores
- "Gestión de redes"
- "Herramienta de matriz de interoperabilidad de NetApp"

Compatibilidad con referencias automáticas de nodos SMB de ONTAP

Antes de habilitar las referencias automáticas al nodo SMB, tiene que tener en cuenta que ciertas funcionalidades de ONTAP no admiten referencias.

- Los siguientes tipos de volúmenes no son compatibles con las referencias de nodo automáticas del bloque de mensajes del servidor:
  - Miembros de solo lectura de un reflejo de carga compartida
  - Volumen de destino de un reflejo de protección de datos
- Las referencias de nodos no se mueven junto a un movimiento LIF.

  Si un cliente utiliza una conexión a la que se hace referencia a través de una conexión SMB 2.x o SMB 3.0 y una LIF de datos se mueve de forma no disruptiva, el cliente sigue usando la misma conexión a la que se hace referencia, aunque la LIF ya no sea local para los datos.

- Las referencias de los nodos no se mueven junto a un movimiento de volumen.

  Si un cliente está usando una conexión a través de cualquier conexión SMB y se produce un movimiento de volúmenes, el cliente sigue utilizando la misma conexión conocida, aunque el volumen ya no esté ubicado en el mismo nodo que la LIF de datos.

Habilitar o deshabilitar las referencias automáticas de nodos de ONTAP SMB

Puede habilitar las referencias de nodo automáticas para SMB para aumentar el rendimiento del acceso de los clientes SMB. Puede deshabilitar las referencias de nodo automáticas si no desea que ONTAP haga referencias a los clientes SMB.

Antes de empezar

Debe configurarse y ejecutarse un servidor CIFS en la máquina virtual de almacenamiento (SVM).

Acerca de esta tarea

La funcionalidad de referencias automáticas al nodo SMB está deshabilitada de manera predeterminada. Puede habilitar o deshabilitar esta funcionalidad en cada SVM, según sea necesario.

Esta opción está disponible en el nivel de privilegio avanzado.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Habilite o deshabilite las referencias de nodo automáticas para SMB según sea necesario:

Si desea que las referencias automáticas de nodo de SMB sean…	Introduzca el siguiente comando…
Activado	`vserver cifs options modify -vserver vserver_name -is-referral-enabled true`
Deshabilitado	`vserver cifs options modify -vserver vserver_name -is-referral-enabled false`

   La configuración de la opción surte efecto para nuevas sesiones SMB. Los clientes con conexión existente pueden utilizar la referencia de nodo sólo cuando caduque el tiempo de espera de caché existente.

3. Cambie al nivel de privilegio de administrador: `set -privilege admin`

Información relacionada

Opciones de servidor disponibles

Utilice estadísticas para supervisar la actividad de referencia automática de nodos de ONTAP SMB

Para determinar cuántas conexiones SMB se hace referencia, puede supervisar la actividad de referencia automática de nodos mediante `statistics` el comando. Al supervisar las referencias puede determinar en qué medida las referencias automáticas están ubicando conexiones en los nodos que alojan los recursos compartidos y si debe

redistribuir sus LIF de datos para proporcionar un mejor acceso local a los recursos compartidos en el servidor CIFS.

Acerca de esta tarea

`cifs`El objeto proporciona varios contadores en el nivel de privilegio avanzado que son útiles al supervisar referencias automáticas de nodos SMB:

- `node_referral_issued`

  Número de clientes a los que se ha emitido una referencia al nodo de la raíz compartida después de que el cliente se haya conectado mediante una LIF alojada por un nodo diferente al nodo de la raíz compartida.

- `node_referral_local`

  Número de clientes que se conectan mediante una LIF alojada por el mismo nodo que aloja la raíz compartida. El acceso local generalmente proporciona un rendimiento óptimo.

- `node_referral_not_possible`

  Número de clientes que no se han emitido una referencia al nodo que aloja el recurso compartido raíz tras la conexión mediante una LIF alojada por un nodo diferente al nodo raíz del recurso compartido. Esto se debe a que no se encontró una LIF de datos activa para el nodo raíz del recurso compartido.

