Gestión del almacenamiento nas

ONTAP 9

NetApp
February 26, 2026

This PDF was generated from https://docs.netapp.com/es-es/ontap/concept_nas_provision_overview.html on February 26, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Gestión del almacenamiento nas . . . 1
Gestione protocolos NAS con System Manager . . . 1
Obtenga más información sobre la administración de NAS con ONTAP System Manager . . . 1
Aprovisione almacenamiento NFS para almacenes de datos de VMware con ONTAP System Manager . . . 1
Aprovisione almacenamiento NAS para directorios domésticos con ONTAP System Manager . . . 2
Aprovisione almacenamiento NAS para servidores Linux mediante NFS con ONTAP System Manager . . . 3
Administre el acceso mediante políticas de exportación con ONTAP System Manager . . . 5
Aprovisione almacenamiento NAS para servidores Windows mediante SMB con ONTAP System Manager . . . 6
Aprovisione almacenamiento NAS para Windows y Linux usando NFS y SMB con ONTAP System Manager . . . 8
Acceso seguro de clientes con Kerberos mediante ONTAP System Manager . . . 10
Proporcionar acceso de cliente con servicios de nombres mediante ONTAP System Manager . . . 12
Administre directorios y archivos con ONTAP System Manager . . . 13
Administre usuarios y grupos específicos del host con ONTAP System Manager . . . 13
Supervisar clientes NFS activos con ONTAP System Manager . . . 16
Habilitar el almacenamiento NAS . . . 17
Configurar NFS . . . 21
Obtenga información sobre la configuración de NFS con la CLI de ONTAP . . . 21
Obtenga más información sobre el flujo de trabajo de configuración de NFS de ONTAP . . . 22
Preparación . . . 23
Configure el acceso de NFS a una SVM . . . 36
Añadir capacidad de almacenamiento a una SVM habilitada para NFS . . . 72
Dónde encontrar información adicional sobre ONTAP NFS . . . 87
En qué se diferencian las exportaciones de ONTAP de las exportaciones de 7-Mode . . . 88
Administrar NFS . . . 92
Obtenga información sobre el acceso a archivos ONTAP para el protocolo NFS . . . 92
Comprender el acceso a archivos NAS . . . 93
Cree y gestione volúmenes de datos en espacios de nombres NAS . . . 101
Configurar estilos de seguridad . . . 107
Configurar el acceso a archivos mediante NFS . . . 112
Gestione el acceso a archivos mediante NFS . . . 150
Admiten versiones y clientes NFS . . . 205
NFS paralelo . . . 209
Dependencias de nomenclatura de archivos y directorios NFS y SMB . . . 234
Gestión de enlaces NFS . . . 240
Obtenga más información sobre la conexión de enlaces NFS de ONTAP . . . 240
Configurar un nuevo servidor NFS y exportar para trunking . . . 241
Adapte las exportaciones NFS existentes para la conexión de enlaces . . . 247
Gestione NFS a través de RDMA . . . 252
Obtenga información sobre NFS sobre RDMA en ONTAP . . . 252
Configure las NIC para NFS a través de RDMA . . . 254

Configure LIF para NFS a través de RDMA . . . 256
Modifique la configuración NFS . . . 259
Configure SMB con la interfaz de línea de comandos . . . 259
Obtenga información sobre la configuración del bloque de mensajes del servidor con la CLI de ONTAP . . . 259
Flujo de trabajo de configuración de SMB de ONTAP . . . 260
Preparación . . . 261
Configure el acceso de SMB a una SVM . . . 272
Configure el acceso de clientes SMB al almacenamiento compartido . . . 294
Gestione SMB con la interfaz de línea de comandos . . . 303
Obtenga más información sobre SMB de ONTAP . . . 303
Compatibilidad con servidores SMB . . . 304
Gestione servidores SMB . . . 311
Configurar el acceso a archivos mediante SMB . . . 409
Gestione el acceso a archivos mediante SMB . . . 478
Ponga en marcha servicios basados en cliente de SMB . . . 572
Ponga en marcha servicios basados en servidor de SMB . . . 587
Dependencias de nomenclatura de archivos y directorios NFS y SMB . . . 659
Proporcione acceso del cliente S3 a los datos NAS . . . 665
Obtenga más información sobre la compatibilidad multiprotocolo de ONTAP S3 . . . 665
Obtenga información sobre los requisitos de datos NAS para el acceso del cliente ONTAP S3 . . . 668
Habilitar el acceso del protocolo S3 a los datos NAS en un SVM de ONTAP . . . 669
Crear un depósito NAS de ONTAP S3 . . . 672
Habilitar usuarios del cliente ONTAP S3 . . . 674
Configuración de SMB para Microsoft Hyper-V y SQL Server . . . 677
Información general de la configuración de SMB para Microsoft Hyper-V y SQL Server . . . 677
Configurar ONTAP para soluciones Microsoft Hyper-V y SQL Server sobre SMB . . . 678
Operaciones no disruptivas para Hyper-V y SQL Server sobre SMB . . . 679
Backups basados en recursos compartidos con VSS remoto . . . 683
Cómo se utiliza la descarga de copias ODX con Hyper-V y SQL Server en recursos compartidos SMB 687
Requisitos y consideraciones de configuración . . . 688
Recomendaciones para configuraciones de SQL Server y Hyper-V mediante SMB . . . 696
Planifique la configuración de Hyper-V o SQL Server con SMB . . . 697
Cree configuraciones de ONTAP para proporcionar operaciones no disruptivas con Hyper-V y SQL Server sobre SMB . . . 700
Gestione Hyper-V y SQL Server con las configuraciones de SMB . . . 715
Utilice estadísticas para supervisar la actividad de Hyper-V y SQL Server mediante SMB . . . 720
Compruebe que la configuración admite operaciones no disruptivas . . . 723

Gestión del almacenamiento nas

Gestione protocolos NAS con System Manager

Obtenga más información sobre la administración de NAS con ONTAP System Manager

Los temas de esta sección muestran cómo configurar y gestionar entornos NAS con System Manager en ONTAP 9.7 y versiones posteriores.

Si utiliza la versión clásica de System Manager (disponible solo en ONTAP 9.7 y versiones anteriores), consulte los temas siguientes:

- "Información general de la configuración DE NFS"
- "Información general de la configuración DE SMB"

System Manager admite flujos de trabajo para:

- Configuración inicial de los clústeres que pretende utilizar para los servicios de archivos NAS.
- Aprovisionamiento de volúmenes adicional para las necesidades de almacenamiento cambiantes.
- Configuración y mantenimiento de las instalaciones de seguridad y autenticación estándar del sector.

Mediante System Manager, puede gestionar servicios NAS en el nivel de componentes:

- Protocolos: NFS, SMB o ambos (NAS multiprotocolo)
- Servicios de nombres: DNS, LDAP y NIS
- Cambio de servicio de nombres
- Seguridad de Kerberos y TLS
- Exportaciones y acciones
- Qtrees
- Asignación de nombres de usuarios y grupos

Aprovisione almacenamiento NFS para almacenes de datos de VMware con ONTAP System Manager

Antes de usar Virtual Storage Console para VMware vSphere (VSC) para aprovisionar volúmenes NFS en un sistema de almacenamiento basado en ONTAP para hosts ESXi, habilite NFS mediante System Manager para ONTAP 9.7 o una versión posterior.

Después de crear un "Máquina virtual de almacenamiento compatible con NFS" en System Manager, a continuación, debe aprovisionar volúmenes de NFS y gestionar almacenes de datos con VSC.

A partir de VSC 7,0, VSC forma parte "Herramientas de ONTAP para el dispositivo virtual de VMware vSphere" de los, que incluyen VSC, las API de vStorage para el proveedor de conocimiento del almacenamiento (VASA) y las funcionalidades del adaptador de replicación de almacenamiento (SRA) para VMware vSphere.

Asegúrese de comprobar "Matriz de interoperabilidad de NetApp" la compatibilidad entre sus versiones actuales de ONTAP y VSC.

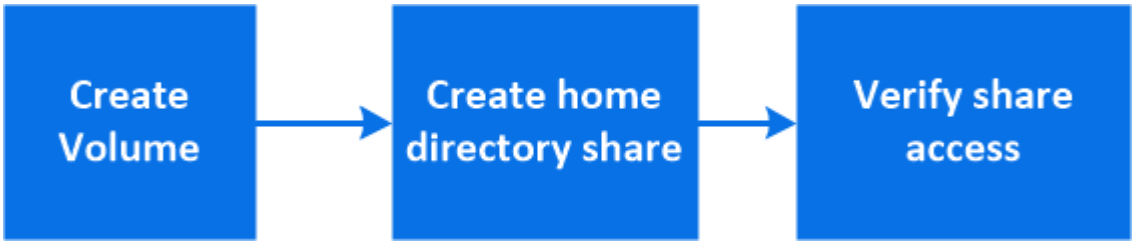
Para configurar el acceso NFS para hosts ESXi de almacenes de datos mediante System Manager Classic (para ONTAP 9,7 y versiones anteriores), consulte "Configuración de NFS para ESXi mediante información general de VSC"

Para obtener más información, consulte "TR-4597: VMware vSphere para ONTAP" y la documentación de su versión de VSC.

Aprovisione almacenamiento NAS para directorios domésticos con ONTAP System Manager

Cree volúmenes para proporcionar almacenamiento para directorios iniciales mediante el protocolo SMB.

Este procedimiento crea nuevos volúmenes para los directorios iniciales en una "Máquinas virtuales de almacenamiento habilitadas para SMB existentes". Puede aceptar los valores predeterminados del sistema al configurar volúmenes o especificar configuraciones personalizadas.



Puede crear volúmenes FlexVol o, para sistemas de archivos grandes con requisitos de alto rendimiento, puede crear volúmenes FlexGroup . Véase también"Cree volúmenes de FlexGroup" .

También puede guardar las especificaciones de este volumen en un libro de aplicaciones de Ansible. Para obtener más información, visite "Utilice libros de aplicaciones Ansible para añadir o editar volúmenes o LUN".

Pasos

1. Añadir un volumen nuevo en una máquina virtual de almacenamiento habilitada para SMB
   a. Seleccione **Almacenamiento > Volúmenes** y, a continuación, haga clic en **Agregar**.
   b. Introduzca un nombre, seleccione la máquina virtual de almacenamiento e introduzca un tamaño.

      Solo se enumeran las máquinas virtuales de almacenamiento configuradas con el protocolo SMB. Si solo hay disponible una VM de almacenamiento configurada con el protocolo SMB, no se muestra el campo **Storage VM**.

      - Si hace clic en **Guardar** en este momento, System Manager utiliza valores predeterminados del sistema para crear y agregar un volumen FlexVol.
      - Puede hacer clic en **más opciones** para personalizar la configuración del volumen y activar servicios como autorización, calidad de servicio y protección de datos. Consulte Personalice la configuración del volumeny, a continuación, vuelva aquí para realizar los siguientes pasos.
2. haga clic en **almacenamiento > recursos compartidos**, haga clic en **Agregar** y seleccione **Directorio inicial**.
3. En un cliente Windows, haga lo siguiente para verificar que se puede acceder al recurso compartido.

a. En el Explorador de Windows, asigne una unidad al recurso compartido en el siguiente formato: `\\<SMB_Server_Name>\<Share_Name>`

   Si el nombre del recurso compartido se creó con variables (%w, %d o %u), asegúrese de probar el acceso con un nombre resuelto.

b. En la unidad recién creada, cree un archivo de prueba y, a continuación, elimine el archivo.

Personalice la configuración del volumen

Se puede personalizar la configuración del volumen cuando se añaden volúmenes en lugar de aceptar los valores predeterminados del sistema.

Pasos

Después de hacer clic en **más opciones**, seleccione la funcionalidad que necesite e introduzca los valores necesarios.

- Caché para volumen remoto.
- Nivel de servicio de rendimiento (calidad de servicio, calidad de servicio).

  A partir de ONTAP 9,8, puede especificar una política de calidad de servicio personalizada o deshabilitar la calidad de servicio, además de la selección de valor predeterminada.

  - Para desactivar QoS, seleccione **personalizado**, **existente** y **ninguno**.
  - Si selecciona **personalizado** y especifica un nivel de servicio existente, se seleccionará automáticamente un nivel local.
  - A partir de ONTAP 9.9.1, si decide crear un nivel de servicio de rendimiento personalizado, puede utilizar System Manager para seleccionar manualmente el nivel local (**colocación manual**) en el que desea colocar el volumen que está creando.

    Esta opción no está disponible si selecciona las opciones de caché remota o volumen FlexGroup.

- FlexGroup Volumes (seleccione **distribuir datos de volumen en el clúster**).

  Esta opción no está disponible si ha seleccionado previamente **colocación manual** en **nivel de servicio de rendimiento**. De lo contrario, el volumen que va a añadir se convierte en volumen FlexVol de forma predeterminada.

- Permisos de acceso para los protocolos para los que se configuró el volumen.
- Protección de datos con SnapMirror (local o remoto) y, a continuación, especifique la política de protección y la configuración para el clúster de destino desde las listas desplegables.
- Seleccione **Guardar** para crear el volumen y agregarlo al clúster y a la VM de almacenamiento.

Una vez que guarde el volumen, vuelva a Paso 2 en el flujo de trabajocompletar el aprovisionamiento de los directorios iniciales.

Aprovisione almacenamiento NAS para servidores Linux mediante NFS con ONTAP System Manager

Cree volúmenes para proporcionar almacenamiento para servidores Linux mediante el protocolo NFS con el Administrador del sistema de ONTAP (9.7 y posterior).

Este procedimiento crea nuevos volúmenes en una "Máquinas virtuales de almacenamiento habilitadas para NFS existentes". Puede aceptar los valores predeterminados del sistema al configurar volúmenes o especificar configuraciones personalizadas.

Puede crear volúmenes FlexVol o, para sistemas de archivos grandes con requisitos de alto rendimiento, puede crear volúmenes FlexGroup . Véase también"Cree volúmenes de FlexGroup" .

También puede guardar las especificaciones de este volumen en un libro de aplicaciones de Ansible. Para obtener más información, visite "Utilice libros de aplicaciones Ansible para añadir o editar volúmenes o LUN".

Si desea obtener más información sobre la gama de capacidades del protocolo NFS de ONTAP, consulte la "Obtenga información sobre el acceso a archivos ONTAP para el protocolo NFS".

Pasos

1. Añadir un volumen nuevo en una máquina virtual de almacenamiento habilitada para NFS
   a. Haga clic en **almacenamiento > volúmenes** y, a continuación, haga clic en **Agregar**.
   b. Introduzca un nombre, seleccione la máquina virtual de almacenamiento e introduzca un tamaño.

      Solo se enumeran las máquinas virtuales de almacenamiento configuradas con el protocolo NFS. Si solo hay disponible una VM de almacenamiento configurada con el protocolo SMB, no se muestra el campo **Storage VM**.

      - Si hace clic en **Guardar** en este momento, System Manager utiliza valores predeterminados del sistema para crear y agregar un volumen FlexVol.

        La política de exportación predeterminada concede acceso completo a todos los usuarios.

      - Puede hacer clic en **más opciones** para personalizar la configuración del volumen y activar servicios como autorización, calidad de servicio y protección de datos. Consulte Personalice la configuración del volumeny, a continuación, vuelva aquí para realizar los siguientes pasos.
2. [[paso 2-Complete-prov,paso 2 en el flujo de trabajo]] en un cliente Linux, haga lo siguiente para verificar el acceso.
   a. Cree y monte el volumen con la interfaz de red de la máquina virtual de almacenamiento.
   b. En el volumen recién montado, cree un archivo de prueba, escriba texto y, a continuación, elimine el archivo.

   Después de verificar el acceso, puede "restrinja el acceso de los clientes con la política de exportación del volumen"establecer cualquier propiedad y permisos de UNIX deseados en el volumen montado.

Personalice la configuración del volumen

Se puede personalizar la configuración del volumen cuando se añaden volúmenes en lugar de aceptar los valores predeterminados del sistema.

Pasos

Después de hacer clic en **más opciones**, seleccione la funcionalidad que necesite e introduzca los valores necesarios.

- Caché para volumen remoto.

- Nivel de servicio de rendimiento (calidad de servicio, calidad de servicio).

  A partir de ONTAP 9,8, puede especificar una política de calidad de servicio personalizada o deshabilitar la calidad de servicio, además de la selección de valor predeterminada.

  - Para desactivar QoS, seleccione **personalizado**, **existente** y **ninguno**.
  - Si selecciona **personalizado** y especifica un nivel de servicio existente, se seleccionará automáticamente un nivel local.
  - A partir de ONTAP 9.9.1, si decide crear un nivel de servicio de rendimiento personalizado, puede utilizar System Manager para seleccionar manualmente el nivel local (**colocación manual**) en el que desea colocar el volumen que está creando.

    Esta opción no está disponible si selecciona las opciones de caché remota o volumen FlexGroup.

- FlexGroup Volumes (seleccione **distribuir datos de volumen en el clúster**).

  Esta opción no está disponible si ha seleccionado previamente **colocación manual** en **nivel de servicio de rendimiento**. De lo contrario, el volumen que va a añadir se convierte en volumen FlexVol de forma predeterminada.

- Permisos de acceso para los protocolos para los que se configuró el volumen.
- Protección de datos con SnapMirror (local o remoto) y, a continuación, especifique la política de protección y la configuración para el clúster de destino desde las listas desplegables.
- Seleccione **Guardar** para crear el volumen y agregarlo al clúster y a la VM de almacenamiento.

Una vez guardado el volumen, vuelva a [step2-complete-prov]completar el aprovisionamiento de servidores Linux mediante NFS.

Otras maneras de hacerlo en ONTAP

Para realizar esta tarea con…	Consulte…
System Manager Classic (ONTAP 9.7 y anterior)	"Información general de la configuración DE NFS"
La interfaz de línea de comandos (CLI) de ONTAP	"Obtenga información sobre la configuración de NFS con la CLI de ONTAP"

Administre el acceso mediante políticas de exportación con ONTAP System Manager

Habilite el acceso del cliente Linux a servidores NFS mediante políticas de exportación.

Este procedimiento crea o modifica políticas de exportación para una "Máquinas virtuales de almacenamiento habilitadas para NFS existentes".

Pasos

1. En System Manager, haga clic en **almacenamiento** > **volúmenes**.
2. Haga clic en un volumen con NFS activado y haga clic en **más**.
3. Haga clic en **Editar directiva de exportación** y, a continuación, haga clic en **Seleccionar una directiva existente** o **Agregar una nueva directiva**.

Aprovisione almacenamiento NAS para servidores Windows mediante SMB con ONTAP System Manager

Cree volúmenes para proporcionar almacenamiento para servidores Windows mediante el protocolo SMB mediante System Manager, que está disponible con ONTAP 9.7 y versiones posteriores.

Este procedimiento crea volúmenes nuevos en un "Máquinas virtuales de almacenamiento habilitadas para SMB existentes" y crea un recurso compartido para el directorio raíz del volumen (/). Puede aceptar los valores predeterminados del sistema al configurar volúmenes o especificar configuraciones personalizadas. Después de la configuración inicial de SMB, también puede crear recursos compartidos adicionales y modificar sus propiedades.

Puede crear volúmenes FlexVol o, para sistemas de archivos grandes con requisitos de alto rendimiento, puede crear volúmenes FlexGroup . Véase también"Cree volúmenes de FlexGroup" .

También puede guardar las especificaciones de este volumen en un libro de aplicaciones de Ansible. Para obtener más información, visite "Utilice libros de aplicaciones Ansible para añadir o editar volúmenes o LUN".

