Gestione servidores SMB

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

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`

Si desea	Introduzca el comando
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

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.
`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`*

Si desea…	Introduzca…
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*

Si desea actualizar…	Introduzca el comando…
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

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`
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`

Si desea determinar si…	Introduzca el comando…
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.