- `node_referral_remote`

  Número de clientes que se conectan mediante una LIF alojada por un nodo diferente al nodo que aloja la raíz compartida. El acceso remoto puede provocar una degradación del rendimiento.

Es posible supervisar las estadísticas de referencia automática de nodos en la máquina virtual de almacenamiento (SVM) mediante la recopilación y la visualización de datos de un período de tiempo específico (una muestra). Puede ver los datos de la muestra si no detiene la recopilación de datos. Al detener la recopilación de datos, se proporciona una muestra fija. No detener la recopilación de datos le ofrece la posibilidad de obtener datos actualizados que puede utilizar para compararlos con consultas anteriores. La comparativa puede ayudarle a identificar las tendencias de rendimiento.

Para evaluar y utilizar la información que recopila del `statistics` comando, debe comprender la distribución de los clientes en sus entornos.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Para ver estadísticas automáticas de referencia de nodo `statistics`, utilice el comando.

   En este ejemplo, se visualizan y recogen estadísticas de referencia automática de nodos:

   a. Inicie la colección: `statistics start -object cifs -instance vs1 -sample-id sample1`

```
Statistics collection is being started for Sample-id: sample1
```

b. Espere a que transcurra el tiempo de recogida deseado.

c. Detener la colección: `statistics stop -sample-id sample1`

```
Statistics collection is being stopped for Sample-id: sample1
```

Obtenga más información sobre `statistics start` y `statistics stop` en el "Referencia de comandos del ONTAP" .

d. Vea las estadísticas automáticas de referencia de nodo: `statistics show -sample-id sample1 -counter` **`node`**

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1

    Counter                                     Value
    --------------------------- ----------------------------
    node_name                                   node1
    node_referral_issued                            0
    node_referral_local                             1
    node_referral_not_possible                      2
    node_referral_remote                            2
    ...