Si desea obtener más información sobre la gama de capacidades del protocolo SMB de ONTAP, consulte la "Descripción general de referencias".

Antes de empezar

- A partir de ONTAP 9.13.1, puede habilitar los análisis de capacidad y el seguimiento de actividades de forma predeterminada en volúmenes nuevos. En System Manager, puede gestionar la configuración predeterminada en el nivel del clúster o de máquina virtual de almacenamiento. Para obtener más información, consulte "Active File System Analytics".

Pasos

1. Añadir un volumen nuevo en una máquina virtual de almacenamiento habilitada para SMB
   a. Haga clic en **almacenamiento > volúmenes** y, a continuación, haga clic en **Agregar**.
   b. Introduzca un nombre, seleccione la máquina virtual de almacenamiento e introduzca un tamaño.

      Solo se enumeran las máquinas virtuales de almacenamiento configuradas con el protocolo SMB. Si solo hay disponible una VM de almacenamiento configurada con el protocolo SMB, no se muestra el campo **Storage VM**.

      - Si selecciona **Guardar** en este punto, System Manager utiliza los valores predeterminados del sistema para crear y añadir un volumen de FlexVol.
      - Puede seleccionar **Más opciones** para personalizar la configuración del volumen y habilitar servicios como autorización, calidad de servicio y protección de datos. Consulte Personalice la configuración del volumeny, a continuación, vuelva aquí para realizar los siguientes pasos.
2. cambie a un cliente de Windows para verificar que el recurso compartido esté accesible.
   a. En el Explorador de Windows, asigne una unidad al recurso compartido en el siguiente formato: `\\_SMB_Server_Name__Share_Name_`
   b. En la unidad recién creada, cree un archivo de prueba, escriba texto y, a continuación, elimine el archivo.

Después de verificar el acceso, puede restringir el acceso de cliente con la ACL compartida y establecer las propiedades de seguridad deseadas en la unidad asignada. Consulte "Crear acciones" para obtener más información.

Añadir o modificar recursos compartidos

Puede añadir recursos compartidos adicionales después de la configuración inicial de SMB. Los recursos compartidos se crean con los valores predeterminados y las propiedades que se seleccionan. Estos se pueden modificar más adelante.

Puede establecer las siguientes propiedades de uso compartido al configurar un recurso compartido:

- Permisos de acceso
- Comparta propiedades
  - Habilitar la disponibilidad continua de los recursos compartidos que contienen Hyper-V y SQL Server en datos de SMB (empezando por ONTAP 9.10.1). Consulte también:
    - "Disponibilidad continua de los requisitos de recursos compartidos para Hyper-V en SMB"
    - "Requisitos de recursos compartidos disponibles de forma continua para SQL Server en SMB"
  - Cifre datos con SMB 3.0 al acceder al recurso compartido.

Después de la configuración inicial, también es posible modificar estas propiedades:

- Enlaces simbólicos
  - Activa o desactiva los enlaces simbólicos y las tintas alámbrica
- Comparta propiedades
  - Permitir que los clientes accedan al directorio de instantáneas.
  - Habilite los bloqueos oportunistas, lo que permite a los clientes bloquear archivos y almacenar el contenido en la caché localmente (predeterminado).
  - Habilite la enumeración basada en acceso (ABE) para que muestre recursos compartidos basados en los permisos de acceso del usuario.

Pasos

1. Para añadir un nuevo recurso compartido en un volumen habilitado para SMB, haga clic en **almacenamiento > recursos compartidos**, haga clic en **Agregar** y seleccione **Compartir**.
2. Para modificar un recurso compartido existente, haga clic en **Almacenamiento > Recursos compartidos**, luego haga clic en ⋮ y seleccione **Editar**.

Personalice la configuración del volumen

Se puede personalizar la configuración del volumen cuando se añaden volúmenes en lugar de aceptar los valores predeterminados del sistema.

Pasos

Después de hacer clic en **más opciones**, seleccione la funcionalidad que necesite e introduzca los valores necesarios.

- Caché para volumen remoto.
- Nivel de servicio de rendimiento (calidad de servicio, calidad de servicio).

  A partir de ONTAP 9,8, puede especificar una política de calidad de servicio personalizada o deshabilitar la calidad de servicio, además de la selección de valor predeterminada.

  - Para desactivar QoS, seleccione **personalizado**, **existente** y **ninguno**.

- Si selecciona **personalizado** y especifica un nivel de servicio existente, se seleccionará automáticamente un nivel local.
- A partir de ONTAP 9.9.1, si decide crear un nivel de servicio de rendimiento personalizado, puede utilizar System Manager para seleccionar manualmente el nivel local (**colocación manual**) en el que desea colocar el volumen que está creando.

  Esta opción no está disponible si selecciona las opciones de caché remota o volumen FlexGroup.

- FlexGroup Volumes (seleccione **distribuir datos de volumen en el clúster**).

  Esta opción no está disponible si ha seleccionado previamente **colocación manual** en **nivel de servicio de rendimiento**. De lo contrario, el volumen que va a añadir se convierte en volumen FlexVol de forma predeterminada.

- Permisos de acceso para los protocolos para los que se configuró el volumen.
- Protección de datos con SnapMirror (local o remoto) y, a continuación, especifique la política de protección y la configuración para el clúster de destino desde las listas desplegables.
- Seleccione **Guardar** para crear el volumen y agregarlo al clúster y a la VM de almacenamiento.

Una vez que guarde el volumen, vuelva a [step2-compl-prov-win]completar el aprovisionamiento para los servidores Windows con SMB.

Otras maneras de hacerlo en ONTAP

Para realizar esta tarea con…	Consulte…
System Manager Classic (ONTAP 9.7 y anterior)	"Información general de la configuración DE SMB"
La interfaz de línea de comandos de ONTAP	"Información general de configuración de SMB con la CLI"

Aprovisione almacenamiento NAS para Windows y Linux usando NFS y SMB con ONTAP System Manager

Cree volúmenes para proporcionar almacenamiento a los clientes mediante el protocolo NFS o SMB.

Este procedimiento crea nuevos volúmenes en una "Máquinas virtuales de almacenamiento existentes habilitadas para los protocolos NFS y SMB".

El protocolo NFS se utiliza con frecuencia en entornos Linux. El protocolo SMB se utiliza generalmente en entornos Windows. Sin embargo, tanto NFS como SMB pueden usarse tanto con Linux como con Windows.

Puede crear volúmenes FlexVol o, para sistemas de archivos grandes con requisitos de alto rendimiento, puede crear volúmenes FlexGroup . Ver"Cree volúmenes de FlexGroup" .

También puede guardar las especificaciones de este volumen en un libro de aplicaciones de Ansible. Para obtener más información, visite "Utilice libros de aplicaciones Ansible para añadir o editar volúmenes o LUN".

Pasos

1. Añadir un nuevo volumen en una máquina virtual de almacenamiento habilitada para NFS y SMB.

   a. Haga clic en **almacenamiento > volúmenes** y, a continuación, haga clic en **Agregar**.

   b. Introduzca un nombre, seleccione la máquina virtual de almacenamiento e introduzca un tamaño.

      Solo se muestran las máquinas virtuales de almacenamiento configuradas con los protocolos NFS y SMB. Si sólo está disponible un equipo virtual de almacenamiento configurado con los protocolos NFS y SMB, no se muestra el campo **Storage VM**.

   c. Haga clic en **Más opciones** y seleccione **Exportar a través de NFS**.

      El valor predeterminado concede acceso total a todos los usuarios. Si lo desea, puede añadir más reglas restrictivas a la política de exportación.

   d. Seleccione **Compartir a través de SMB/CIFS**.

      El recurso compartido se crea con una lista predeterminada de control de acceso (ACL) establecida en "Control total" para el grupo **Everyone**. Puede agregar restricciones a la ACL más adelante.

   e. Si hace clic en **Guardar** en este momento, System Manager utiliza valores predeterminados del sistema para crear y agregar un volumen FlexVol.

   También puede continuar habilitiendo cualquier servicio necesario adicional, como la autorización, la calidad del servicio y la protección de datos. Consulte Personalice la configuración del volumeny, a continuación, vuelva aquí para realizar los siguientes pasos.

2. en un cliente Linux, verifique que se pueda acceder a la exportación.

   a. Cree y monte el volumen con la interfaz de red de la máquina virtual de almacenamiento.

   b. En el volumen recién montado, cree un archivo de prueba, escriba texto y, a continuación, elimine el archivo.

3. En un cliente Windows, haga lo siguiente para verificar que se puede acceder al recurso compartido.

   a. En el Explorador de Windows, asigne una unidad al recurso compartido en el siguiente formato: `\\_SMB_Server_Name__Share_Name_`

   b. En la unidad recién creada, cree un archivo de prueba, escriba texto y, a continuación, elimine el archivo.

   Después de verificar el acceso, puede "Restrinja el acceso de los clientes con la política de exportación del volumen y restrinja el acceso de los clientes con la ACL de recursos compartidos"y establecer cualquier propiedad y permisos deseados en el volumen exportado y compartido.

Personalice la configuración del volumen

Se puede personalizar la configuración del volumen cuando se añaden volúmenes en lugar de aceptar los valores predeterminados del sistema.

Pasos

Después de hacer clic en **más opciones**, seleccione la funcionalidad que necesite e introduzca los valores necesarios.

- Caché para volumen remoto.
- Nivel de servicio de rendimiento (calidad de servicio, calidad de servicio).

  A partir de ONTAP 9,8, puede especificar una política de calidad de servicio personalizada o deshabilitar la calidad de servicio, además de la selección de valor predeterminada.

  - Para desactivar QoS, seleccione **personalizado**, **existente** y **ninguno**.
  - Si selecciona **personalizado** y especifica un nivel de servicio existente, se seleccionará automáticamente un nivel local.
  - A partir de ONTAP 9.9.1, si decide crear un nivel de servicio de rendimiento personalizado, puede utilizar System Manager para seleccionar manualmente el nivel local (**colocación manual**) en el que desea colocar el volumen que está creando.

    Esta opción no está disponible si selecciona las opciones de caché remota o volumen FlexGroup.

- FlexGroup Volumes (seleccione **distribuir datos de volumen en el clúster**).

  Esta opción no está disponible si ha seleccionado previamente **colocación manual** en **nivel de servicio de rendimiento**. De lo contrario, el volumen que va a añadir se convierte en volumen FlexVol de forma predeterminada.

- Permisos de acceso para los protocolos para los que se configuró el volumen.
- Protección de datos con SnapMirror (local o remoto) y, a continuación, especifique la política de protección y la configuración para el clúster de destino desde las listas desplegables.
- Seleccione **Guardar** para crear el volumen y agregarlo al clúster y a la VM de almacenamiento.

Una vez que guarde el volumen, vuelva al [step2-compl-prov-nfs-smb]aprovisionamiento multiprotocolo completo para servidores Windows y Linux.

Otras maneras de hacerlo en ONTAP

Para ejecutar estas tareas con…	Ver este contenido…
System Manager Classic (ONTAP 9.7 y anterior)	"Información general de la configuración de varios protocolos de SMB y NFS"
La interfaz de línea de comandos de ONTAP	• "Información general de configuración de SMB con la CLI" • "Obtenga información sobre la configuración de NFS con la CLI de ONTAP" • "Aprenda sobre los estilos de seguridad y sus efectos." • "Distinción entre mayúsculas y minúsculas de nombres de archivos y directorios en un entorno multiprotocolo"

Acceso seguro de clientes con Kerberos mediante ONTAP System Manager

Active Kerberos para garantizar el acceso al almacenamiento seguro para clientes NAS.

Este procedimiento configura Kerberos en una VM de almacenamiento existente habilitada para "NFS" o "SMB".

Antes de empezar, debe haber configurado DNS, NTP y "LDAP" en el sistema de almacenamiento.

Pasos

1. En la línea de comandos de ONTAP, establezca permisos UNIX para el volumen raíz de la máquina virtual de almacenamiento.

   a. Muestre los permisos relevantes en el volumen raíz de la máquina virtual de almacenamiento `volume show -volume root_vol_name-fields user,group,unix-permissions`: . Obtenga más información sobre `volume show` en el "Referencia de comandos del ONTAP".

      El volumen raíz del equipo virtual de almacenamiento debe tener la siguiente configuración:

Nombre…	Estableciendo…
UID	Raíz o ID 0
GID	Raíz o ID 0
Permisos de UNIX	755

   a. Si no se muestran estos valores, utilice `volume modify` el comando para actualizarlos. Obtenga más información sobre `volume modify` en el "Referencia de comandos del ONTAP".

2. Configure los permisos de usuario para el volumen raíz de la máquina virtual de almacenamiento.

   a. Mostrar los usuarios locales de UNIX `vserver services name-service unix-user show -vserver vserver_name`: . Obtenga más información sobre `vserver services name-service unix-user show` en el "Referencia de comandos del ONTAP".

      El equipo virtual de almacenamiento debe tener configurados los siguientes usuarios UNIX:

Nombre de usuario	ID de usuario	ID del grupo principal
nfs	500	0
raíz	0	0

+
Nota: el usuario NFS no es necesario si existe una asignación de nombres Kerberos-UNIX para el SPN del usuario cliente NFS; consulte el paso 5.

   a. Si no se muestran estos valores, utilice `vserver services name-service unix-user modify` el comando para actualizarlos. Obtenga más información sobre `vserver services name-service unix-user modify` en el "Referencia de comandos del ONTAP".

3. Configure permisos de grupo para el volumen raíz de la máquina virtual de almacenamiento.

   a. Mostrar los grupos UNIX locales `vserver services name-service unix-group show`

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

El equipo virtual de almacenamiento debe tener configurados los siguientes grupos UNIX:

Nombre del grupo	ID de grupo
daemon	1
raíz	0

a. Si no se muestran estos valores, utilice `vserver services name-service unix-group modify` el comando para actualizarlos. Obtenga más información sobre `vserver services name-service unix-group modify` en el "Referencia de comandos del ONTAP".

4. Cambie a System Manager para configurar Kerberos
5. En System Manager, haga clic en **almacenamiento > Storage VMs** y seleccione la VM de almacenamiento.
6. Haga clic en **Configuración**.
7. Haga clic en → en Kerberos.
8. Haga clic en **Agregar** en Kerberos Realm y complete las siguientes secciones:
   - Añada Kerberos Realm

     Introduzca los detalles de configuración según el proveedor de KDC.
   - Agregue interfaz de red a Realm

     Haga clic en **Agregar** y seleccione una interfaz de red.
9. Si lo desea, agregue asignaciones de nombres principales de Kerberos a nombres de usuario locales.
   a. Haga clic en **almacenamiento > Storage VMs** y seleccione la VM de almacenamiento.
   b. Haga clic en **Configuración**, y luego haga clic en → **Asignación de nombres**.
   c. En **Kerberos a UNIX**, agregue patrones y reemplazos usando expresiones regulares.

Proporcionar acceso de cliente con servicios de nombres mediante ONTAP System Manager

Habilite ONTAP para que busque información de host, usuario, grupo o grupo de red mediante LDAP o NIS para autenticar clientes NAS.

Este procedimiento crea o modifica configuraciones LDAP o NIS en una VM de almacenamiento existente activada para "NFS" o "SMB".

Para las configuraciones LDAP, debe tener los detalles de configuración LDAP necesarios en el entorno y debe usar un esquema LDAP de ONTAP predeterminado.

Pasos

1. Configure el servicio requerido: Haga clic en **almacenamiento > Storage VMs**.
2. Seleccione la máquina virtual de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en ⚙ para LDAP o NIS.

3. Incluya cualquier cambio en el conmutador de servicios de nombres: Haga clic en Cambiar servicios de nombres.

Administre directorios y archivos con ONTAP System Manager

Expanda la visualización de volumen de System Manager para ver y eliminar directorios y archivos.

A partir de ONTAP 9.9,1, los directorios se eliminan con una funcionalidad de eliminación de directorios asíncrona de baja latencia.

Para obtener más información sobre la visualización de sistemas de archivos en ONTAP 9.9,1 y posteriores, consulte "Descripción general de File System Analytics".

Paso

1. Seleccione **almacenamiento > volúmenes**. Expanda un volumen para ver su contenido.

Administre usuarios y grupos específicos del host con ONTAP System Manager

A partir de ONTAP 9.10.1, puede utilizar System Manager para gestionar usuarios y grupos específicos de un host UNIX o Windows.

Puede realizar los siguientes procedimientos:

Windows	UNIX
• Ver usuarios y grupos de Windows • [add-edit-delete-Windows] • [manage-windows-users]	• Ver usuarios y grupos UNIX • [add-edit-delete-UNIX] • [manage-unix-users]

Ver usuarios y grupos de Windows

En System Manager, puede ver una lista de usuarios y grupos de Windows.

Pasos

1. En System Manager, haga clic en **almacenamiento > Storage VMs**.
2. Seleccione el equipo virtual de almacenamiento y, a continuación, seleccione la ficha **Configuración**.
3. Desplácese hasta el área **usuarios de host y grupos**.

   La sección **Windows** muestra un resumen del número de usuarios de cada grupo asociado con el equipo virtual de almacenamiento seleccionado.

4. Haga clic en la sección **Windows**.
5. Haga clic en la pestaña **Grupos** y, a continuación, haga clic en junto al nombre de un grupo para ver los detalles de ese grupo.
6. Para ver los usuarios de un grupo, seleccione el grupo y, a continuación, haga clic en la ficha **usuarios**.

Agregar, editar o eliminar un grupo Windows

En System Manager, puede gestionar grupos de Windows añadiendo, editando o eliminando grupos.

Pasos

1. En System Manager, consulte la lista de grupos de Windows. Consulte Ver usuarios y grupos de Windows.
2. En la ficha **grupos**, puede administrar grupos con las siguientes tareas:

Para realizar esta acción…	Realice estos pasos…
Agregar un grupo	1. Haga clic en + Add . 2. Introduzca la información del grupo. 3. Especifique los privilegios. 4. Especificar miembros de grupo (agregar usuarios locales, usuarios de dominio o grupos de dominio).
Editar un grupo	1. Junto al nombre del grupo, haga clic en ⋮ y, a continuación, haga clic en **Editar**. 2. Modifique la información del grupo.
Eliminar un grupo	1. Marque la casilla situada junto al grupo o grupos que desee eliminar. 2. Haga clic en Delete . **Nota:** También puede eliminar un solo grupo haciendo clic ⋮ junto al nombre del grupo y luego haciendo clic en **Eliminar**.

Administrar usuarios de Windows

En System Manager, puede gestionar usuarios de Windows añadiendo, editando, eliminando, habilitando o deshabilitando. También puede cambiar la contraseña de un usuario de Windows.

Pasos

1. En System Manager, puede ver la lista de usuarios del grupo. Consulte Ver usuarios y grupos de Windows.
2. En la ficha **usuarios**, puede administrar usuarios con las siguientes tareas:

Para realizar esta acción…	Realice estos pasos…
Agregar un usuario	1. Haga clic en + Add . 2. Introduzca la información del usuario.
Editar un usuario	1. Junto al nombre de usuario, haga clic en ⋮ y, a continuación, haga clic en **Editar**. 2. Modifique la información del usuario.

Eliminar un usuario	1. Active la casilla situada junto al usuario o usuarios que desee eliminar. 2. Haga clic en Delete . **Nota:** También puede eliminar un solo usuario haciendo clic junto al nombre de usuario y luego haciendo clic en **Eliminar**.
Cambiar contraseña de usuario	1. Junto al nombre de usuario, haga clic en y, a continuación, haga clic en **Cambiar contraseña**. 2. Introduzca la nueva contraseña y confírmela.
Habilitar un usuario	1. Marque la casilla situada junto a cada usuario deshabilitado que desee activar. 2. Haga clic en Enable .
Desactivar usuarios	1. Marque la casilla junto a cada usuario habilitado que desee deshabilitar. 2. Haga clic en Disable .

Ver usuarios y grupos UNIX

En System Manager, puede ver una lista de usuarios y grupos de UNIX.

Pasos

1. En System Manager, haga clic en **almacenamiento > Storage VMs**.
2. Seleccione el equipo virtual de almacenamiento y, a continuación, seleccione la ficha **Configuración**.
3. Desplácese hasta el área **usuarios de host y grupos**.

   La sección **UNIX** muestra un resumen del número de usuarios de cada grupo asociado al VM de almacenamiento seleccionado.

4. Haga clic en la sección **unix**.
5. Haga clic en la ficha **grupos** para ver los detalles de ese grupo.
6. Para ver los usuarios de un grupo, seleccione el grupo y, a continuación, haga clic en la ficha **usuarios**.

Agregar, editar o eliminar un grupo UNIX

En System Manager, puede gestionar grupos UNIX agregándolos, editánéndolos o eliminarlos.

Pasos

1. En System Manager, consulte la lista de grupos UNIX. Consulte Ver usuarios y grupos UNIX.
2. En la ficha **grupos**, puede administrar grupos con las siguientes tareas:

Para realizar esta acción…	Realice estos pasos…

Agregar un grupo	1. Haga clic en + Add . 2. Introduzca la información del grupo. 3. (Opcional) indique los usuarios asociados.
Editar un grupo	1. Seleccione el grupo. 2. Haga clic en Edit . 3. Modifique la información del grupo. 4. (Opcional) Añada o elimine usuarios.
Eliminar un grupo	1. Seleccione el grupo o los grupos que desea eliminar. 2. Haga clic en Delete .

Gestionar usuarios UNIX

En System Manager, puede gestionar usuarios de Windows añadiendo, editando o eliminando usuarios.

Pasos

1. En System Manager, puede ver la lista de usuarios del grupo. Consulte Ver usuarios y grupos UNIX.
2. En la ficha **usuarios**, puede administrar usuarios con las siguientes tareas:

Para realizar esta acción…	Realice estos pasos…
Agregar un usuario	1. Haga clic en + Add . 2. Introduzca la información del usuario.
Editar un usuario	1. Seleccione el usuario que desea editar. 2. Haga clic en Edit . 3. Modifique la información del usuario.
Eliminar un usuario	1. Seleccione el usuario o los usuarios que desee eliminar. 2. Haga clic en Delete .

Supervisar clientes NFS activos con ONTAP System Manager

A partir de ONTAP 9.8, System Manager muestra qué conexiones de cliente NFS están activas cuando se otorga una licencia para NFS en un clúster.

Esto le permite verificar rápidamente qué clientes NFS se conectan de forma activa con una máquina virtual de almacenamiento, que está conectada pero inactiva, y que está desconectada.

Para cada dirección IP del cliente NFS, la pantalla **clientes NFS** muestra: * Hora del último acceso * Dirección IP de la interfaz de red * Versión de la conexión NFS * Nombre del equipo virtual de almacenamiento

Además, una lista de clientes NFS activos en las últimas 48 horas también se muestra en la pantalla **Storage>Volumes** y un recuento de clientes NFS se incluye en la pantalla **Dashboard**.

Paso

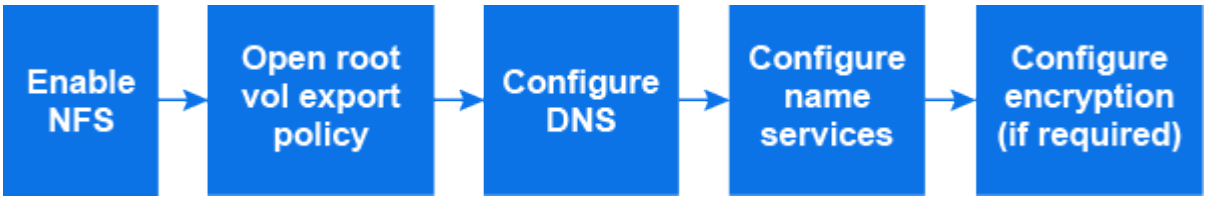
1. Mostrar la actividad del cliente NFS: Haga clic en **hosts > clientes NFS**.

Habilitar el almacenamiento NAS

Habilite el almacenamiento NAS para servidores Linux mediante NFS con ONTAP System Manager

Crear o modificar equipos virtuales de almacenamiento para permitir que los servidores NFS sirva datos a clientes Linux.

Habilite una máquina virtual de almacenamiento nueva o existente para el protocolo NFS mediante este procedimiento.



Antes de empezar

Asegúrese de haber anotado los detalles de configuración de los servicios de red, autenticación o seguridad necesarios en su entorno.

Pasos

1. Activación de NFS en una máquina virtual de almacenamiento.
   - Para nuevas máquinas virtuales de almacenamiento: Haga clic en **Almacenamiento > Storage VMs**, haga clic en **Add**, introduzca un nombre de VM de almacenamiento y, en la pestaña **SMB/CIFS, NFS, S3**, seleccione **Enable NFS**.
     i. Confirme el idioma predeterminado.
     ii. Agregue interfaces de red.
     iii. Actualizar la información de cuenta del administrador de máquinas virtuales de almacenamiento (opcional).
   - Para VM de almacenamiento existentes: Haga clic en **Almacenamiento > VM de almacenamiento**, seleccione una VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en **NFS**.
2. Abra la política de exportación del volumen raíz del equipo virtual de almacenamiento:
   a. Haga clic en **almacenamiento > volúmenes**, seleccione el volumen raíz de la VM de almacenamiento (que por defecto es *volume-name* _root) y, a continuación, haga clic en la directiva que aparece en **Política de exportación**.
   b. Haga clic en **Agregar** para agregar una regla.
      - Especificación del cliente = `0.0.0.0/0`
      - Protocolos de acceso = NFS
      - Detalles de acceso = solo lectura para UNIX
3. Configure DNS para la resolución de nombres de host: Haga clic en **Almacenamiento > VM de**

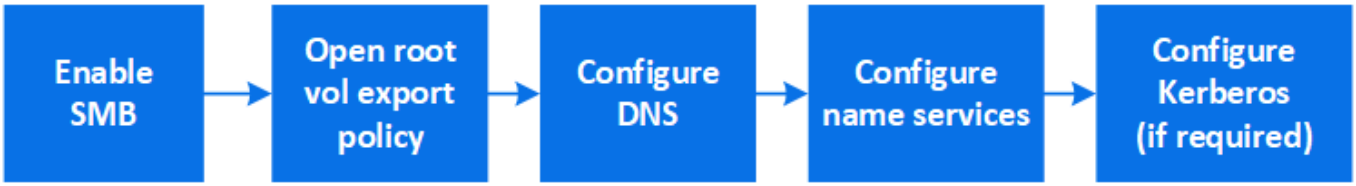
almacenamiento, seleccione la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en **DNS**.

4. Configure los servicios de nombres como corresponda.
   a. Haga clic en **Almacenamiento > Storage VMs**, seleccione la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en LDAP o NIS.
   b. Haga clic en en el icono Cambio de servicios de nombres para incluir cualquier cambio.
5. Configure Kerberos si es necesario:
   a. Haga clic en **almacenamiento > Storage VMs**, seleccione la VM de almacenamiento y, a continuación, haga clic en **Configuración**.
   b. Haga clic en el mosaico Kerberos y luego haga clic en **Agregar**.

Habilite el almacenamiento NAS para servidores Windows mediante SMB con ONTAP System Manager

Cree o modifique máquinas virtuales de almacenamiento para permitir que los servidores SMB sirviendo datos a clientes Windows.

Este procedimiento habilita una máquina virtual de almacenamiento nueva o existente para el protocolo SMB. Se asume que los detalles de la configuración están disponibles para cualquier servicio de red, autenticación o seguridad que requiera el entorno.



Pasos

1. Activación de SMB en una máquina virtual de almacenamiento.
   a. Para los nuevos equipos virtuales de almacenamiento: Haga clic en **almacenamiento > Storage VMs**, haga clic en **Agregar**, escriba un nombre de VM de almacenamiento y, en la ficha **SMB/CIFS, NFS, S3**, seleccione **Activar SMB/CIFS**.
      - Introduzca la siguiente información:
        - Nombre y contraseña del administrador
        - Nombre del servidor
        - Dominio de Active Directory
      - Confirme la unidad organizativa.
      - Confirme los valores DNS.
      - Confirme el idioma predeterminado.
      - Agregue interfaces de red.
      - Actualizar la información de cuenta del administrador de máquinas virtuales de almacenamiento (opcional).
   b. Para VM de almacenamiento existentes: Haga clic en **Almacenamiento > VM de almacenamiento**, seleccione una VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en **SMB**.
2. Abra la política de exportación del volumen raíz del equipo virtual de almacenamiento:

a. Haga clic en **almacenamiento > volúmenes**, seleccione el volumen raíz de la VM de almacenamiento (que por defecto es *volume-name_root*) y, a continuación, haga clic en la directiva que aparece en **Política de exportación**.

b. Haga clic en **Agregar** para agregar una regla.

- Especificación del cliente = `0.0.0.0/0`
- Protocolos de acceso = bloque de mensajes del servidor
- Detalles de acceso = solo lectura para NTFS

3. Configure DNS para la resolución de nombres de host:

a. Haga clic en **Almacenamiento > Storage VMs**, seleccione la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en **DNS**.

b. Cambie al servidor DNS y asigne el servidor SMB.

- Cree entradas de búsqueda hacia delante (a - Registro de dirección) e inversa (PTR - Registro de puntero) para asignar el nombre del servidor SMB a la dirección IP de la interfaz de red de datos.
- Si utiliza alias NetBIOS, cree una entrada de búsqueda de nombre canónico (registro de recursos CNAME) de alias para asignar cada alias a la dirección IP de la interfaz de red de datos del servidor SMB.

4. Configure los servicios de nombres como corresponda

a. Haga clic en **Almacenamiento > Storage VMs**, seleccione la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en **LDAP** o **NIS**.

b. Incluya cualquier cambio en el archivo de cambio de servicios de nombres: Haga clic en **Cambio de servicios de nombres**.

5. Configure Kerberos si es necesario:

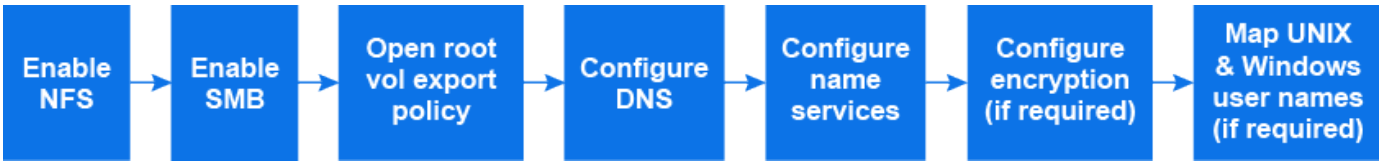
a. Haga clic en **almacenamiento > Storage VMs**, seleccione la VM de almacenamiento y, a continuación, haga clic en **Configuración**.

b. Haga clic en **Kerberos** y luego haga clic en **Agregar**.

Habilite el almacenamiento NAS para Windows y Linux usando NFS y SMB con ONTAP System Manager

Crear o modificar máquinas virtuales de almacenamiento para permitir que los servidores NFS y SMB proporcionen datos a clientes de Linux y Windows.

Habilite una máquina virtual de almacenamiento nueva o existente para que sirva los protocolos NFS y SMB mediante este procedimiento.



Antes de empezar

Asegúrese de haber anotado los detalles de configuración de los servicios de red, autenticación o seguridad necesarios en su entorno.

Pasos

1. Habilite NFS y SMB en una máquina virtual de almacenamiento.

a. Para los nuevos equipos virtuales de almacenamiento: Haga clic en **almacenamiento > Storage VMs**, haga clic en **Agregar**, escriba el nombre de un equipo virtual de almacenamiento y, en la ficha **SMB/CIFS, NFS, S3**, seleccione **Activar SMB/CIFS** y **Activar NFS**.

b. Introduzca la siguiente información:

- Nombre y contraseña del administrador
- Nombre del servidor
- Dominio de Active Directory

c. Confirme la unidad organizativa.

d. Confirme los valores DNS.

e. Confirme el idioma predeterminado.

f. Agregue interfaces de red.

g. Actualizar la información de cuenta del administrador de máquinas virtuales de almacenamiento (opcional).

h. Para las VM de almacenamiento existentes: Haga clic en **almacenamiento > Storage VMs**, seleccione una VM de almacenamiento y, a continuación, haga clic en **Configuración**. Complete los siguientes subpasos si NFS o SMB todavía no está habilitado.

- Haga clic en **nfs**.
- Haga clic en **SMB**.

2. Abra la política de exportación del volumen raíz del equipo virtual de almacenamiento:

a. Haga clic en **almacenamiento > volúmenes**, seleccione el volumen raíz de la VM de almacenamiento (que por defecto es *volume-name_root*) y, a continuación, haga clic en la directiva que aparece en **Política de exportación**.

b. Haga clic en **Agregar** para agregar una regla.

- Especificación del cliente = `0.0.0.0/0`
- Protocolos de acceso = NFS
- Detalles de acceso = solo lectura para NFS

3. Configure DNS para la resolución de nombres de host:

a. Haga clic en **Almacenamiento > Storage VMs**, seleccione la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en **DNS**.

b. Cuando se complete la configuración de DNS, cambie al servidor DNS y asigne el servidor SMB.

- Cree entradas de búsqueda hacia delante (a - Registro de dirección) e inversa (PTR - Registro de puntero) para asignar el nombre del servidor SMB a la dirección IP de la interfaz de red de datos.
- Si utiliza alias NetBIOS, cree una entrada de búsqueda de nombre canónico (registro de recursos CNAME) de alias para asignar cada alias a la dirección IP de la interfaz de red de datos del servidor SMB.

4. Configure los servicios de nombres según sea necesario:

a. Haga clic en **Almacenamiento > Storage VMs**, seleccione la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en LDAP o NIS.

b. Incluya cualquier cambio en el archivo de cambio de servicios de nombres: Haga clic en **Cambio de servicios de nombres**.

5. Configure Kerberos si es necesario:

a. Haga clic en **almacenamiento > Storage VMs**, seleccione la VM de almacenamiento y, a continuación, haga clic en **Configuración**.

b. Haga clic en → el mosaico Kerberos y luego haga clic en **Agregar**.

6. Asignar nombres de usuario de UNIX y Windows si es necesario: Haga clic en → **Asignación de nombre** y luego haga clic en **Agregar**.

   Debe hacer esto solo si su sitio tiene cuentas de usuario de Windows y UNIX que no se asignan implícitamente, que es cuando la versión en minúscula de cada nombre de usuario de Windows coincide con el nombre de usuario de UNIX. Puede asignar nombres de usuario con usuarios LDAP, NIS o locales. Si tiene dos conjuntos de usuarios que no coinciden, debe configurar la asignación de nombres.

Configurar NFS

Obtenga información sobre la configuración de NFS con la CLI de ONTAP

Puede usar comandos de la CLI de ONTAP 9 para configurar el acceso del cliente de NFS a los archivos ubicados en un volumen o un qtree de una máquina virtual de almacenamiento (SVM) nueva o existente.

Use estos procedimientos si desea configurar el acceso a un volumen o qtree de la siguiente forma:

- Desea utilizar cualquier versión de NFS compatible actualmente con ONTAP: NFSv3, NFSv4, NFSv4.1, NFSv4.2 o NFSv4.1 con pNFS.
- Desea usar la interfaz de línea de comandos (CLI), no System Manager ni una herramienta de secuencias de comandos automatizadas.

  Para utilizar System Manager para configurar el acceso multiprotocolo NAS, consulte "Aprovisione almacenamiento NAS para Windows y Linux usando NFS y SMB".

- Quiere utilizar las prácticas recomendadas, no explorar todas las opciones disponibles.

  Obtenga más información sobre la sintaxis de comandos en el "Referencia de comandos del ONTAP".

- Se utilizarán permisos de archivo UNIX para proteger el nuevo volumen.
- Tiene privilegios de administrador de clúster, no de administrador de SVM.

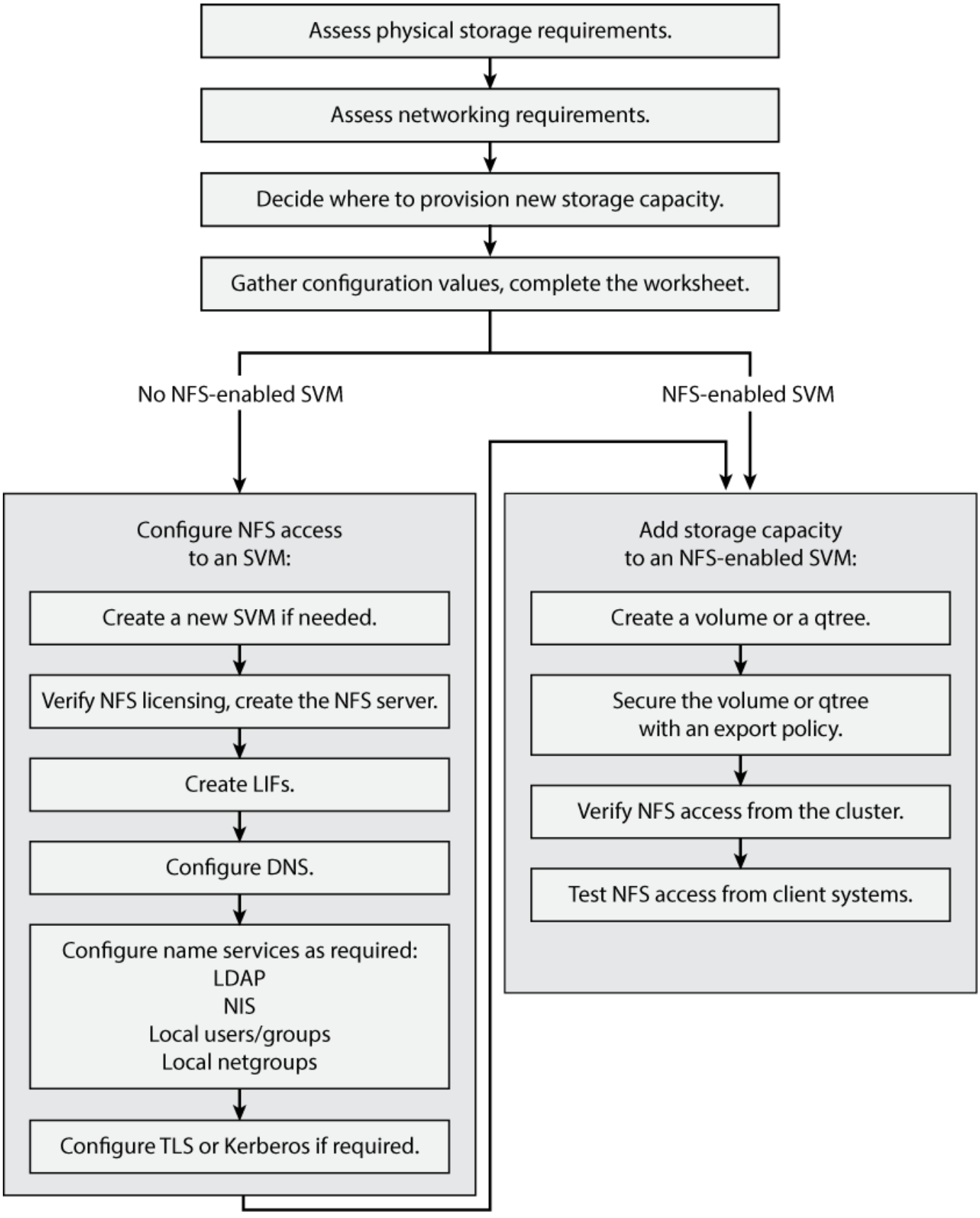
Si desea obtener más información sobre la gama de capacidades del protocolo NFS de ONTAP, consulte la "Obtenga información sobre el acceso a archivos ONTAP para el protocolo NFS".