    node_name                                   node2
    node_referral_issued                            2
    node_referral_local                             1
    node_referral_not_possible                      0
    node_referral_remote                            2
    ...
```

La salida muestra los contadores de todos los nodos que participan en SVM vs1. Para mayor claridad, en el ejemplo solo se proporcionan los campos de salida relacionados con las estadísticas automáticas de referencia de nodos.

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

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

Información relacionada

- Mostrar estadísticas
- "Configuración de supervisión del rendimiento"

Supervisar la información de referencia automática de nodos de ONTAP SMB del lado del cliente mediante un cliente de Windows

Para determinar qué referencias se hacen desde la perspectiva del cliente, puede usar la `dfsutil.exe` utilidad de Windows.

El kit de herramientas de administración remota del servidor (RSAT) disponible con clientes de Windows 7 y posteriores contiene la `dfsutil.exe` utilidad. Con esta utilidad, puede mostrar información acerca del contenido de la caché de referencias así como ver información acerca de cada referencia que esté utilizando actualmente el cliente. También puede utilizar la utilidad para borrar la memoria caché de referencia del cliente. Para obtener más información, consulte la biblioteca de Microsoft TechNet.

Información relacionada

"Biblioteca de Microsoft TechNet: technet.microsoft.com/en-us/library/"

Proporcione seguridad de carpetas en recursos compartidos con enumeración basada en acceso

Proporcionar seguridad de carpetas SMB de ONTAP en recursos compartidos con enumeración basada en acceso

Cuando se habilita la enumeración basada en acceso (ABE) en un recurso compartido SMB, los usuarios que no tienen permiso para acceder a una carpeta o archivo contenido en el recurso compartido (ya sea mediante restricciones de permisos individuales o de grupo) no ven el recurso compartido que se muestra en su entorno, aunque el recurso compartido en sí sigue siendo visible.

Las propiedades de uso compartido convencionales permiten especificar qué usuarios (individualmente o en grupos) tienen permiso para ver o modificar archivos o carpetas contenidos en el recurso compartido. Sin embargo, no le permiten controlar si las carpetas o archivos dentro del recurso compartido son visibles para los usuarios que no tienen permiso para tener acceso a ellos. Esto podría plantear problemas si los nombres de estas carpetas o archivos del recurso compartido describen información confidencial, como los nombres de los clientes o los productos en desarrollo.

La enumeración basada en acceso (ABE) amplía las propiedades de recursos compartidos para incluir la enumeración de archivos y carpetas dentro del recurso compartido. POR tanto, ABE permite filtrar la visualización de archivos y carpetas dentro del recurso compartido en función de los derechos de acceso del usuario. Es decir, el recurso compartido en sí sería visible para todos los usuarios, pero los archivos y carpetas dentro del recurso compartido podrían mostrarse u ocultarse de los usuarios designados. Además de proteger la información confidencial en su lugar de trabajo, ABE le permite simplificar la presentación de grandes estructuras de directorio en beneficio de los usuarios que no necesitan acceso a su gama completa de contenido. Por ejemplo, el recurso compartido en sí sería visible para todos los usuarios, pero los archivos y carpetas dentro del recurso compartido podrían mostrarse u ocultarse.

Obtenga más información "Impacto sobre el rendimiento al utilizar la enumeración basada en SMB/CIFS Access"sobre .

Habilitar o deshabilitar la enumeración basada en acceso en recursos compartidos SMB de ONTAP

Puede habilitar o deshabilitar la enumeración basada en acceso (ABE) en recursos compartidos SMB para permitir o impedir que los usuarios vean recursos compartidos a los que no tienen permiso para acceder.

Acerca de esta tarea

De forma predeterminada, ABE está desactivado.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el comando…
Habilite ABE en un nuevo recurso compartido	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration` Puede especificar configuraciones de recursos compartidos opcionales y propiedades de recursos compartidos adicionales al crear un recurso compartido de SMB. Obtenga más información sobre `vserver cifs share create` en el "Referencia de comandos del ONTAP".
Habilite ABE en un recurso compartido existente	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` Se conservan las propiedades de recurso compartido existentes. La propiedad ABE share se agrega a la lista existente de propiedades compartidas.
Deshabilite ABE en un recurso compartido existente	`vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` Se conservan otras propiedades de recurso compartido. Sólo la propiedad compartida ABE se elimina de la lista de propiedades de recursos compartidos.

2. Compruebe que la configuración del recurso compartido sea correcta mediante `vserver cifs share show` el comando.

Ejemplos

El siguiente ejemplo crea un recurso compartido SMB de ABE llamado “ventas” con una ruta de `/sales` en SVM VS1. El recurso compartido se crea con `access-based-enumeration` como propiedad de recurso compartido:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales  -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

                      Vserver: vs1
                        Share: sales
     CIFS Server NetBIOS Name: VS1
                         Path: /sales
             Share Properties: access-based-enumeration
                               oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

El siguiente ejemplo agrega la `access-based-enumeration` propiedad de recurso compartido a un recurso compartido SMB llamado «ATA2»:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
------- ---------- ------------------------------------------------------
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration
```

Información relacionada

Agregar o eliminar propiedades de recursos compartidos en recursos compartidos existentes

Habilitar o deshabilitar la enumeración basada en acceso desde un cliente de Windows en recursos compartidos SMB de ONTAP

Puede habilitar o deshabilitar la enumeración basada en acceso (ABE) en recursos compartidos SMB desde un cliente Windows, que permite configurar esta configuración de recurso compartido sin tener que conectarse al servidor CIFS.

`abecmd`La utilidad no está disponible en nuevas versiones de Windows Server y clientes Windows. Se lanzó como parte de Windows Server 2008. El soporte finalizó para Windows Server 2008 el 14 de enero de 2020.

Pasos

1. Desde un cliente Windows compatible con ABE, introduzca el siguiente comando: `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

   Para obtener más información acerca `abecmd` del comando, consulte la documentación del cliente de Windows.