Otras maneras de hacerlo en ONTAP

Para ejecutar estas tareas con…	Consulte…
System Manager rediseñado (disponible con ONTAP 9.7 y versiones posteriores)	"Aprovisionar almacenamiento NAS para servidores Linux mediante NFS"
System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores)	"Información general de la configuración DE NFS"

Obtenga más información sobre el flujo de trabajo de configuración de NFS de ONTAP

La configuración de NFS implica la evaluación de los requisitos de almacenamiento físico y de red, y la selección de un flujo de trabajo específico para el objetivo; entre otras, la configuración del acceso NFS a una SVM nueva o existente, o la adición de un volumen o un qtree a una SVM existente que ya esté completamente configurada para el acceso NFS.



Preparación

Evaluar los requisitos de almacenamiento físico de ONTAP NFS

Antes de aprovisionar almacenamiento de NFS para clientes, debe asegurarse de que haya espacio suficiente en un agregado existente para el nuevo volumen. Si no lo hay, puede añadir discos a un agregado existente o crear uno nuevo con el tipo deseado.

Pasos

1. Mostrar el espacio disponible en los agregados existentes:

   ```
   storage aggregate show
   ```

   Si hay un agregado con suficiente espacio, registre su nombre en la hoja de cálculo.

   ```
   cluster::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
   --------- -------- --------- ----- ------- ------ ------ -----------
   aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                             normal
   aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                             normal
   6 entries were displayed.
   ```

2. Si no hay agregados con espacio suficiente, añada discos a un agregado existente mediante `storage aggregate add-disks` el comando o cree un agregado nuevo mediante el `storage aggregate create` comando.

Información relacionada

- "Añadir discos a un nivel local (agregado)"
- "agregado de almacenamiento, agregar discos"
- "creación de agregados de almacenamiento"

Evaluar los requisitos de configuración de la red NFS de ONTAP

Antes de proporcionar almacenamiento NFS a los clientes, debe comprobar que las redes se han configurado correctamente para cumplir los requisitos de aprovisionamiento de NFS.

Antes de empezar

Deben configurarse los siguientes objetos de red de clúster:

- Puertos físicos y lógicos
- Dominios de retransmisión
- Subredes (si es necesario)
- Espacios IP (según se requiera, además del espacio IP predeterminado)
- Grupos de conmutación por error (según sea necesario, además del grupo de conmutación por error predeterminado para cada dominio de retransmisión).
- Firewalls externos

Pasos

1. Mostrar los puertos físicos y virtuales disponibles:

   `network port show`

   - Cuando sea posible, debe utilizar el puerto con la velocidad más alta para la red de datos.
   - Todos los componentes de la red de datos deben tener la misma configuración de MTU para obtener el mejor rendimiento.
   - Obtenga más información sobre `network port show` en el "Referencia de comandos del ONTAP".

2. Si tiene pensado utilizar un nombre de subred para asignar la dirección IP y el valor de máscara de red para una LIF, compruebe que la subred existe y que tenga suficientes direcciones disponibles: +

   `network subnet show`

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

   Las subredes contienen un grupo de direcciones IP que pertenecen a la misma subred de capa 3. Las subredes se crean con `network subnet create` el comando.

   Obtenga más información sobre `network subnet create` en el "Referencia de comandos del ONTAP".

3. Mostrar espacios IP disponibles:

   `network ipspace show`

   Puede usar el espacio IP predeterminado o un espacio IP personalizado.

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

4. Si desea usar direcciones IPv6, compruebe que IPv6 esté habilitado en el clúster:

   `network options ipv6 show`

   Si es necesario, puede habilitar IPv6 con `network options ipv6 modify` el comando.

   Obtenga más información sobre `network options ipv6 show` y `network options ipv6 modify` en el "Referencia de comandos del ONTAP".

Obtenga más información sobre el aprovisionamiento de capacidad de almacenamiento NFS de ONTAP

Antes de crear un volumen o qtree de NFS nuevo, debe decidir si colocarlo en una SVM nueva o existente y cuánta configuración requiere la SVM. Esta decisión determina su flujo de trabajo.

Opciones

- Si desea aprovisionar un volumen o qtree en una SVM nueva o en una SVM existente con NFS habilitado pero no configurado, complete los pasos de "Configuración del acceso NFS a una SVM" y "adición de almacenamiento NFS a una SVM habilitada para NFS".

  Configure el acceso de NFS a una SVM

  Añada almacenamiento NFS a una SVM habilitada para NFS

  Puede optar por crear una nueva SVM si se cumple alguna de las siguientes condiciones:

  - Debe habilitar NFS en un clúster por primera vez.
  - Tiene SVM existentes en un clúster en el cual no desea habilitar la compatibilidad con NFS.
  - Tiene una o varias SVM habilitadas para NFS en un clúster y desea otro servidor NFS en un espacio de nombres aislado (escenario multi-tenancy). También debe elegir esta opción para aprovisionar almacenamiento en una SVM existente con NFS habilitado pero sin configurar. Este puede ser el caso si se creó la SVM para el acceso SAN o si no se habilitó ningún protocolo cuando se creó la SVM.

  Después de habilitar NFS en la SVM, continúe aprovisionando un volumen o un qtree.

- Si desea aprovisionar un volumen o un qtree en una SVM existente que esté completamente configurada para el acceso NFS, complete los pasos descritos en "Cómo añadir almacenamiento NFS a una SVM habilitada para NFS".

  Adición de almacenamiento NFS a una SVM habilitada para NFS

Hoja de datos de configuración de NFS de ONTAP

La hoja de datos de configuración de NFS permite recopilar la información necesaria para configurar el acceso NFS para clientes.

Debe rellenar una o ambas secciones de la hoja de datos en función de la decisión que haya tomado sobre dónde aprovisionar almacenamiento:

Si va a configurar el acceso NFS a una SVM, debe completar ambas secciones.

- Configurar el acceso de NFS a una SVM
- Se añade capacidad de almacenamiento a una SVM habilitada para NFS

Si va a añadir capacidad de almacenamiento a una SVM habilitada para NFS, solo debe completar:

- Se añade capacidad de almacenamiento a una SVM habilitada para NFS

Parámetros para crear una SVM

Debe proporcionar estos valores con `vserver create` el comando si va a crear una SVM nueva.

Campo	Descripción	Su valor
`-vserver`	Un nombre que se proporciona para la SVM nueva que es un nombre de dominio completo (FQDN) o sigue otra convención que aplica nombres de SVM únicos en un clúster.	
`-aggregate`	El nombre de un agregado en el clúster con espacio suficiente para la nueva capacidad de almacenamiento de NFS.	
`-rootvolume`	Un nombre único que se proporciona para el volumen raíz de SVM.	
`-rootvolume-security-style`	Utilice el estilo de seguridad UNIX para la SVM.	`unix`
`-language`	Utilice la configuración de idioma predeterminada en este flujo de trabajo.	`C.UTF-8`
`ipspace`	Los espacios IP son espacios de direcciones IP distintos en los que residen (máquinas virtuales de almacenamiento (SVM).	

Parámetros para crear un servidor NFS

Debe proporcionar estos valores con el `vserver nfs create` comando al crear un nuevo servidor NFS y especificar versiones NFS compatibles.

Si habilita NFSv4 o posterior, debe utilizar LDAP para mejorar la seguridad.

Campo	Descripción	Su valor

`-v3`, `-v4.0`, `-v4.1`, , `-v4.1 -pnfs`	Habilite las versiones de NFS según sea necesario. v4,2 también es compatible con ONTAP 9.8 y posterior cuando `v4.1` está activado.	
`-v4-id-domain`	ID asignando nombre de dominio.	
`-v4-numeric-ids`	Compatibilidad con ID de propietario numéricos (activado o desactivado).	

Parámetros para crear una LIF

Proporcione estos valores con `network interface create` el comando cuando cree las LIF. Obtenga más información sobre `network interface create` en el "Referencia de comandos del ONTAP".

Si utiliza Kerberos, debe habilitar Kerberos en varias LIF.

Campo	Descripción	Su valor
`-lif`	Nombre que se proporciona para la nueva LIF.	
`-role`	Utilice el rol de LIF de datos en este flujo de trabajo.	`data`
`-data-protocol`	Utilice solo el protocolo NFS en este flujo de trabajo.	`nfs`
`-home-node`	El nodo al que devuelve la LIF cuando `network interface revert` se ejecuta el comando en la LIF. Obtenga más información sobre `network interface revert` en el "Referencia de comandos del ONTAP".	
`-home-port`	El puerto o grupo de interfaces al que devuelve la LIF cuando `network interface revert` se ejecuta el comando en la LIF.	

`-address`	La dirección IPv4 o IPv6 del clúster que se usará para el acceso a los datos mediante la nueva LIF.	
`-netmask`	La máscara de red y la puerta de enlace para la LIF.	
`-subnet`	Un conjunto de direcciones IP. Se utiliza en lugar de `-address` y `-netmask` para asignar direcciones y máscaras de red automáticamente.	
`-firewall-policy`	Utilice la política de firewall de datos predeterminada en este flujo de trabajo.	`data`

Parámetros para la resolución del nombre de host DNS

Proporcione estos valores con `vserver services name-service dns create` el comando cuando configura DNS.

Campo	Descripción	Su valor
`-domains`	Hasta cinco nombres de dominio DNS.	
`-name-servers`	Hasta tres direcciones IP para cada servidor de nombres DNS.	

Información del servicio de nombres

Parámetros para crear usuarios locales

Debe proporcionar estos valores si está creando usuarios locales mediante el `vserver services name-service unix-user create` comando. Si va a configurar usuarios locales cargando un archivo que contiene usuarios UNIX de un identificador de recursos uniforme (URI), no es necesario especificar estos valores manualmente.

	Nombre de usuario `(-user)`	ID de usuario `(-id)`	ID de grupo `(-primary-gid)`	Nombre completo `(-full-name)`
Ejemplo	javier martínez	123	100	John Miller
1				
2				

3				
…				
n				

Parámetros para crear grupos locales

Proporcione estos valores si está creando grupos locales mediante el `vserver services name-service unix-group create` comando. Si va a configurar grupos locales cargando un archivo que contiene grupos UNIX de un URI, no es necesario especificar estos valores manualmente.

	Nombre del grupo (`-name`)	ID Grupo (`-id`)
Ejemplo	Ingeniería	100
1		
2		
3		
…		
n		

Parámetros para NIS

Proporcione estos valores con el `vserver services name-service nis-domain create` comando.

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

Campo	Descripción	Su valor
`-domain`	El dominio NIS que utilizará la SVM para las búsquedas de nombres.	
`-active`	El servidor de dominio NIS activo.	`true` o. `false`
`-nis-servers`	Una lista separada por comas de direcciones IP y nombres de host para los servidores NIS utilizados por la configuración del dominio.	

Parámetros para LDAP

Proporcione estos valores con el `vserver services name-service ldap client create` comando.

También se necesita `.pem` un archivo de certificado de CA raíz autofirmado.

Campo	Descripción	Su valor
`-vserver`	El nombre de la SVM para la cual se creará la configuración de cliente LDAP.	
`-client-config`	El nombre que se asigna para la nueva configuración de cliente LDAP.	
`-ldap-servers`	Lista separada por comas de direcciones IP y nombres de host para los servidores LDAP.	
`-query-timeout`	Utilice los `3` segundos predeterminados para este flujo de trabajo.	`3`
`-min-bind-level`	El nivel de autenticación de enlace mínimo. El valor predeterminado es `anonymous`. Debe establecerse en `sasl` si la firma y el sellado están configuradas.	
`-preferred-ad-servers`	Uno o varios servidores de Active Directory preferidos por dirección IP en una lista delimitada por comas.	
`-ad-domain`	El dominio de Active Directory.	
`-schema`	La plantilla de esquema que se va a utilizar. Puede utilizar un esquema predeterminado o personalizado.	
`-port`	Utilice el puerto del servidor LDAP predeterminado `389` para este flujo de trabajo.	`389`
`-bind-dn`	El nombre distintivo del usuario Bind.	
`-base-dn`	El nombre distintivo de la base. El valor por defecto es `""` (root).	

Campo	Descripción	Su valor
`-base-scope`	Utilice el ámbito de búsqueda base por defecto `subnet` para este flujo de trabajo.	`subnet`
`-session-security`	Habilita la firma, firma y sellado LDAP. El valor predeterminado es `none`.	
`-use-start-tls`	Habilita LDAP sobre TLS. El valor predeterminado es `false`.	

Parámetros para la autenticación Kerberos

Proporcione estos valores con el `vserver nfs kerberos realm create` comando. Algunos de los valores variarán dependiendo de si utiliza Microsoft Active Directory como servidor de Key Distribution Center (KDC), o MIT u otro servidor UNIX KDC.

Campo	Descripción	Su valor
`-vserver`	La SVM que se comunicará con el KDC.	
`-realm`	El dominio Kerberos.	
`-clock-skew`	Desfase de reloj permitido entre clientes y servidores.	
`-kdc-ip`	Dirección IP de KDC.	
`-kdc-port`	Número de puerto KDC.	
`-adserver-name`	Sólo Microsoft KDC: Nombre DEL servidor DE ANUNCIOS.	
`-adserver-ip`	Sólo Microsoft KDC: Dirección IP del servidor DE ANUNCIOS.	
`-adminserver-ip`	Sólo UNIX KDC: Dirección IP del servidor de administración.	
`-adminserver-port`	Sólo UNIX KDC: Número de puerto del servidor de administración.	
`-passwordserver-ip`	Sólo UNIX KDC: Dirección IP del servidor de contraseñas.	

`-passwordserver-port`	Sólo UNIX KDC: Puerto del servidor de contraseñas.	
`-kdc-vendor`	Proveedor KDC.	{ `Microsoft`
`Other` }	`-comment`	Cualquier comentario deseado.

Proporcione estos valores con el `vserver nfs kerberos interface enable` comando.

Campo	Descripción	Su valor
`-vserver`	El nombre de la SVM para la cual desea crear una configuración de Kerberos.	
`-lif`	La LIF de datos en la que activará Kerberos. Puede habilitar Kerberos en varias LIF.	
`-spn`	El nombre del principio de servicio (SPN)	
`-permitted-enc-types`	`` `aes-256`Se recomiendan los tipos de cifrado permitidos para Kerberos sobre NFS;, según las capacidades del cliente. ``	
`-admin-username`	Las credenciales de administrador de KDC para recuperar la clave secreta SPN directamente del KDC. Se requiere una contraseña	
`-keytab-uri`	El archivo keytab del KDC que contiene la clave SPN si no tiene credenciales de administrador KDC.	
`-ou`	La unidad organizativa (OU) en la que se creará la cuenta de servidor de Microsoft Active Directory al habilitar Kerberos mediante un Reino para Microsoft KDC.	

Parámetros para crear políticas y reglas de exportación

Proporcione estos valores con el `vserver export-policy create` comando.

Campo	Descripción	Su valor
`-vserver`	El nombre de la SVM que alojará el nuevo volumen.	
`-policyname`	Nombre que se proporciona para una nueva política de exportación.	

Proporcione estos valores para cada regla con el `vserver export-policy rule create` comando.

Campo	Descripción	Su valor
`-clientmatch`	Especificación de coincidencia del cliente.	
`-ruleindex`	Posición de la regla de exportación en la lista de reglas.	
`-protocol`	Utilice NFS en este flujo de trabajo.	`nfs`
`-rorule`	Método de autenticación de acceso de solo lectura.	
`-rwrule`	Método de autenticación para acceso de lectura/escritura.	
`-superuser`	Método de autenticación para acceso de superusuario.	
`-anon`	ID de usuario al que se asignan usuarios anónimos.	

Debe crear una o varias reglas para cada política de exportación.

`-ruleindex`	**`-clientmatch`**	**`-rorule`**	**`-rwrule`**	**`-superuser`**	**`-anon`**
Ejemplos	0.0.0.0/0,@roota ccess_netgroup	cualquiera	krb5	act	65534
1					
2					

3					
…					
n					

Parámetros para crear un volumen

Debe introducir estos valores con `volume create` el comando si va a crear un volumen en lugar de un qtree.

Campo	Descripción	Su valor
`-vserver`	El nombre de una SVM nueva o existente que alojará el nuevo volumen.	
`-volume`	Se suministra un nombre descriptivo único para el volumen nuevo.	
`-aggregate`	El nombre de un agregado en el clúster de con espacio suficiente para el nuevo volumen de NFS.	
`-size`	Se proporciona un entero para el tamaño del nuevo volumen.	
`-user`	Nombre o ID del usuario que se establece como el propietario de la raíz del volumen.	
`-group`	Nombre o ID del grupo que se establece como el propietario de la raíz del volumen.	
`--security-style`	Utilice el estilo de seguridad UNIX para este flujo de trabajo.	`unix`
`-junction-path`	Ubicación bajo la raíz (/) donde se va a montar el nuevo volumen.	
`-export-policy`	Si tiene pensado utilizar una política de exportación existente, puede introducir su nombre al crear el volumen.	

Parámetros para crear un qtree

Debe proporcionar estos valores con `volume qtree create` el comando si va a crear un qtree en lugar de un volumen.

Campo	Descripción	Su valor
`-vserver`	El nombre de la SVM en la que reside el volumen que contiene el qtree.	
`-volume`	El nombre del volumen que contendrá el nuevo qtree.	
`-qtree`	Nombre descriptivo único que se proporciona para el nuevo qtree, con 64 caracteres o menos.	
`-qtree-path`	El argumento de la ruta de qtree en el formato `/vol/volume_name/qtree_name\>` se puede especificar en lugar de especificar el volumen y el qtree como argumentos independientes.	
`-unix-permissions`	Optional: Los permisos de UNIX para el qtree.	
`-export-policy`	Si tiene pensado usar una política de exportación existente, puede introducir su nombre al crear el qtree.	

Información relacionada

- "Referencia de comandos del ONTAP"

Configure el acceso de NFS a una SVM

Crear SVM de ONTAP para el acceso a datos NFS

Si no tiene al menos una SVM en un clúster para proporcionar acceso a los datos a los clientes de NFS, debe crear una.

Antes de empezar

- A partir de ONTAP 9.13.1, puede establecer una capacidad máxima para una máquina virtual de almacenamiento. También puede configurar alertas cuando la SVM se acerca a un nivel de umbral de capacidad. Para obtener más información, consulte Gestionar la capacidad de SVM.

Pasos

1. Cree una SVM:

```
vserver create -vserver vserver_name -rootvolume root_volume_name -aggregate
```

aggregate_name -rootvolume-security-style unix -language C.UTF-8 -ipspace *ipspace_name*

- Utilice la configuración de UNIX para `-rootvolume-security-style` la opción.
- Utilice `-language` la opción predeterminada C.UTF-8.
- `ipspace`El ajuste es opcional.

2. Compruebe la configuración y el estado de la SVM recién creada:

vserver show -vserver *vserver_name*

`Allowed Protocols`El campo debe incluir NFS. Puede editar esta lista más tarde.