Dependencias de nomenclatura de archivos y directorios NFS y SMB

Obtenga información sobre las dependencias de nombres de archivos y directorios de ONTAP NFS y SMB

Las convenciones de nomenclatura de archivos y directorios dependen tanto de los sistemas operativos de los clientes de red como de los protocolos de uso compartido de archivos, además de la configuración de idioma del clúster ONTAP y de los clientes.

El sistema operativo y los protocolos de uso compartido de archivos determinan lo siguiente:

- Caracteres que puede utilizar un nombre de archivo
- Distinción entre mayúsculas y minúsculas de un nombre de archivo

ONTAP admite caracteres de varios bytes en nombres de archivos, directorios y qtrees, según la versión de ONTAP.

Obtenga información sobre los caracteres válidos para los nombres de archivos o directorios SMB de ONTAP

Si accede a un archivo o directorio desde clientes con sistemas operativos diferentes, debe utilizar caracteres válidos en ambos sistemas operativos.

Por ejemplo, si utiliza UNIX para crear un archivo o directorio, no utilice dos puntos (:) en el nombre porque no se permiten dos puntos en los nombres de archivos o directorios de MS-dos. Debido a que las restricciones de caracteres válidos varían de un sistema operativo a otro, consulte la documentación del sistema operativo cliente para obtener más información acerca de los caracteres prohibidos.

Distinción entre mayúsculas y minúsculas en los nombres de archivos y directorios SMB de ONTAP en un entorno multiprotocolo

Los nombres de archivo y directorio distinguen mayúsculas y minúsculas para los clientes NFS y no distinguen entre mayúsculas y minúsculas, pero sí lo hacen para los clientes SMB. Debe comprender las implicaciones que tiene en un entorno multiprotocolo y las acciones que podría tener que tomar al especificar la ruta al crear recursos compartidos de SMB y al acceder a datos dentro de los recursos compartidos.

Si un cliente SMB crea un directorio denominado `testdir`, los clientes SMB y NFS muestran el nombre del archivo como `testdir`. Sin embargo, si un usuario SMB intenta crear un nombre de directorio más adelante `TESTDIR` , el nombre no está permitido porque, para el cliente SMB, ese nombre existe actualmente. Si un usuario NFS crea posteriormente un directorio denominado `TESTDIR`, los clientes NFS y SMB muestran el nombre del directorio de forma diferente, de la siguiente manera:

- En los clientes NFS, puede ver los nombres de directorio a medida que se crearon, por ejemplo `testdir` y `TESTDIR`, porque los nombres de directorio distinguen entre mayúsculas y minúsculas.
- Los clientes SMB utilizan los nombres 8.3 para distinguir entre los dos directorios. Un directorio tiene el nombre del archivo base. A directorios adicionales se les asigna un nombre de archivo 8.3.
  - En clientes SMB, puede ver `testdir` y `TESTDI~1`.
  - ONTAP crea el `TESTDI~1` nombre del directorio para diferenciar los dos directorios.

    En este caso, debe usar el nombre 8.3 al especificar una ruta de recurso compartido mientras crea o modifica un recurso compartido en una máquina virtual de almacenamiento (SVM).

Del mismo modo para los archivos, si un cliente SMB lo crea `test.txt`, los clientes SMB y NFS muestran el nombre del archivo como `text.txt`. Sin embargo, si un usuario SMB intenta crear `Test.txt`, el nombre no está permitido porque, para el cliente SMB, ese nombre existe actualmente. Si un usuario NFS crea posteriormente un archivo denominado `Test.txt`, los clientes NFS y SMB muestran el nombre del archivo de forma diferente, de la siguiente manera:

- En los clientes NFS, verá los nombres de archivo a medida que se crearon y `test.txt` `Test.txt` , porque los nombres de archivo distinguen entre mayúsculas y minúsculas.
- Los clientes SMB utilizan los nombres 8.3 para distinguir entre los dos archivos. Un archivo tiene el nombre del archivo base. Se asigna un nombre de archivo 8.3 a archivos adicionales.
  - En clientes SMB, puede ver `test.txt` y `TEST~1.TXT`.
  - ONTAP crea el `TEST~1.TXT` nombre de archivo para diferenciar los dos archivos.