`Vserver Operational State`El campo debe mostrar `running` el estado. Si muestra `initializing` el estado, significa que se produjo un error en alguna operación intermedia como la creación del volumen raíz, y debe eliminar la SVM y volver a crearla.

Ejemplos

El siguiente comando crea una SVM para acceder a los datos en el espacio IP ipspaceA:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

El siguiente comando muestra que una SVM se creó con un volumen raíz de 1 GB, y se inició automáticamente y está `running` en estado. El volumen raíz tiene una política de exportación predeterminada que no incluye reglas, por lo que el volumen raíz no se exporta tras la creación.

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                               Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                         Vserver Admin State: running
                   Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

A partir de ONTAP 9.13.1, puede establecer una plantilla de grupo de políticas de calidad de servicio adaptativa, aplicando un límite máximo y mínimo de rendimiento a los volúmenes en la SVM. Solo puede aplicar esta política después de crear la SVM. Para obtener más información sobre este proceso, consulte Defina una plantilla de grupo de políticas adaptativas.

Verificar la habilitación del protocolo NFS en ONTAP SVM

Antes de poder configurar y utilizar NFS en las SVM, debe comprobar que el protocolo esté habilitado.

Acerca de esta tarea

Esto suele realizarse durante la configuración de la SVM, pero si no habilitó el protocolo durante la configuración, puede habilitarlo más adelante mediante `vserver add-protocols` el comando.

Una vez creado, no puede agregar ni quitar un protocolo de una LIF.

También puede deshabilitar los protocolos en las SVM con `vserver remove-protocols` el comando.

Pasos

1. Compruebe qué protocolos están habilitados y deshabilitados actualmente para la SVM:

```
vserver show -vserver vserver_name -protocols
```

También puede utilizar el `vserver show-protocols` comando para ver los protocolos habilitados actualmente en todas las SVM del clúster.

2. Si es necesario, habilite o deshabilite un protocolo:
   - Para habilitar el protocolo NFS:
     `vserver add-protocols -vserver vserver_name -protocols nfs`
   - Para desactivar un protocolo:
     `vserver remove-protocols -vserver vserver_name -protocols protocol_name [,protocol_name,…]`
3. Confirme que los protocolos activados y deshabilitados se han actualizado correctamente:

```
vserver show -vserver vserver_name -protocols
```

Ejemplo

El siguiente comando muestra qué protocolos están habilitados y deshabilitados actualmente (permitidos y deshabilitados) en la SVM llamada vs1:

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    -----------------------
vs1.example.com   nfs                       cifs, fcp, iscsi, ndmp
```

El siguiente comando permite el acceso a través de NFS agregando `nfs` a la lista de protocolos habilitados en la SVM llamada VS1:

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

Abrir el acceso del cliente NFS en ONTAP SVM

La política de exportación predeterminada del volumen raíz de la SVM debe incluir una regla para permitir que todos los clientes tengan acceso abierto a través de NFS. Sin esta regla, se deniega el acceso a la SVM y a sus volúmenes a todos los clientes NFS.

Acerca de esta tarea

Cuando se crea una SVM nueva, se crea automáticamente una política de exportación predeterminada (denominada predeterminada) para el volumen raíz de la SVM. Debe crear una o varias reglas para la política de exportación predeterminada para que los clientes puedan acceder a los datos de la SVM.

Debe verificar que el acceso está abierto a todos los clientes NFS de la política de exportación predeterminada y, más adelante, restringir el acceso a volúmenes individuales mediante la creación de políticas de exportación personalizadas para volúmenes o qtrees individuales.

Pasos

1. Si va a utilizar una SVM existente, compruebe la política de exportación de volumen raíz predeterminada:

`vserver export-policy rule show`

El resultado del comando debe ser similar a lo siguiente:

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                    Vserver: vs1.example.com
                                Policy Name: default
                                 Rule Index: 1
                            Access Protocol:  nfs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                             RO Access Rule: any
                             RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                   Superuser Security Types: any
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

Si existe una regla de este tipo que permite el acceso abierto, esta tarea se completa. De lo contrario, continúe con el siguiente paso.

2. Cree una regla de exportación para el volumen raíz de la SVM:

   `vserver export-policy rule create -vserver` *`vserver_name`* `-policyname default -ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`

   Si la SVM solo contendrá volúmenes protegidos por Kerberos, puede establecer las opciones de la regla de exportación `-rorule` , `-rwrule` y `-superuser` para el volumen raíz en `krb5` o `krb5i`. Por ejemplo:

   `-rorule krb5i -rwrule krb5i -superuser krb5i`

3. Verifique la creación de reglas con el `vserver export-policy rule show` comando.

Resultado

Ahora, cualquier cliente de NFS puede acceder a cualquier volumen o qtree creado en la SVM.

Crear servidores NFS de ONTAP

Después de verificar que NFS tiene licencia en el clúster, puede utilizar `vserver nfs create` el comando para crear un servidor NFS en la SVM y especificar las versiones de NFS compatibles.

Acerca de esta tarea

Es posible configurar SVM para que admita una o varias versiones de NFS. Si admite NFSv4 o posteriores:

- El nombre de dominio de asignación del ID de usuario de NFSv4 debe ser igual en el servidor NFSv4 y en los clientes de destino.

No necesariamente debe ser el mismo que un nombre de dominio LDAP o NIS siempre que el servidor NFSv4 y los clientes utilicen el mismo nombre.

- Los clientes de destino deben admitir la configuración de ID numérico de NFSv4.
- Por motivos de seguridad, debe utilizar LDAP para los servicios de nombres en las puestas en marcha de NFSv4.

Antes de empezar

Debe haber configurado la SVM para permitir el protocolo NFS.

Pasos

1. Compruebe que NFS tiene licencia en el clúster:

   ```
   system license show -package nfs
   ```

   Si no lo está, póngase en contacto con su representante de ventas.

2. Cree un servidor NFS:

   ```
   vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0
   {enabled|disabled} -v4-id-domain nfsv4_id_domain -v4-numeric-ids
   {enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
   ```

   Puede optar por habilitar cualquier combinación de versiones de NFS. Si desea ser compatible con pNFS, debe habilitar las dos `-v4.1` opciones y `-v4.1-pnfs`.

   Si activa v4 o posterior, también debe estar seguro de que las siguientes opciones están configuradas correctamente:

   - `-v4-id-domain`

     Este parámetro opcional especifica la parte de dominio del formulario de cadena de nombres de usuario y de grupo, tal como lo define el protocolo NFSv4. De forma predeterminada, ONTAP utiliza el dominio NIS si se establece uno; si no es así, se utiliza el dominio DNS. Debe proporcionar un valor que coincida con el nombre de dominio utilizado por los clientes de destino.

   - `-v4-numeric-ids`

     Este parámetro opcional especifica si la compatibilidad con identificadores de cadena numéricos en los atributos de propietario de NFSv4 está habilitada. La configuración predeterminada está habilitada, pero debe verificar que los clientes de destino lo admitan.

   Puede habilitar funciones adicionales de NFS más adelante con `vserver nfs modify` el comando.

3. Compruebe que NFS está ejecutando:

   ```
   vserver nfs status -vserver vserver_name
   ```

4. Compruebe que NFS está configurado como se desea:

   ```
   vserver nfs show -vserver vserver_name
   ```

Ejemplos

El siguiente comando crea un servidor NFS en la SVM llamada vs1 con NFSv3 y NFSv4.0 habilitado:

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id
-domain my_domain.com
```

Los siguientes comandos verifican el estado y los valores de configuración del nuevo servidor NFS llamado vs1:

```
vs1::> vserver nfs status -vserver vs1
The NFS server is running on Vserver "vs1".

vs1::> vserver nfs show -vserver vs1

                              Vserver: vs1
                    General NFS Access: true
                                NFS v3: enabled
                              NFS v4.0: enabled
                         UDP Protocol: enabled
                         TCP Protocol: enabled
                  Default Windows User: -
                   NFSv4.0 ACL Support: disabled
      NFSv4.0 Read Delegation Support: disabled
     NFSv4.0 Write Delegation Support: disabled
               NFSv4 ID Mapping Domain: my_domain.com
...
```

Crear LIF de ONTAP NFS

Una LIF es una dirección IP asociada con un puerto físico o lógico. Si hay un fallo de un componente, un LIF puede conmutar al respaldo o migrarse a un puerto físico diferente, lo que continúa comunicándose con la red.

Antes de empezar

- El puerto de red físico o lógico subyacente debe haberse configurado en el `up` estado administrativo. Obtenga más información sobre `up` en el "Referencia de comandos del ONTAP".
- Si tiene pensado utilizar un nombre de subred para asignar la dirección IP y el valor de máscara de red para una LIF, la subred ya debe existir.

  Las subredes contienen un grupo de direcciones IP que pertenecen a la misma subred de capa 3. Se crean mediante el `network subnet create` comando.

  Obtenga más información sobre `network subnet create` en el "Referencia de comandos del ONTAP".

- El mecanismo para especificar el tipo de tráfico que maneja una LIF ha cambiado. Para ONTAP 9.5 y versiones anteriores, LIF usaba funciones para especificar el tipo de tráfico que gestionaría. A partir de ONTAP 9.6, los LIF utilizan políticas de servicio para especificar el tipo de tráfico que manejaría.

Acerca de esta tarea

- Puede crear tanto LIF IPv4 como IPv6 en el mismo puerto de red.
- Si utiliza la autenticación de Kerberos, habilite Kerberos en varias LIF.
- Si tiene un gran número de LIF en su clúster, puede comprobar la capacidad de LIF compatible en el clúster mediante `network interface capacity show` el comando y la capacidad de LIF admitida en cada nodo mediante el comando `network interface capacity details show` (en el nivel de privilegio avanzado).

  Obtenga más información sobre `network interface capacity show` y `network interface capacity details show` en el "Referencia de comandos del ONTAP".

- A partir de ONTAP 9.7, si ya existen otras LIF para la SVM en la misma subred, no es necesario especificar el puerto de inicio de la LIF. ONTAP elige automáticamente un puerto aleatorio en el nodo raíz especificado en el mismo dominio de retransmisión que las otras LIF ya configuradas en la misma subred.

A partir de la versión 9.4 de ONTAP, se admite FC-NVMe. Si crea una LIF FC-NVMe, debe tener en cuenta lo siguiente:

- El protocolo NVMe debe ser compatible con el adaptador de FC en el que se crea la LIF.
- FC-NVMe puede ser el único protocolo de datos en las LIF de datos.
- Debe configurarse un LIF que gestiona el tráfico de gestión para cada máquina virtual de almacenamiento (SVM) compatible con SAN.
- Las LIF y los espacios de nombres de NVMe deben alojarse en el mismo nodo.
- Solo se puede configurar una LIF NVMe que gestiona el tráfico de datos por SVM

Pasos

1. Cree una LIF:

   `network interface create -vserver` *`vserver_name`* `-lif` *`lif_name`* `-role data -data -protocol nfs -home-node` *`node_name`* `-home-port` *`port_name`* `{-address` *`IP_address`* `-netmask` *`IP_address`* `| -subnet-name` *`subnet_name`*`} -firewall-policy data -auto -revert {true|false}`

   Obtenga más información sobre `network interface create` en el "Referencia de comandos del ONTAP".

Opción	Descripción
ONTAP 9.5 y anteriores	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`
ONTAP 9.6 y posterior	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*

-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`

- `-role`No es necesario utilizar el parámetro cuando se crea una LIF mediante una política de servicio (a partir de ONTAP 9,6).
- `-data-protocol`El parámetro debe especificarse cuando se crea la LIF, y no se puede modificar posteriormente sin destruir ni volver a crear la LIF de datos.

  ```
  `-data-protocol`No es necesario utilizar el parámetro cuando se crea una LIF mediante una política de servicio (empezando por ONTAP 9.6).
  ```

- `-home-node` Es el nodo al que devuelve la LIF cuando `network interface revert` se ejecuta el comando en la LIF.

  También puede especificar si el LIF debe volver automáticamente al nodo de inicio y al puerto de inicio con `-auto-revert` la opción.

  Obtenga más información sobre `network interface revert` en el "Referencia de comandos del ONTAP".

- `-home-port` Es el puerto físico o lógico al que devuelve la LIF cuando `network interface revert` el comando se ejecuta en la LIF.
- Puede especificar una dirección IP con las `-address` `-netmask` opciones y, o bien habilitar la asignación desde una subred con `-subnet_name` la opción.
- Al usar una subred para suministrar la dirección IP y la máscara de red, si la subred se definió con una puerta de enlace, se añadirá automáticamente a la SVM una ruta predeterminada a esa puerta de enlace cuando se cree una LIF con dicha subred.
- Si asigna direcciones IP manualmente (sin una subred), es posible que deba configurar una ruta predeterminada para una puerta de enlace si hay clientes o controladores de dominio en una subred IP diferente. Obtenga más información sobre `network route create` y cómo crear una ruta estática dentro de una SVM en el "Referencia de comandos del ONTAP".
- Para `-firewall-policy` la opción, utilice el mismo valor predeterminado `data` que el rol LIF.

  Si lo desea, puede crear y agregar una política de firewall personalizada más adelante.

  > ⓘ A partir de ONTAP 9.10.1, las políticas de firewall están obsoletas y sustituidas por completo por políticas de servicios LIF. Para obtener más información, consulte "Configurar políticas de firewall para LIF".

- `-auto-revert` Permite especificar si una LIF de datos se revierte automáticamente a su nodo de inicio en circunstancias como el inicio, los cambios en el estado de la base de datos de gestión o el momento en que se establece la conexión de red. El valor por defecto es `false`, pero puede definirlo en `false` función de las políticas de gestión de red del entorno.

  a. Compruebe que la LIF se ha creado correctamente mediante `network interface show` el comando.

  b. Compruebe que se pueda acceder a la dirección IP configurada:

Para verificar una…	Usar…
Dirección IPv4	`network ping`
Dirección IPv6	`network ping6`

c. Si utiliza Kerberos, repita los pasos 1 a 3 para crear LIF adicionales.

   Kerberos debe habilitarse por separado en cada uno de estos LIF.

Ejemplos

El siguiente comando crea una LIF y especifica la dirección IP y los valores de la máscara de red mediante `-address` `-netmask` los parámetros y:

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

El siguiente comando crea una LIF y asigna valores de dirección IP y máscara de red a partir de la subred especificada (denominada cliente1_sub):

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

El siguiente comando muestra todas las LIF del clúster-1. Data LIF datalif1 y datalif3 están configurados con direcciones IPv4, y datalif4 está configurado con una dirección IPv6:

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

El siguiente comando muestra cómo crear una LIF de datos NAS que está asignada a la `default-data-files` política de servicio:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

Información relacionada

- "ping de red"
- "interfaz de red"

Habilitar DNS para la resolución de nombres de host de ONTAP NFS SVM

Puede usar `vserver services name-service dns` el comando para habilitar DNS en una SVM y configurarlo para que utilice DNS para la resolución de nombre de host. Los nombres de host se resuelven mediante servidores DNS externos.

Antes de empezar

Un servidor DNS para todo el sitio debe estar disponible para las búsquedas de nombre de host.

Debe configurar más de un servidor DNS para evitar un único punto de error. El `vserver services name-service dns create` comando emite una advertencia si se introduce solo un nombre de servidor DNS.

Acerca de esta tarea

Más información sobre "Configuración de DNS dinámico en la SVM".

Pasos

1. Habilite DNS en la SVM:

   `vserver services name-service dns create -vserver` *`vserver_name`* `-domains` *`domain_name`* `-name-servers` *`ip_addresses`* `-state enabled`

   El siguiente comando habilita los servidores DNS externos en la SVM vs1:

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   > El `vserver services name-service dns create` comando realiza una validación automática de la configuración y informa un mensaje de error si ONTAP no puede contactar con el servidor de nombres.

2. Muestra la configuración del dominio DNS mediante `vserver services name-service dns show` el comando.

   El siguiente comando muestra las configuraciones de DNS de todas las SVM del clúster:

   ```
   vserver services name-service dns show
                                                Name
   Vserver           State     Domains             Servers
   ----------------- --------- ------------------- -------------
   cluster1          enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   vs1.example.com   enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   ```

   El siguiente comando muestra información detallada de la configuración de DNS para SVM vs1:

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
          Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. Valide el estado de los servidores de nombres mediante `vserver services name-service dns check` el comando.

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

Configure los servicios de nombres

Obtenga más información sobre los servicios de nombres NFS de ONTAP

Según la configuración del sistema de almacenamiento, ONTAP debe poder buscar la información del host, usuario, grupo o grupo de red para proporcionar un acceso adecuado a los clientes. Es necesario configurar los servicios de nombres para permitir que ONTAP acceda a los servicios de nombres locales o externos para obtener esta información.

Debe utilizar un servicio de nombres como NIS o LDAP para facilitar las búsquedas de nombres durante la autenticación del cliente. Se recomienda utilizar LDAP siempre que sea posible para obtener una mayor seguridad, especialmente cuando se pone en marcha NFSv4 o posteriores. También debe configurar usuarios y grupos locales en caso de que los servidores de nombres externos no estén disponibles.

La información del servicio de nombres debe mantenerse sincronizada en todas las fuentes.

Configurar la tabla de conmutación del servicio de nombres NFS de ONTAP

Debe configurar correctamente la tabla del conmutador del servicio de nombres para permitir que ONTAP consulte servicios de nombres locales o externos para recuperar información de asignación de hosts, usuarios, grupos, netgroup o nombres.

Antes de empezar

Debe haber decidido qué servicios de nombre desea utilizar para la asignación de host, usuario, grupo, netgroup o nombre según corresponda a su entorno.

Si planea utilizar netgroups, todas las direcciones IPv6 especificadas en netgroups deben acortarse y comprimirse según se especifica en RFC 5952.

Acerca de esta tarea

No incluya fuentes de información que no se estén utilizando. Por ejemplo, si no se utiliza NIS en el entorno, no especifique la `-sources nis` opción.

Pasos

1. Agregue las entradas necesarias a la tabla de cambio de servicio de nombres:

   `vserver services name-service ns-switch create -vserver` *`vserver_name`* `-database` *`database_name`* `-sources` *`source_names`*

2. Compruebe que la tabla de cambio de servicio de nombres contiene las entradas esperadas en el orden deseado:

   `vserver services name-service ns-switch show -vserver` *`vserver_name`*

   Si desea realizar alguna corrección, debe usar `vserver services name-service ns-switch modify` `vserver services name-service ns-switch delete` los comandos o.

Ejemplo

En el siguiente ejemplo se crea una entrada nueva en la tabla de switches del servicio de nombres para la SVM vs1 para utilizar el archivo de netgroup local y un servidor NIS externo para buscar información de netgroup en ese orden:

```
cluster::> vserver services name-service ns-switch create -vserver vs1
-database netgroup -sources files,nis
```

Después de terminar

- Debe configurar los servicios de nombres que haya especificado para la SVM a fin de proporcionar acceso a los datos.
- Si elimina cualquier servicio de nombres para la SVM, también debe quitarlo de la tabla de switch de servicio de nombres.

  Es posible que el acceso del cliente al sistema de almacenamiento no funcione como se espera, si no puede eliminar el servicio de nombres de la tabla de switches de servicio de nombres.

Configurar usuarios y grupos UNIX locales

Obtenga información sobre los usuarios y grupos locales de UNIX para SVM NFS de ONTAP

Se pueden usar usuarios y grupos UNIX locales en la SVM para fines de autenticación y asignaciones de nombres. Puede crear usuarios y grupos de UNIX manualmente, o bien cargar un archivo que contenga usuarios o grupos de UNIX a partir de un identificador de recursos (URI) uniforme.

Hay un límite máximo predeterminado de 32,768 grupos de usuarios UNIX locales y miembros de grupo combinados en el clúster. El administrador del clúster puede modificar este límite.

Crear usuarios locales de UNIX en SVM NFS de ONTAP

Puede utilizar `vserver services name-service unix-user create` el comando para crear usuarios locales de UNIX. Un usuario UNIX local es un usuario de UNIX que se crea en la SVM como una opción de servicios de nombres UNIX que se va a utilizar en el procesamiento de asignaciones de nombres.

Paso

1. Crear un usuario local de UNIX:

   `vserver services name-service unix-user create -vserver` *`vserver_name`* `-user` *`user_name`* `-id` *`integer`* `-primary-gid` *`integer`* `-full-name` *`full_name`*

   `-user` *`user_name`* especifica el nombre de usuario. La longitud del nombre de usuario debe ser de 64 caracteres o menos.

   `-id` *`integer`* Especifica el ID de usuario que se asigna.

   `-primary-gid` *`integer`* Especifica el ID de grupo principal. Esto agrega el usuario al grupo principal. Después de crear el usuario, puede agregar manualmente el usuario a cualquier grupo adicional deseado.

Ejemplo

El siguiente comando crea un usuario local de UNIX llamado johnm (nombre completo "John Miller") en la SVM llamada vs1. El usuario tiene el ID 123 y el ID 100 del grupo principal.

```
node::> vserver services name-service unix-user create -vserver vs1 -user
johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

Cargar listas de usuarios locales de UNIX en SVM NFS de ONTAP

Como alternativa a la creación manual de usuarios UNIX locales individuales en SVM, puede simplificar la tarea cargando una lista de usuarios UNIX locales en SVM desde un identificador de recursos uniforme (URI) (`vserver services name-service unix-user load-from-uri`).

Pasos

1. Cree un archivo que contenga la lista de usuarios UNIX locales que desee cargar.

   El archivo debe contener información del usuario `/etc/passwd` en formato UNIX:

   `user_name: password: user_ID: group_ID: full_name`

   El comando descarta el valor *`password`* del campo y los valores de los campos después del *`full_name`* campo (*`home_directory`* y *`shell`*).

   El tamaño máximo de archivo admitido es de 2.5 MB.

2. Compruebe que la lista no contiene ninguna información duplicada.

Si la lista contiene entradas duplicadas, se produce un error al cargar la lista.

3. Copie el archivo en un servidor.

   El sistema de almacenamiento debe acceder al servidor a través de HTTP, HTTPS, FTP o FTPS.

4. Determine cuál es el URI del archivo.

   El URI es la dirección que se proporciona al sistema de almacenamiento para indicar dónde se encuentra el archivo.

5. Cargue el archivo que contiene la lista de usuarios UNIX locales en SVM desde el URI:

   `vserver services name-service unix-user load-from-uri -vserver` *`vserver_name`* `-uri {ftp|http|ftps|https}://`*`uri`* `-overwrite {true|false}`

   `-overwrite {true false}` especifica si se sobrescribirán las entradas. El valor predeterminado es `false`.

Ejemplo

El siguiente comando carga una lista de usuarios UNIX locales del URI `ftp://ftp.example.com/passwd` en la SVM llamada VS1. Los usuarios existentes del SVM no se sobrescriben por información del URI.

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

Crear grupos UNIX locales en SVM NFS de ONTAP

Puede utilizar `vserver services name-service unix-group create` el comando para crear grupos UNIX locales a la SVM. Los grupos UNIX locales se utilizan con usuarios UNIX locales.

Paso

1. Crear un grupo UNIX local:

   `vserver services name-service unix-group create -vserver` *`vserver_name`* `-name` *`group_name`* `-id` *`integer`*

   `-name` *`group_name`* especifica el nombre del grupo. La longitud del nombre del grupo debe ser de 64 caracteres o menos.

   `-id` *`integer`* Especifica el ID de grupo que asigna.

Ejemplo

El siguiente comando crea un grupo local llamado eng en la SVM llamada vs1. El grupo tiene el ID 101.

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name
eng -id 101
```

Agregar usuarios al grupo local de UNIX en SVM NFS de ONTAP

Puede utilizar `vserver services name-service unix-group adduser` el comando para agregar un usuario a un grupo UNIX complementario local a la SVM.

Paso

1. Agregar un usuario a un grupo UNIX local:

`vserver services name-service unix-group adduser -vserver` *`vserver_name`* `-name` *`group_name`* `-username` *`user_name`*

`-name` *`group_name`* Especifica el nombre del grupo UNIX al que se agregará el usuario además del grupo primario del usuario.

Ejemplo

El siguiente comando agrega un usuario llamado max a un grupo UNIX local llamado eng en la SVM llamada vs1:

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name
eng
-username max
```

Cargar grupos UNIX locales desde URI en SVM NFS de ONTAP

Como alternativa a la creación manual de grupos UNIX locales individuales, puede cargar una lista de grupos UNIX locales en SVM desde un identificador de recursos uniforme (URI) mediante el `vserver services name-service unix-group load-from-uri` comando.

Pasos

1. Cree un archivo que contenga la lista de grupos UNIX locales que desee cargar.

   El archivo debe contener información del grupo en `/etc/group` formato UNIX:

   `group_name: password: group_ID: comma_separated_list_of_users`

   El comando descarta el valor *`password`* del campo.

   El tamaño máximo de archivo admitido es de 1 MB.

   La longitud máxima de cada línea del archivo de grupo es de 32,768 caracteres.

2. Compruebe que la lista no contiene ninguna información duplicada.

   La lista no debe contener entradas duplicadas o, de lo contrario, se producirá un error al cargar la lista. Si ya hay entradas presentes en la SVM, debe configurar `-overwrite` el parámetro para `true` que sobrescriba todas las entradas existentes con el nuevo archivo o asegurarse de que el nuevo archivo no contenga ninguna entrada que duplique las entradas existentes.

3. Copie el archivo en un servidor.

El sistema de almacenamiento debe acceder al servidor a través de HTTP, HTTPS, FTP o FTPS.

4. Determine cuál es el URI del archivo.

   El URI es la dirección que se proporciona al sistema de almacenamiento para indicar dónde se encuentra el archivo.

5. Cargue el archivo que contiene la lista de grupos UNIX locales en la SVM desde el URI:

   `vserver services name-service unix-group load-from-uri -vserver` *vserver_name* `-uri {ftp|http|ftps|https}://`*uri* `-overwrite {true|false}`

   `-overwrite true false}` especifica si se sobrescribirán las entradas. El valor predeterminado es `false`. Si especifica este parámetro como `true`, ONTAP reemplaza toda la base de datos de grupo UNIX local existente de la SVM especificada por las entradas del archivo que está cargando.

Ejemplo

El siguiente comando carga una lista de grupos UNIX locales del URI `ftp://ftp.example.com/group` en la SVM llamada VS1. Los grupos existentes de la SVM no se sobrescriben por información del URI.

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

Trabajar con netgroups

Obtenga información sobre los grupos de redes en las SVM NFS de ONTAP

Puede utilizar netgroups para la autenticación de usuarios y para que coincida con los clientes en las reglas de directiva de exportación. Puede proporcionar acceso a netgroups desde servidores de nombres externos (LDAP o NIS), o puede cargar netgroups desde un identificador de recursos uniforme (URI) en SVM mediante el `vserver services name-service netgroup load` comando.

Antes de empezar

Antes de trabajar con netgroups, debe asegurarse de que se cumplen las siguientes condiciones:

- Todos los hosts de los grupos de red, independientemente del origen (NIS, LDAP o archivos locales), deben tener registros DNS tanto de reenvío (A) como de retroceso (PTR) para proporcionar búsquedas DNS de reenvío e inversa coherentes.

  Además, si una dirección IP de un cliente tiene varios registros PTR, todos esos nombres de host deben ser miembros del netgroup y tener registros Correspondientes.

- Los nombres de todos los hosts de netgroups, independientemente de su origen (NIS, LDAP o archivos locales), deben estar escritos correctamente y utilizar el caso correcto. Las incoherencias de los casos en los nombres de host utilizados en los grupos de redes pueden dar lugar a un comportamiento inesperado, como las comprobaciones de exportación fallidas.
- Todas las direcciones IPv6 especificadas en los grupos de red deben acortarse y comprimirse como se especifica en RFC 5952.

Por ejemplo, 2011:hu9:0:0:0:0:3:1 debe acortarse a 2011:hu9::3:1.

Acerca de esta tarea

Al trabajar con netgroups, puede realizar las siguientes operaciones:

- Puede utilizar el `vserver export-policy netgroup check-membership` comando para ayudar a determinar si una IP de cliente es miembro de un determinado grupo de red.
- Puede utilizar el `vserver services name-service getxxbyyy netgrp` comando para comprobar si un cliente forma parte de un grupo de red.

  El servicio subyacente para realizar la búsqueda se selecciona según el orden de cambio de servicio de nombres configurado.

Cargar grupos de redes desde URI en SVM NFS de ONTAP

Uno de los métodos que se pueden utilizar para hacer coincidir clientes en las reglas de directiva de exportación es utilizando los hosts enumerados en netgroups. Puede cargar netgroups desde un identificador de recursos uniforme (URI) en SVM como alternativa al uso de netgroups almacenados en servidores de nombres externos (`vserver services name-service netgroup load`).

Antes de empezar

Los archivos de grupos de red deben cumplir los siguientes requisitos antes de cargarlos en una SVM:

- El archivo debe utilizar el mismo formato de archivo de texto de netgroup adecuado que se utiliza para rellenar NIS.

  ONTAP comprueba el formato del archivo de texto del grupo de red antes de cargarlo. Si el archivo contiene errores, no se cargará y se mostrará un mensaje que indique las correcciones que debe realizar en el archivo. Después de corregir los errores, puede volver a cargar el archivo netgroup en la SVM especificada.

- Los caracteres alfabéticos en los nombres de host del archivo netgroup deben ser en minúscula.
- El tamaño máximo de archivo admitido es de 5 MB.
- El nivel máximo admitido para los grupos de red de anidamiento es 1000.
- Sólo se pueden utilizar nombres de host DNS primarios al definir nombres de host en el archivo de grupo de red.

  Para evitar problemas de acceso a la exportación, los nombres de host no deben definirse mediante registros CNAME o round robin de DNS.

- Las porciones de triples del usuario y del dominio en el archivo de netgroup deben mantenerse vacías porque ONTAP no las admite.

  Solo se admite la parte host/IP.

Acerca de esta tarea

ONTAP admite búsquedas netgroup-by-host para el archivo de netgroup local. Después de cargar el archivo netgroup, ONTAP crea automáticamente un mapa netgroup.byhost para habilitar búsquedas netgroup-by-host. Esto puede acelerar significativamente las búsquedas de grupos de red locales al procesar reglas de políticas

de exportación para evaluar el acceso de los clientes.

Paso

1. Cargue los grupos de redes en SVM desde un URI:

   `vserver services name-service netgroup load -vserver` *`vserver_name`* `-source {ftp|http|ftps|https}://`*`uri`*

   La carga del archivo de netgroup y la creación del mapa netgroup.byhost pueden tardar varios minutos.

   Si desea actualizar los grupos de red, puede editar el archivo y cargar el archivo de netgroup actualizado en la SVM.

Ejemplo

El siguiente comando carga las definiciones de netgroup en la SVM llamada VS1 desde la URL HTTP `http://intranet/downloads/corp-netgroup`:

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

Verificar las definiciones de grupos de redes SVM de ONTAP NFS

Después de cargar netgroups en la SVM, puede utilizar `vserver services name-service netgroup status` el comando para comprobar el estado de las definiciones de netgroup. Esto permite determinar si las definiciones de grupos de red son consistentes en todos los nodos que forman parte de la SVM.

Pasos

1. Configure el nivel de privilegio en Advanced:

   `set -privilege advanced`

2. Compruebe el estado de las definiciones de netgroup:

   `vserver services name-service netgroup status`

   Puede visualizar información adicional en una vista más detallada.

3. Vuelva al nivel de privilegio de administrador:

   `set -privilege admin`

Ejemplo

Una vez establecido el nivel de privilegio, el siguiente comando muestra el estado de netgroup para todas las SVM:

```
vs1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when
         directed to do so by technical support.
Do you wish to continue? (y or n): y

vs1::*> vserver services name-service netgroup status
Virtual
Server    Node            Load Time           Hash Value
--------- --------------- -------------------
--------------------------------
vs1
          node1           9/20/2006 16:04:53
e6cb38ec1396a280c0d2b77e3a84eda2
          node2           9/20/2006 16:06:26
e6cb38ec1396a280c0d2b77e3a84eda2
          node3           9/20/2006 16:08:08
e6cb38ec1396a280c0d2b77e3a84eda2
          node4           9/20/2006 16:11:33
e6cb38ec1396a280c0d2b77e3a84eda2
```

Crear configuraciones de dominio NIS para SVM NFS de ONTAP

Si se utiliza un servicio de información de red (NIS) en el entorno para servicios de nombres, debe crear una configuración de dominio NIS para la SVM mediante `vserver services name-service nis-domain create` el comando.

Antes de empezar

Todos los servidores NIS configurados deben estar disponibles y accesibles antes de configurar el dominio NIS en la SVM.

Si tiene previsto utilizar NIS para búsquedas en directorios, los mapas de sus servidores NIS no pueden tener más de 1,024 caracteres para cada entrada. No especifique el servidor NIS que no cumpla con este límite. De lo contrario, es posible que se produzca un error en el acceso del cliente que depende de las entradas NIS.

Acerca de esta tarea

Si su base de datos NIS contiene un `netgroup.byhost` mapa, ONTAP puede utilizarlo para búsquedas más rápidas. Los `netgroup.byhost` `netgroup` mapas y del directorio se deben mantener sincronizados en todo momento para evitar problemas de acceso de los clientes. A partir de ONTAP 9.7, `netgroup.byhost` las entradas NIS se pueden almacenar en caché con los `vserver services name-service nis-domain netgroup-database` comandos.

No se admite el uso de NIS para la resolución del nombre de host.

Pasos

1. Cree una configuración de dominio NIS:

```
vserver services name-service nis-domain create -vserver vs1 -domain
<domain_name> -nis-servers <IP_addresses>
```

Puede especificar hasta 10 servidores NIS.

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

2. Compruebe que se ha creado el dominio:

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

Ejemplo

El siguiente comando crea una configuración de dominio NIS para un dominio NIS llamado en la SVM `vs1` llamada `nisdomain` con un servidor NIS en la dirección IP `192.0.2.180` :