> Si ha habilitado o modificado la asignación de caracteres mediante los comandos de asignación de caracteres CIFS del Vserver, una búsqueda de Windows normalmente no distingue mayúsculas y minúsculas se convierte en sensible a mayúsculas y minúsculas.

Aprenda a crear nombres de archivos y directorios SMB de ONTAP

ONTAP crea y mantiene dos nombres para archivos o directorios en cualquier directorio que tenga acceso desde un cliente SMB: El nombre largo original y un nombre en formato 8.3.

Para los nombres de archivos o directorios que excedan el nombre de ocho caracteres o el límite de extensión de tres caracteres (para archivos), ONTAP genera un nombre de formato de 8.3 de la siguiente manera:

- Trunca el nombre del archivo o directorio original a seis caracteres, si el nombre supera los seis.
- Agrega una tilde (~) y un número, de uno a cinco, a los nombres de archivo o directorio que ya no son únicos después de truncarse.

  Si se queda sin números porque hay más de cinco nombres similares, crea un nombre único que no tiene relación con el nombre original.

- En el caso de los archivos, trunca la extensión del nombre de archivo a tres caracteres.

Por ejemplo, si un cliente NFS crea un archivo llamado `specifications.html`, el nombre de archivo de formato 8,3 creado por ONTAP es `specif~1.htm`. Si este nombre ya existe, ONTAP utiliza un número diferente al final del nombre de archivo. Por ejemplo, si un cliente NFS crea otro archivo denominado `specifications_new.html`, el formato 8,3 de `specifications_new.html` es `specif~2.htm`.

Obtenga información sobre los nombres de archivos, directorios y qtree multibyte SMB de ONTAP

A partir de ONTAP 9.5, la compatibilidad con nombres codificados UTF-8 de 4 bytes permite la creación y visualización de nombres de archivos, directorios y árboles que incluyen caracteres complementarios Unicode fuera del plano multilingüe básico (BMP). En las versiones anteriores, estos caracteres complementarios no se mostraba correctamente en entornos multiprotocolo.

Para habilitar la compatibilidad con nombres codificados UTF-8 de 4 bytes, hay disponible un nuevo código de idioma *utf8mb4* para las `vserver volume` familias de comandos y.

Debe crear un nuevo volumen de una de las siguientes maneras:

- Configuración `-language` explícita de la opción volume: `volume create -language utf8mb4 {…}`
- Heredar `-language` la opción de volumen de una SVM que se haya creado o modificado para la opción: `vserver [create|modify] -language utf8mb4 {…}``volume create {…}`
- En ONTAP 9,6 y versiones anteriores, no puede modificar los volúmenes existentes para la compatibilidad con utf8mb4. Debe crear un volumen listo para utf8mb4 y después migrar los datos con las herramientas de copia basadas en cliente.

  Puede actualizar las SVM para que admitan utf8mb4, pero los volúmenes existentes conservan sus códigos de idioma originales.

  Si utiliza ONTAP 9.7P1 o una versión posterior, puede modificar los volúmenes existentes para utf8mb4 con una solicitud de soporte. Para obtener más información, consulte "¿Se puede cambiar el idioma del volumen después de crearlo en ONTAP?".

- A partir de ONTAP 9.8, puede usar `[-language <Language code>]` el parámetro para cambiar el idioma del volumen de *.utf-8 a utf8mb4. Para cambiar el idioma de un volumen, póngase en contacto con "Soporte de NetApp".

> Los nombres de las LUN con caracteres UTF-8 de 4 bytes no se admiten actualmente.

- Los datos de caracteres Unicode se suelen representar en aplicaciones de sistemas de archivos Windows que utilizan el formato de transformación Unicode de 16 bits (UTF-16) y en sistemas de archivos NFS que utilizan el formato de transformación Unicode de 8 bits (UTF-8).

  En las versiones anteriores a ONTAP 9.5, los nombres incluidos los caracteres complementarios UTF-16 creados por los clientes de Windows se mostraban correctamente a otros clientes de Windows pero no se tradujeron correctamente a UTF-8 para los clientes NFS. Del mismo modo, los nombres con caracteres complementarios UTF-8 de los clientes NFS creados no se tradujeron correctamente a UTF-16 para los clientes Windows.

- Cuando se crean nombres de archivo en sistemas que ejecutan ONTAP 9.4 o una versión anterior que contienen caracteres complementarios válidos o no válidos, ONTAP rechaza el nombre de archivo y devuelve un error de nombre de archivo no válido.

  Para evitar este problema, utilice sólo los caracteres BMP en los nombres de archivo y evite utilizar caracteres complementarios, o actualice a ONTAP 9.5 o posterior.

A partir de ONTAP 9, se permiten caracteres Unicode en nombres de qtree.

- Puede usar `volume qtree` la familia de comandos o System Manager para configurar o modificar los nombres de qtree.
- Los nombres de qtree pueden incluir caracteres de varios bytes en formato Unicode, como los caracteres japoneses y chinos.
- En versiones anteriores a ONTAP 9.5, sólo se admiten los caracteres BMP (es decir, los que podrían representarse en 3 bytes).

> En las versiones anteriores a ONTAP 9.5, la ruta de unión del volumen principal del qtree puede contener nombres de qtree y directorio con caracteres Unicode. El `volume show` comando muestra estos nombres correctamente cuando el volumen primario tiene una configuración de idioma UTF-8. Sin embargo, si el idioma del volumen principal no es uno de los valores de idioma UTF-8, algunas partes de la ruta de unión se muestran utilizando un nombre NFS alternativo numérico.

- En las versiones 9.5 y posteriores, se admiten caracteres de 4 bytes en nombres de qtree, siempre y cuando el qtree se encuentre en un volumen habilitado para utf8mb4.

Configurar la asignación de caracteres para la traducción de nombres de archivos SMB de ONTAP en volúmenes

Los clientes NFS pueden crear nombres de archivo que contengan caracteres que no son válidos para los clientes SMB y ciertas aplicaciones Windows. Puede configurar la asignación de caracteres para la traducción de nombres de archivo en volúmenes para permitir que los clientes SMB accedan a archivos con nombres NFS que, de lo contrario, no serían válidos.

Acerca de esta tarea

Cuando los clientes SMB acceden a los archivos creados por los clientes NFS, ONTAP observa el nombre del archivo. Si el nombre no es un nombre de archivo SMB válido (por ejemplo, si tiene un carácter "':'" incrustado en dos puntos), ONTAP devuelve el nombre de archivo 8.3 que se mantiene para cada archivo. Sin embargo, esto causa problemas para las aplicaciones que codifican información importante en nombres de archivos largos.

Por lo tanto, si comparte un archivo entre clientes en diferentes sistemas operativos, debe utilizar caracteres en los nombres de archivo válidos en ambos sistemas operativos.

Sin embargo, si tiene clientes NFS que crean nombres de archivo que contienen caracteres que no son nombres de archivo válidos para clientes SMB, puede definir un mapa que convierte los caracteres NFS no válidos en caracteres Unicode que tanto SMB como determinadas aplicaciones Windows aceptan. Por ejemplo, esta funcionalidad admite las aplicaciones CATIA MCAD y Mathematica, así como otras aplicaciones que tienen este requisito.

Puede configurar la asignación de caracteres de volumen a volumen.

Debe tener en cuenta lo siguiente al configurar la asignación de caracteres en un volumen:

- La asignación de caracteres no se aplica a través de puntos de unión.

  Debe configurar explícitamente la asignación de caracteres para cada volumen de unión.

- Debe asegurarse de que los caracteres Unicode que se utilizan para representar caracteres no válidos o ilegales son caracteres que normalmente no aparecen en los nombres de archivo; de lo contrario, se producen asignaciones no deseadas.

  Por ejemplo, si intenta asignar dos puntos (:) a un guión (-) pero el guión (-) se utilizó correctamente en el nombre del archivo, un cliente de Windows que intente acceder a un archivo denominado «'a-b'» tendría su solicitud asignada al nombre NFS de «'a:b'» (no al resultado deseado).

- Después de aplicar la asignación de caracteres, si la asignación aún contiene un carácter de Windows no válido, ONTAP vuelve a los nombres de archivo de Windows 8.3.
- En las notificaciones de FPolicy, los registros de auditoría de NAS y los mensajes de seguimiento de seguridad, se muestran los nombres de archivos asignados.
- Cuando se crea una relación de SnapMirror del tipo DP, la asignación de caracteres del volumen de origen no se replica en el volumen de DP de destino.
- Distinción entre mayúsculas y minúsculas: Debido a que los nombres de Windows asignados se convierten en nombres NFS, la búsqueda de los nombres sigue a la semántica NFS. Esto incluye el hecho de que las búsquedas de NFS distinguen mayúsculas de minúsculas. Esto significa que las aplicaciones que acceden a recursos compartidos asignados no deben depender de un comportamiento que no distingue mayúsculas y minúsculas de Windows. Sin embargo, el nombre 8.3 está disponible y no distingue mayúsculas y minúsculas.
- Asignaciones parciales o no válidas: Tras asignar un nombre para devolver a los clientes que realizan enumeración de directorios ("dir"), se comprueba la validez de Windows en el nombre Unicode resultante. Si ese nombre sigue teniendo caracteres no válidos, o si no es válido para Windows (p. ej., finaliza en "". o en blanco) se devuelve el nombre 8.3 en lugar del nombre no válido.

Paso

1. Configurar asignación de caracteres: +

`vserver cifs character-mapping create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-mapping` *`mapping_text`*`, …` +

El mapeo consta de una lista de pares de caracteres fuente-objetivo separados por "':'". Los caracteres son caracteres Unicode introducidos mediante dígitos hexadecimales. Por ejemplo: 3C:E03C. +

El primer valor de cada `mapping_text` par que está separado por dos puntos es el valor hexadecimal del carácter NFS que desea traducir, y el segundo valor es el valor Unicode que utiliza SMB. Las parejas de asignación deben ser únicas (debe existir una asignación uno a uno).

- Asignación de fuentes +

La siguiente tabla muestra el conjunto de caracteres Unicode permisible para la asignación de origen:

+

Carácter Unicode	Carácter impreso	Descripción
0x01-0x19	No aplicable	Caracteres de control que no se imprimen
0x5C		Barra invertida
0x3A	:	Dos puntos
0x2A	*	Asterisco
0x3F	?	Signo de interrogación
0x22	"	Entre comillas
0x3C	<	Menor que
0x3E	>	Mayor que
0x7C		
Línea vertical	0xB1	±

- Asignación de objetivos

  Puede especificar caracteres de destino en el "'Área de uso privado'" de Unicode en el siguiente intervalo: U+E0000…U+F8FF.

Ejemplo

El siguiente comando crea una asignación de caracteres para un volumen denominado «data» en la máquina virtual de almacenamiento (SVM) vs1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  -----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

Información relacionada

Obtenga información sobre cómo crear y administrar volúmenes de datos en espacios de nombres

Comandos ONTAP para administrar asignaciones de caracteres para la traducción de nombres de archivos SMB

Puede gestionar la asignación de caracteres creando, modificando, mostrando información o eliminando asignaciones de caracteres de archivo utilizadas para la traducción del nombre del archivo SMB en volúmenes FlexVol.

Si desea…	Se usa este comando…
Cree nuevas asignaciones de caracteres de archivo	`vserver cifs character-mapping create`
Mostrar información acerca de las asignaciones de caracteres de archivo	`vserver cifs character-mapping show`
Modifique las asignaciones de caracteres de archivo existentes	`vserver cifs character-mapping modify`
Eliminar asignaciones de caracteres de archivo	`vserver cifs character-mapping delete`

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

Información relacionada

Configurar la asignación de caracteres para la traducción de nombres de archivos en volúmenes