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -nis-servers 192.0.2.180
```

Utilice LDAP

Obtenga información sobre el uso de servicios de nombres LDAP en SVM NFS de ONTAP

Si se utiliza LDAP en su entorno para servicios de nombre, debe trabajar con el administrador de LDAP para determinar los requisitos y las configuraciones del sistema de almacenamiento adecuadas, habilitar la SVM como cliente LDAP.

A partir de ONTAP 9.10.1, el enlace de canal LDAP se admite de forma predeterminada tanto para las conexiones LDAP de los servicios de nombres como de Active Directory. 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 canales LDAP con los servidores de nombres, utilice `-try-channel-binding` el parámetro con `ldap client modify` el comando.

Para obtener más información, consulte "2020 requisitos de enlace de canal LDAP y firma LDAP para Windows".

- Antes de configurar LDAP para ONTAP, debe verificar que la implementación del sitio cumple las prácticas recomendadas para la configuración del cliente y el servidor LDAP. En particular, deben cumplirse las siguientes condiciones:
  - El nombre de dominio del servidor LDAP debe coincidir con la entrada del cliente LDAP.
  - Los tipos hash de contraseña de usuario LDAP compatibles con el servidor LDAP deben incluir los compatibles con ONTAP:
    - CRIPTA (todos los tipos) y SHA-1 (SHA, SSHA).
    - A partir de los valores hash de ONTAP 9.8, SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, También se admiten SSHA-384 y SSHA-512).

- Si el servidor LDAP requiere medidas de seguridad de la sesión, debe configurarlas en el cliente LDAP.

  Están disponibles las siguientes opciones de seguridad de la sesión:

  - La firma LDAP (proporciona comprobación de la integridad de los datos) y la firma y el sellado LDAP (proporciona cifrado y comprobación de la integridad de los datos).
  - INICIE TLS
  - LDAPS (LDAP sobre TLS o SSL)
- Para habilitar consultas LDAP firmadas y selladas, se deben configurar los siguientes servicios:
  - Los servidores LDAP deben ser compatibles con el mecanismo SASL GSSAPI (Kerberos).
  - Los servidores LDAP deben tener registros DNS A/AAAA, así como registros PTR configurados en el servidor DNS.
  - Los servidores Kerberos deben tener registros SRV presentes en el servidor DNS.
- Para habilitar el INICIO de TLS o LDAPS, se deben tener en cuenta los siguientes puntos.
  - Se trata de una práctica recomendada de NetApp para usar Start TLS en lugar de LDAPS.
  - Si se usa LDAPS, el servidor LDAP debe habilitar para TLS o SSL en ONTAP 9.5 y versiones posteriores. SSL no es compatible con ONTAP 9.0-9.4.
  - Ya debe configurarse un servidor de certificados en el dominio.
- Para habilitar la búsqueda de referencias LDAP (en ONTAP 9.5 y posterior), se deben cumplir las siguientes condiciones:
  - Ambos dominios deben configurarse con una de las siguientes relaciones de confianza:
    - Bidireccional
    - Unidireccional, donde la primaria confía en el dominio de referencia
    - Padre-hijo
  - El DNS debe configurarse de modo que resuelva todos los nombres de servidor a los que se hace referencia.
  - Las contraseñas de dominio deben coincidir para autenticarse cuando --bind-as-cifs-Server se establece en true.

  > Las siguientes configuraciones no son compatibles con la búsqueda de referencias LDAP.
  >
  > - Para todas las versiones de ONTAP:
  >   - Clientes LDAP en una SVM de administrador
  > - Para ONTAP 9.8 y versiones anteriores (se admiten en la versión 9.9.1 y posteriores):
  >   - Firma y sellado LDAP (`-session-security`opción)
  >   - Conexiones TLS cifradas (la `-use-start-tls` opción)
  >   - Comunicaciones a través del puerto LDAPS 636 (la `-use-ldaps-for-ad-ldap` opción)

- Debe introducir un esquema de LDAP al configurar el cliente LDAP en la SVM.

  En la mayoría de los casos, uno de los esquemas ONTAP predeterminados será apropiado. Sin embargo, si el esquema LDAP del entorno difiere de éste, debe crear un nuevo esquema de cliente LDAP para

ONTAP antes de crear el cliente LDAP. Consulte a su administrador LDAP sobre los requisitos de su entorno.

- No se admite el uso de LDAP para la resolución del nombre de host.

Si quiere más información

- "Informe técnico de NetApp 4835: Cómo configurar LDAP en ONTAP"
- "Instale los certificados de CA raíz autofirmados en la SVM SMB de ONTAP"

Crear nuevos esquemas de cliente LDAP para SVM NFS de ONTAP

Si el esquema LDAP del entorno difiere de los valores predeterminados de ONTAP, debe crear un nuevo esquema de cliente LDAP para ONTAP antes de crear la configuración de cliente LDAP.

Acerca de esta tarea

La mayoría de los servidores LDAP pueden utilizar los esquemas predeterminados proporcionados por ONTAP:

- MS-AD-BIS (el esquema preferido para la mayoría de los servidores AD de Windows 2012 y posteriores)
- AD-IDMU (Windows 2008, Windows 2012 y servidores AD posteriores)
- AD-SFU (servidores Windows 2003 y anteriores de AD)
- RFC-2307 (SERVIDORES UNIX LDAP)

Si necesita utilizar un esquema LDAP no predeterminado, debe crearlo antes de crear la configuración del cliente LDAP. Consulte con el administrador LDAP antes de crear un nuevo esquema.

Los esquemas LDAP predeterminados proporcionados por ONTAP no se pueden modificar. Para crear un nuevo esquema, cree una copia y, a continuación, modifique la copia en consecuencia.

Pasos

1. Mostrar las plantillas de esquema de cliente LDAP existentes para identificar la que desea copiar:

   ```
   vserver services name-service ldap client schema show
   ```

2. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

3. Haga una copia de un esquema de cliente LDAP existente:

   ```
   vserver services name-service ldap client schema copy -vserver vserver_name
   -schema existing_schema_name -new-schema-name new_schema_name
   ```

4. Modifique el nuevo esquema y personalícelo para su entorno:

   ```
   vserver services name-service ldap client schema modify
   ```

5. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Crear configuraciones de cliente LDAP para el acceso NFS de ONTAP

Si desea que ONTAP acceda a los servicios LDAP o Active Directory externos en el entorno, primero debe configurar un cliente LDAP en el sistema de almacenamiento.

Antes de empezar

Uno de los tres primeros servidores de la lista de dominios resueltos de Active Directory debe estar activo y servir datos. De lo contrario, esta tarea falla.

> Hay varios servidores, de los cuales más de dos servidores están inactivos en cualquier momento.

Pasos

1. Consulte al administrador de LDAP para determinar los valores de configuración adecuados para `vserver services name-service ldap client create` el comando:

   a. Especifique una conexión basada en dominio o en dirección a los servidores LDAP.

   ```
   `-ad-domain` `-servers`Las opciones y se excluyen mutuamente.
   ```

   - Utilice `-ad-domain` la opción para habilitar la detección del servidor LDAP en el dominio de Active Directory.
     - Puede usar la `-restrict-discovery-to-site` opción para restringir la detección del servidor LDAP al sitio predeterminado de CIFS del dominio especificado. Si utiliza esta opción, también debe especificar el sitio predeterminado de CIFS con `-default-site`.
   - Puede usar `-preferred-ad-servers` la opción para especificar uno o más servidores de Active Directory preferidos por dirección IP en una lista delimitada por comas. Después de crear el cliente, puede modificar esta lista mediante `vserver services name-service ldap client modify` el comando.
   - Utilice `-servers` la opción para especificar uno o más servidores LDAP (Active Directory o UNIX) por dirección IP en una lista delimitada por comas.

     > opción está obsoleta. `-ldap-servers` El campo reemplaza el `-servers` campo. Este campo puede tomar un nombre de host o una dirección IP para el servidor LDAP.

   b. Especifique un esquema LDAP predeterminado o personalizado.

   La mayoría de los servidores LDAP pueden utilizar los esquemas de sólo lectura predeterminados que proporciona ONTAP. Lo mejor es utilizar esos esquemas predeterminados a menos que haya un requisito para hacer lo contrario. Si es así, puede crear su propio esquema copiando un esquema predeterminado (son de sólo lectura) y modificando la copia.

   Esquemas predeterminados:

   - MS-AD-BIS

     Basado en RFC-2307bis, este es el esquema LDAP preferido para la mayoría de implementaciones LDAP estándar de Windows 2012 y posteriores.

- `AD-IDMU`

  Basado en Administración de identidades de Active Directory para UNIX, este esquema es apropiado para la mayoría de servidores AD de Windows 2008, Windows 2012 y posteriores.

- `AD-SFU`

  Basado en los Servicios de Active Directory para UNIX, este esquema es apropiado para la mayoría de servidores de AD anteriores y Windows 2003.

- `RFC-2307`

  Basado en RFC-2307 (*an Approach for using LDAP as a Network Information Service*), este esquema es apropiado para la mayoría de servidores UNIX AD.

c. Seleccione valores de enlace.

- `-min-bind-level {anonymous|simple|sasl}` especifica el nivel de autenticación de enlace mínimo.

  El valor predeterminado es **`anonymous`**.

- `-bind-dn` *`LDAP_DN`* especifica el usuario de enlace.

  Para los servidores de Active Directory, debe especificar el usuario en el formulario de cuenta (DOMINIO\usuario) o principal (user@domain.com). De lo contrario, debe especificar el usuario en el formulario Nombre completo (CN=user,DC=domain,DC=com).

- `-bind-password` *`password`* especifica la contraseña de enlace.

d. Seleccione las opciones de seguridad de la sesión, si es necesario.

Puede habilitar la firma y el sellado LDAP o LDAP over TLS si lo requiere el servidor LDAP.

- `--session-security {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`.

  También debe definir `-min-bind-level {sasl}` a menos que desee que la autenticación de enlace se retroceda **`anonymous`** o **`simple`** si el enlace de firma y sellado falla.

- `-use-start-tls {true|false}`

  Si se establece en **`true`** y el servidor LDAP lo admite, el cliente LDAP utiliza una conexión TLS cifrada con el servidor. El valor predeterminado es **`false`**. Debe instalar un certificado de CA raíz autofirmado del servidor LDAP para usar esta opción.

> Si la máquina virtual de almacenamiento tiene un servidor SMB añadido a un dominio y el servidor LDAP es uno de los controladores de dominio del dominio inicial del servidor SMB, puede modificar la `-session-security-for-ad-ldap` opción mediante `vserver cifs security modify` el comando.

e. Seleccione los valores de puerto, consulta y base.

Se recomiendan los valores predeterminados, pero debe verificar con el administrador de LDAP que son adecuados para su entorno.

- `-port port` Especifica el puerto del servidor LDAP.

  El valor predeterminado es `389`.

Si tiene pensado utilizar Start TLS para proteger la conexión LDAP, debe utilizar el puerto predeterminado 389. Start TLS comienza como una conexión de texto sin formato sobre el puerto 389 predeterminado LDAP y esa conexión se actualiza a TLS. Si cambia el puerto, Start TLS falla.

- `-query-timeout integer` especifica el tiempo de espera de la consulta en segundos.

  El intervalo permitido es de 1 a 10 segundos. El valor predeterminado es `3` segundos.

- `-base-dn LDAP_DN` Especifica el DN base.

  Se pueden introducir varios valores si es necesario (por ejemplo, si la búsqueda de referencias LDAP está activada). El valor predeterminado es `""` (root).

- `-base-scope` {`base`|`onelevel`|`subtree`} especifica el ámbito de búsqueda base.

  El valor predeterminado es `subtree`.

- `-referral-enabled` {`true`|`false`} Especifica si el seguimiento de referencias LDAP está activado.

  A partir de ONTAP 9.5, esto permite al cliente LDAP de ONTAP remitir solicitudes de búsqueda a otros servidores LDAP si el servidor LDAP principal devuelve una respuesta de referencia LDAP que indica que los registros deseados están presentes en los servidores LDAP remitidos. El valor predeterminado es **`false`**.

Para buscar registros presentes en los servidores LDAP a los que se hace referencia, se debe agregar la base-dn de los registros referidos a la base-dn como parte de la configuración del cliente LDAP.

2. Cree una configuración de cliente LDAP en la máquina virtual de almacenamiento:

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```

> Debe proporcionar el nombre de la máquina virtual de almacenamiento al crear una configuración de cliente LDAP.

3. Compruebe que la configuración del cliente LDAP se ha creado correctamente:

```
vserver services name-service ldap client show -client-config
client_config_name
```

Ejemplos

El siguiente comando crea una nueva configuración de cliente LDAP llamada ldap1 para que la máquina virtual de almacenamiento VS1 funcione con un servidor de Active Directory para LDAP:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

El siguiente comando crea una nueva configuración de cliente LDAP denominada ldap1 para la máquina virtual de almacenamiento VS1 con el fin de funcionar con un servidor de Active Directory para LDAP en el que se requiere firma y sellado, y la detección del servidor LDAP está restringida a un sitio determinado para el dominio especificado:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

El siguiente comando crea una nueva configuración de cliente LDAP denominada ldap1 para que la máquina virtual de almacenamiento VS1 funcione con un servidor de Active Directory para LDAP en el que se requiere la búsqueda de referencias de LDAP:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

El siguiente comando modifica la configuración de cliente LDAP llamada ldap1 para la máquina virtual de almacenamiento VS1 especificando el DN base:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

El siguiente comando modifica la configuración de cliente LDAP denominada ldap1 para la máquina virtual de almacenamiento VS1 habilitando la búsqueda de referencias:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com"  -referral-enabled true
```

Asociar configuraciones de cliente LDAP con SVM NFS de ONTAP

Para habilitar LDAP en una SVM, debe usar `vserver services name-service ldap create` el comando para asociar una configuración de cliente LDAP con la SVM.

Antes de empezar

- Debe haber un dominio de LDAP dentro de la red y estar accesible para el clúster en el que está ubicada la SVM.
- Debe haber una configuración de cliente LDAP en la SVM.

Pasos

1. Habilite LDAP en la SVM:

   `vserver services name-service ldap create -vserver` *`vserver_name`* `-client-config` *`client_config_name`*

   > El `vserver services name-service ldap create` El comando realiza una validación de configuración automática e informa un mensaje de error si ONTAP no puede comunicarse con el servidor de nombres.

   El siguiente comando habilita LDAP en el SVM "vs1"SVM y lo configura para utilizar la configuración del cliente LDAP "ldap1":

   ```
   cluster1::> vserver services name-service ldap create -vserver vs1
   -client-config ldap1 -client-enabled true
   ```

2. Validar el estado de los servidores de nombres mediante el comando vserver Services NAME-service ldap check.

   El siguiente comando valida los servidores LDAP en la SVM VS1.

   ```
   cluster1::> vserver services name-service ldap check -vserver vs1

   | Vserver: vs1                                                  |
   | Client Configuration Name: c1                                 |
   | LDAP Status: up                                               |
   | LDAP Status Details: Successfully connected to LDAP server
   "10.11.12.13".                                                |
   ```

Verificar fuentes LDAP para SVM NFS de ONTAP

Debe comprobar que los orígenes LDAP para servicios de nombres figuran correctamente en la tabla de switches de servicio de nombres para la SVM.

Pasos

1. Mostrar el contenido de la tabla de cambio de servicio de nombres actual:

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

   El siguiente comando muestra los resultados de la SVM My_SVM:

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
                                 Source
Vserver         Database         Order
--------------- ------------   ---------
My_SVM          hosts          files,
                               dns
My_SVM          group          files,ldap
My_SVM          passwd         files,ldap
My_SVM          netgroup       files
My_SVM          namemap        files
5 entries were displayed.
```

   `namemap` especifica los orígenes para buscar información de asignación de nombres y en qué orden. En un entorno únicamente UNIX, esta entrada no es necesaria. La asignación de nombres sólo es necesaria en un entorno mixto que utilice UNIX y Windows.

2. Actualice la `ns-switch` entrada según corresponda:

Si desea actualizar la entrada del interruptor ns para…	Introduzca el comando…
Información del usuario	`vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files`
Información de grupo	`vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files`
Información de netgroup	`vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files`

Utilice Kerberos con NFS para una mayor seguridad

Obtenga información sobre el uso de Kerberos con ONTAP NFS para la autenticación de seguridad

Si se utiliza Kerberos en su entorno para autenticación segura, debe trabajar con el administrador de Kerberos para determinar requisitos y configuraciones del sistema de almacenamiento apropiadas y, a continuación, habilitar la SVM como cliente Kerberos.

Su entorno debe cumplir las siguientes directrices:

- La implementación de su sitio debe seguir las prácticas recomendadas para la configuración del servidor Kerberos y del cliente antes de configurar Kerberos para ONTAP.
- Si es posible, utilice NFSv4 o posteriores si es necesaria la autenticación de Kerberos.

  NFSv3 se puede utilizar con Kerberos. Sin embargo, todas las ventajas de seguridad de Kerberos solo se materian en puestas en marcha de ONTAP de NFSv4 o posteriores.

- Para promover el acceso redundante al servidor, se debe habilitar Kerberos en varias LIF de datos en varios nodos del clúster mediante el mismo SPN.
- Cuando se habilita Kerberos en la SVM, debe especificarse uno de los siguientes métodos de seguridad en las reglas de exportación para volúmenes o qtrees en función de la configuración del cliente NFS.
  - `krb5` (Protocolo Kerberos v5)
  - `krb5i` (Protocolo Kerberos v5 con comprobación de integridad con sumas de comprobación)
  - `krb5p` (Protocolo Kerberos v5 con servicio de privacidad)

Además del servidor Kerberos y los clientes, para ONTAP se deben configurar los siguientes servicios externos con el fin de admitir Kerberos:

- Servicio de directorio

  Debe utilizar un servicio de directorio seguro en su entorno, como Active Directory u OpenLDAP, que esté configurado para usar LDAP sobre SSL/TLS. No utilice NIS, cuyas solicitudes se envían en texto claro y, por lo tanto, no son seguras.

- NTP

  Debe tener un servidor de tiempo de trabajo que ejecute NTP. Esto es necesario para evitar errores de autenticación de Kerberos debido a una desviación de tiempo.

- Resolución de nombres de dominio (DNS)

  Cada cliente UNIX y cada LIF de SVM deben tener un registro de servicio (SRV) adecuado registrado con el KDC en zonas de búsqueda inversa y de reenvío. Todos los participantes deben poder resolverse correctamente a través de DNS.

Verificar los permisos de UNIX para las configuraciones NFS Kerberos en las SVM de ONTAP

Kerberos requiere que se establezcan determinados permisos de UNIX para el volumen raíz de la SVM y para los usuarios y grupos locales.

Pasos

1. Visualice los permisos relevantes en el volumen raíz de la SVM:

   `volume show -volume root_vol_name-fields user,group,unix-permissions`

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

Nombre…	Estableciendo…
UID	Raíz o ID 0
GID	Raíz o ID 0
Permisos de UNIX	755

   Si no se muestran estos valores, utilice `volume modify` el comando para actualizarlos.

2. Mostrar los usuarios UNIX locales:

   `vserver services name-service unix-user show -vserver vserver_name`

   La SVM debe tener configurados los siguientes usuarios de UNIX:

Nombre de usuario	ID de usuario	ID del grupo principal	Comentar
nfs	500	0	Necesario para la fase DE INICIALIZACIÓN de GSS. El primer componente del SPN de usuario del cliente NFS se utiliza como usuario. El usuario nfs no es necesario si existe una asignación de nombre Kerberos-UNIX para el SPN del usuario cliente NFS.
raíz	0	0	Necesario para el montaje.

   Si no se muestran estos valores, puede usar `vserver services name-service unix-user modify` el comando para actualizarlos.

3. Mostrar los grupos UNIX locales:

   `vserver services name-service unix-group show -vserver vserver _name`

   La SVM debe tener configurados los siguientes grupos UNIX:

Nombre del grupo	ID de grupo
daemon	1
raíz	0

Si no se muestran estos valores, puede usar `vserver services name-service unix-group modify` el comando para actualizarlos.

Crear configuraciones de dominio Kerberos de NFS en SVM de ONTAP

Si desea que ONTAP acceda a servidores Kerberos externos en su entorno, primero debe configurar la SVM para que utilice un Reino de Kerberos existente. Para ello, debe recopilar valores de configuración para el servidor KDC de Kerberos y, a continuación, utilizar el `vserver nfs kerberos realm create` comando para crear la configuración del dominio de Kerberos en una SVM.

Antes de empezar

El administrador del clúster debe haber configurado NTP en el sistema de almacenamiento, el cliente y el servidor KDC para evitar problemas de autenticación. Las diferencias de tiempo entre un cliente y un servidor (desfase de reloj) son una causa común de fallos de autenticación.

Pasos

1. Consulte con su administrador de Kerberos para determinar los valores de configuración adecuados que se deben proporcionar con el `vserver nfs kerberos realm create` comando.
2. Cree una configuración de dominio de Kerberos en la SVM:

   `vserver nfs kerberos realm create -vserver` *`vserver_name`* `-realm` *`realm_name`* *`{AD_KDC_server_values |AD_KDC_server_values}`* `-comment "`*`text`*`"`
3. Compruebe que la configuración de dominio Kerberos se ha creado correctamente:

   `vserver nfs kerberos realm show`

Ejemplos

El siguiente comando crea una configuración de dominio Kerberos para NFS para la SVM vs1 que utiliza un servidor de Microsoft Active Directory como servidor KDC. El dominio Kerberos es AUTH.EXAMPLE.COM. El servidor de Active Directory se denomina ad-1 y su dirección IP es 10.10.8.14. La desviación del reloj permitida es de 300 segundos (valor predeterminado). La dirección IP del servidor KDC es 10.10.8.14 y su número de puerto es 88 (el valor predeterminado). "Microsoft Kerberos config" es el comentario.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

El siguiente comando crea una configuración de dominio de Kerberos para NFS para la SVM vs1 que utiliza un MIT KDC. El dominio Kerberos es SECURITY.EXAMPLE.COM. La desviación del reloj permitida es de 300 segundos. La dirección IP del servidor KDC es 10.10.9.1 y su número de puerto es 88. El proveedor de KDC es otro que indica un proveedor de UNIX. La dirección IP del servidor de administración es 10.10.9.1 y su número de puerto es 749 (el valor predeterminado). La dirección IP del servidor de contraseñas es 10.10.9.1 y su número de puerto es 464 (el valor predeterminado). "UNIX Kerberos config" es el comentario.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

Configurar los tipos de cifrado permitidos por NFS Kerberos para las SVM de ONTAP

De forma predeterminada, ONTAP admite los siguientes tipos de cifrado para NFS Kerberos: DES, 3DES, AES-128 y AES-256. Puede configurar los tipos de cifrado permitidos para cada SVM de modo que se adapten a los requisitos de seguridad de su entorno en particular mediante `vserver nfs modify` el comando con el `-permitted -enc-types` parámetro.

Acerca de esta tarea

Para obtener la mayor compatibilidad del cliente, ONTAP admite de forma predeterminada tanto el cifrado des débil como el AES sólido. Esto significa, por ejemplo, que si desea aumentar la seguridad y su entorno lo admite, puede utilizar este procedimiento para deshabilitar DES y 3DES y requerir que los clientes utilicen sólo el cifrado AES.

Debería utilizar el cifrado más potente disponible. Para ONTAP, esto es AES-256. Debe confirmar con el administrador de KDC que este nivel de cifrado es compatible con su entorno.

- Habilitar o deshabilitar completamente AES (tanto AES-128 como AES-256) en las SVM es disruptivo porque destruye el archivo ORIGINAL DE DES principal/keytab, lo que requiere que se deshabilite la configuración de Kerberos en todos los LIF para la SVM.

  Antes de realizar este cambio, debe comprobar que los clientes NFS no utilizan el cifrado AES en la SVM.

- La habilitación o deshabilitación DE DES o 3DES no requiere ningún cambio en la configuración de Kerberos en las LIF.

Paso

1. Habilite o deshabilite el tipo de cifrado permitido que desee:

Si desea habilitar o deshabilitar…	Siga estos pasos…
DES o 3DES	a. Configure los tipos de cifrado permitidos por Kerberos NFS de la SVM: `vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`* Separe varios tipos de cifrado con una coma. b. Compruebe que el cambio se ha realizado correctamente: `vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`

AES-128 o AES-256	a. Identifique en qué SVM y LIF Kerberos se han habilitado:
	`vserver nfs kerberos interface show`
	
	b. Deshabilite Kerberos en todas las LIF de la SVM cuyo Kerberos NFS permitió el tipo de cifrado que desee modificar:
	`vserver nfs kerberos interface disable -lif` *`lif_name`*
	
	c. Configure los tipos de cifrado permitidos por Kerberos NFS de la SVM:
	`vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`*
	
	Separe varios tipos de cifrado con una coma.
	
	d. Compruebe que el cambio se ha realizado correctamente:
	`vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`
	
	e. Vuelva a habilitar Kerberos en todas las LIF en la SVM:
	`vserver nfs kerberos interface enable -lif` *`lif_name`* `-spn` *`service_principal_name`*
	
	f. Compruebe que Kerberos está habilitado en todas las LIF:
	`vserver nfs kerberos interface show`

Habilitar NFS Kerberos en LIF de ONTAP

Puede usar `vserver nfs kerberos interface enable` el comando para habilitar

Kerberos en una LIF de datos. Esto permite que la SVM utilice servicios de seguridad Kerberos para NFS.

Acerca de esta tarea

Si utiliza un KDC de Active Directory, los primeros 15 caracteres de los SPN utilizados deben ser únicos entre las SVM dentro de un dominio o dominio.

Pasos

1. Cree la configuración de Kerberos NFS:

   `vserver nfs kerberos interface enable -vserver` *`vserver_name`* `-lif` *`logical_interface`* `-spn` *`service_principal_name`*

   ONTAP requiere la clave secreta del SPN desde el KDC para habilitar la interfaz Kerberos.

   Para los KDC de Microsoft, se contacta con el KDC y se emite un mensaje de nombre de usuario y contraseña en la CLI para obtener la clave secreta. Si necesita crear el SPN en una OU diferente del dominio Kerberos, puede especificar el `-ou` parámetro opcional.

   Para los KDC que no son de Microsoft, la clave secreta se puede obtener utilizando uno de los dos métodos:

Si…	**También debe incluir el siguiente parámetro con el comando…**
Tenga las credenciales de administrador de KDC para recuperar la clave directamente desde el KDC	`-admin-username` *`kdc_admin_username`*
No tiene las credenciales de administrador de KDC, pero tiene un archivo keytab del KDC que contiene la clave	`-keytab-uri` {ftp

2. Compruebe que Kerberos estaba habilitado en la LIF:

   `vserver nfs kerberos-config show`

3. Repita los pasos 1 y 2 para habilitar Kerberos en varios LIF.

Ejemplo

El siguiente comando crea y verifica una configuración Kerberos de NFS para la SVM denominada vs1 en la interfaz lógica ves03-d1, con el SPN nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM en la OU lab2ou:

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
        Logical
Vserver Interface Address       Kerberos  SPN
------- --------- -------       --------- ------------------------------
vs0     ves01-a1
                  10.10.10.30   disabled  -
vs2     ves01-d1
                  10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

Añadir capacidad de almacenamiento a una SVM habilitada para NFS

Obtenga información sobre cómo agregar capacidad de almacenamiento a un SVM habilitado para NFS de ONTAP

Para añadir capacidad de almacenamiento a una SVM habilitada para NFS, debe crear un volumen o un qtree para proporcionar un contenedor de almacenamiento y crear o modificar una política de exportación para ese contenedor. Después, puede verificar el acceso del cliente NFS desde el clúster y probar el acceso desde los sistemas cliente.

Antes de empezar

- NFS debe estar configurado completamente en la SVM.
- La política de exportación predeterminada del volumen raíz de la SVM debe contener una regla que permita el acceso a todos los clientes.
- Se debe completar cualquier actualización de la configuración de los servicios de nombres.
- Deben completarse todas las adiciones o modificaciones que se realicen en una configuración de Kerberos.

Crear una política de exportación de NFS de ONTAP

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

Pasos

1. Cree una política de exportación:

   `vserver export-policy create -vserver` *`vserver_name`* `-policyname` *`policy_name`*

   El nombre de la política puede tener hasta 256 caracteres.

2. Compruebe que se ha creado la política de exportación:

```
vserver export-policy show -policyname policy_name
```

Ejemplo

Los siguientes comandos crean y verifican la creación de una política de exportación llamada exp1 en la SVM llamada vs1:

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
---------------  -------------------
vs1              exp1
```

Agregar una regla a una política de exportación de NFS de ONTAP

Sin reglas, la política de exportación no puede ofrecer a los clientes acceso a los datos. Para crear una nueva regla de exportación, debe identificar los clientes y seleccionar un formato de coincidencia de cliente, seleccionar los tipos de acceso y seguridad, especificar una asignación de ID de usuario anónimo, seleccionar un número de índice de regla y seleccionar el protocolo de acceso. A continuación, puede usar `vserver export-policy rule create` el comando para añadir la nueva regla a una política de exportación.

Antes de empezar

- La política de exportación a la que desea añadir las reglas de exportación ya debe existir.
- DNS debe haberse configurado correctamente en la SVM de datos y los servidores DNS deben tener entradas correctas para los clientes NFS.

  Esto se debe a que ONTAP realiza búsquedas de DNS mediante la configuración de DNS de la SVM de datos para determinados formatos de coincidencia del cliente. Además, si se produce un error en la coincidencia de reglas de política de exportación, se puede evitar el acceso a los datos del cliente.

- Si va a autenticarse con Kerberos, debe haber determinado cuál de los siguientes métodos de seguridad se utiliza en sus clientes NFS:
  - `krb5` (Protocolo Kerberos V5)
  - `krb5i` (Protocolo Kerberos V5 con comprobación de integridad con sumas de comprobación)
  - `krb5p` (Protocolo Kerberos V5 con servicio de privacidad)

Acerca de esta tarea

No es necesario crear una nueva regla si una regla existente en una política de exportación cubre las coincidencias del cliente y los requisitos de acceso.

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

Pasos

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

`-clientmatch`La opción especifica los clientes a los que se aplica la regla. Se pueden especificar valores de coincidencia de clientes individuales o múltiples; las especificaciones de varios valores deben estar separadas por comas. Puede especificar la coincidencia en cualquiera de los siguientes formatos:

Formato de coincidencia del cliente	Ejemplo
Nombre de dominio precedido por "." carácter	`.example.com` o. `.example.com,.example.net,...`
Nombre de host	`host1` o. `host1,host2, ...`
Dirección IPv4	`10.1.12.24` o. `10.1.12.24,10.1.12.25, ...`
Dirección IPv4 con una máscara de subred expresada como un número de bits	`10.1.12.10/4` o. `10.1.12.10/4,10.1.12.11/4,...`
La dirección IPv4 con una máscara de red	`10.1.16.0/255.255.255.0` o. `10.1.16.0/255.255.255.0,10.1.17.0/255.255.255.0,...`
Dirección IPv6 en formato punteado	`::1.2.3.4` o. `::1.2.3.4,::1.2.3.5,...`
Dirección IPv6 con una máscara de subred expresada como un número de bits	`ff::00/32` o. `ff::00/32,ff::01/32,...`
Un solo netgroup con el nombre del netgroup precedido por el carácter @	`@netgroup1` o. `@netgroup1,@netgroup2,...`

También puede combinar tipos de definiciones de cliente; por ejemplo, `.example.com,@netgroup1`.

Al especificar direcciones IP, tenga en cuenta lo siguiente:

- No se permite introducir un rango de direcciones IP, como 10.1.12.10-10.1.12.70.

  Las entradas con este formato se interpretan como cadenas de texto y se consideran nombres de host.

- Al especificar direcciones IP individuales en reglas de exportación para la gestión granular del acceso a clientes, no especifique direcciones IP que se encuentren asignadas de forma dinámica (por ejemplo, DHCP) o temporalmente (por ejemplo, IPv6).

  De lo contrario, el cliente pierde el acceso cuando cambia su dirección IP.

- No se permite introducir una dirección IPv6 con una máscara de red, como ff::12/ff::00.

2. Seleccione los tipos de acceso y seguridad de las coincidencias del cliente.

   Puede especificar uno o varios de los siguientes modos de acceso a los clientes que se autentican con los tipos de seguridad especificados:

   - `-rorule` (acceso de solo lectura)
   - `-rwrule` (acceso de lectura y escritura)
   - `-superuser` (acceso a raíz)

   > Un cliente solo puede obtener acceso de lectura y escritura para un tipo de seguridad específico si la regla de exportación permite también el acceso de solo lectura para ese tipo de seguridad. Si el parámetro de solo lectura es más restrictivo para un tipo de seguridad que el parámetro de lectura y escritura, es posible que el cliente no obtenga acceso de lectura/escritura. Lo mismo es cierto para el acceso de superusuario.

   Puede especificar una lista separada por comas de varios tipos de seguridad para una regla. Si especifica el tipo de seguridad `any` como o `never`, no especifique ningún otro tipo de seguridad. Elija entre los siguientes tipos de seguridad válidos:

Cuando el tipo de seguridad se establece en…	Un cliente coincidente puede acceder a los datos exportados…
`any`	Siempre, independientemente del tipo de seguridad entrante.
`none`	Si se enumera solo, a los clientes con cualquier tipo de seguridad se les concede acceso como anónimos. Si se enumera con otros tipos de seguridad, se concede acceso a los clientes con un tipo de seguridad especificado y se concede acceso como anónimos a los clientes con cualquier otro tipo de seguridad.
`never`	Nunca, independientemente del tipo de seguridad entrante.
`krb5`	Si está autenticada por Kerberos 5. Sólo autenticación: El encabezado de cada solicitud y respuesta está firmado.
`krb5i`	Si está autenticada por Kerberos 5i. Autenticación e integridad: Se firma el encabezado y el cuerpo de cada solicitud y respuesta.

Cuando el tipo de seguridad se establece en…	Un cliente coincidente puede acceder a los datos exportados…
`krb5p`	Si está autenticada por Kerberos 5p. Autenticación, integridad y privacidad: Se firma el encabezado y el cuerpo de cada solicitud y respuesta, y la carga útil de datos NFS está cifrada.
`ntlm`	Si se autentica con CIFS NTLM.
`sys`	Si se autentica mediante NFS AUTH_SYS.

El tipo de seguridad recomendado es `sys`, o si se utiliza Kerberos, `krb5`, `krb5i` o `krb5p`.

Si utiliza Kerberos con NFSv3, la regla de política de exportación debe permitir `-rorule` y `-rwrule` acceder a `sys` además `krb5` de . Esto se debe a la necesidad de permitir el acceso de Network Lock Manager (NLM) a la exportación.

3. Especifique una asignación de ID de usuario anónimo.

```
`-anon`La opción especifica un ID de usuario de UNIX o un nombre de
usuario asignado a solicitudes de cliente que llegan con un ID de
usuario de 0 (cero), que normalmente está asociado con el nombre de
usuario root. El valor predeterminado es `65534`. Los clientes NFS
normalmente asocian el ID de usuario 65534 con el nombre de usuario
nobody (también conocido como _root squashing_). En ONTAP, este ID de
usuario está asociado con el usuario pcuser. Para desactivar el acceso
de cualquier cliente con un ID de usuario de 0, especifique un valor de
`65535`.
```

4. Seleccione el orden de índice de reglas.

```
`-ruleindex`La opción especifica el número de índice de la regla. Las
reglas se evalúan según su orden en la lista de números de índice; las
reglas con números de índice más bajos se evalúan primero. Por ejemplo,
la regla con el número de índice 1 se evalúa antes que la regla con el
número de índice 2.
```

Si va a añadir…	Realice lo siguiente…
La primera regla a una política de exportación	Introduzca `1`.

Si va a añadir…	Realice lo siguiente…
Reglas adicionales a una política de exportación	a. Mostrar reglas existentes en la política: `vserver export-policy rule show -instance -policyname your_policy` b. Seleccione un número de índice para la nueva regla dependiendo de la orden en la que se debe evaluar.

5. Seleccione el valor de acceso NFS aplicable{`nfs`|`nfs3`|`nfs4`: }.

   `nfs` coincide con cualquier versión y `nfs3` `nfs4` solo coincide con esas versiones específicas.

6. Cree la regla de exportación y añádala a una política de exportación existente:

   `vserver export-policy rule create -vserver vserver_name -policyname policy_name -ruleindex integer -protocol {nfs|nfs3|nfs4} -clientmatch { text | "text,text,…" } -rorule security_type -rwrule security_type -superuser security_type -anon user_ID`

7. Muestre las reglas de la política de exportación para verificar que la nueva regla esté presente:

   `vserver export-policy rule show -policyname policy_name`

   El comando muestra un resumen de esa política de exportación, incluida una lista de reglas aplicadas a esa política. ONTAP asigna a cada regla un número de índice de regla. Una vez que conozca el número de índice de regla, puede utilizarlo para mostrar información detallada acerca de la regla de exportación especificada.

8. Compruebe que las reglas aplicadas a la política de exportación se han configurado correctamente:

   `vserver export-policy rule show -policyname policy_name -vserver vserver_name -ruleindex integer`

Ejemplos

Los siguientes comandos crean y verifican la creación de una regla de exportación en la SVM llamada vs1 en una política de exportación llamada rs1. La regla tiene el número de índice 1. La regla coincide con cualquier cliente del dominio eng.company.com y el netgroup @netgroup1. La regla habilita todo el acceso NFS. Permite el acceso de solo lectura y de lectura y escritura a los usuarios autenticados con AUTH_SYS. Los clientes con el ID de usuario de UNIX 0 (cero) se anóniman a menos que se autentiquen con Kerberos.

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname exp1
-ruleindex 1 -protocol nfs
-clientmatch .eng.company.com,@netgoup1 -rorule sys -rwrule sys -anon
65534 -superuser krb5

vs1::> vserver export-policy rule show -policyname nfs_policy
Virtual      Policy         Rule    Access    Client           RO
Server       Name           Index   Protocol  Match            Rule
------------ -------------- ------  --------  ---------------- ------
vs1          exp1           1       nfs       eng.company.com, sys
                                              @netgroup1

vs1::> vserver export-policy rule show -policyname exp1 -vserver vs1
-ruleindex 1

                                Vserver: vs1
                            Policy Name: exp1
                             Rule Index: 1
                           Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
                            RO Access Rule: sys
                            RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
                  Superuser Security Types: krb5
              Honor SetUID Bits in SETATTR: true
                 Allow Creation of Devices: true
```

Los siguientes comandos crean y verifican la creación de una regla de exportación en la SVM llamada vs2 en una política de exportación llamada expol2. La regla tiene el número de índice 21. La regla coincide con los clientes con los miembros del netgroup dev_netgroup_main. La regla habilita todo el acceso NFS. Permite el acceso de solo lectura para los usuarios que se autentican con AUTH_SYS y requiere autenticación de Kerberos para acceso de lectura/escritura y raíz. A los clientes con el ID de usuario de UNIX 0 (cero) se les deniega el acceso raíz a menos que se autentiquen con Kerberos.

```
vs2::> vserver export-policy rule create -vserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5

vs2::> vserver export-policy rule show -policyname nfs_policy
Virtual  Policy       Rule    Access    Client              RO
Server   Name         Index   Protocol  Match               Rule
-------- ------------ ------  --------  ------------------  ------
vs2      expol2       21       nfs      @dev_netgroup_main  sys

vs2::> vserver export-policy rule show -policyname expol2 -vserver vs1
-ruleindex 21

                                Vserver: vs2
                            Policy Name: expol2
                             Rule Index: 21
                          Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
                                         @dev_netgroup_main
                          RO Access Rule: sys
                          RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
                 Superuser Security Types: krb5
             Honor SetUID Bits in SETATTR: true
                Allow Creation of Devices: true
```

Cree un volumen o un contenedor de almacenamiento Qtree

Crear un volumen NFS de ONTAP

Puede crear un volumen y especificar su punto de unión y otras propiedades mediante `volume create` el comando.

Acerca de esta tarea

Un volumen debe incluir una *ruta de unión* para que sus datos estén disponibles para los clientes. Puede especificar la ruta de unión cuando cree un nuevo volumen. Si crea un volumen sin especificar una ruta de unión, debe *mount* el volumen en el espacio de nombres de la SVM con `volume mount` el comando.

Antes de empezar

- NFS debe estar configurado y en ejecución.
- El estilo de seguridad de la SVM debe ser UNIX.
- A partir de ONTAP 9.13.1, se pueden crear volúmenes con análisis de capacidad y seguimiento de actividades habilitados. Para activar la capacidad o el seguimiento de actividad, ejecute el `volume create` comando con `-analytics-state` o `-activity-tracking-state` establezca en `on`.

Para obtener más información sobre el análisis de capacidad y el seguimiento de actividades, consulte "Active File System Analytics". Obtenga más información sobre `volume create` en el "Referencia de comandos del ONTAP".

Pasos

1. Cree el volumen con un punto de unión:

   `volume create -vserver` *`svm_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {`*`integer`*`[KB|MB|GB|TB|PB]} -security-style unix -user` *`user_name_or_number`* `-group` *`group_name_or_number`* `-junction-path` *`junction_path`* `[-policy` *`export_policy_name`*`]`

   Las opciones para `-junction-path` son las siguientes:

   - Directamente bajo raíz, por ejemplo, */new_vol*

     Puede crear un nuevo volumen y especificar que se monte directamente en el volumen raíz de SVM.

   - En un directorio existente, por ejemplo, */existing_dir/new_vol*

     Puede crear un nuevo volumen y especificar que se monte en un volumen existente (en una jerarquía existente), expresado como un directorio.

     Si desea crear un volumen en un nuevo directorio (en una jerarquía nueva en un volumen nuevo), por ejemplo, */new_dir/new_vol*, primero debe crear un volumen primario nuevo que esté unido al volumen raíz de la SVM. A continuación, creará el nuevo volumen secundario en la ruta de unión del nuevo volumen principal (nuevo directorio).

   + Si planea utilizar una política de exportación existente, puede especificarla al crear el volumen. También puede agregar una política de exportación más adelante con `volume modify` el comando.

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

   `volume show -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction`

Ejemplos

El siguiente comando crea un nuevo volumen denominado user1 en la SVM vs1.example.com y el agregado aggr1. El nuevo volumen está disponible en `/users`. El tamaño del volumen es de 750 GB y su garantía de volumen es del tipo volumen (de forma predeterminada).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver          Volume    Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  users1    true     /users          RW_volume
```

El siguiente comando crea un nuevo volumen llamado «home4» en la SVM "vs1.example.com" y el agregado «aggr1». El directorio `/eng/` ya existe en el espacio de nombres para la SVM de VS1, y el nuevo volumen está disponible en `/eng/home`, que se convierte en el directorio inicial del `/eng/` espacio de nombres. El volumen tiene un tamaño de 750 GB y su garantía de volumen es de tipo `volume` (de forma predeterminada).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

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

Crear un qtree NFS de ONTAP

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

Antes de empezar

- La SVM y el volumen que contendrán el nuevo qtree ya deben existir.
- El estilo de seguridad de la SVM debe ser UNIX y el NFS debe configurarse y ejecutarse.

Pasos

1. Cree el qtree:

   `volume qtree create -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `} -security-style unix [-policy` *`export_policy_name`*`]`

   Puede especificar el volumen y el qtree como argumentos independientes, o bien especificar el argumento de la ruta de qtree en el formato `/vol/`*`volume_name/_qtree_name`*.

   De forma predeterminada, los qtrees heredan las políticas de exportación de su volumen principal, pero se pueden configurar para que utilicen las suyas propias. Si piensa utilizar una política de exportación existente, puede especificarla al crear el qtree. También puede agregar una política de exportación más adelante con `volume qtree modify` el comando.

2. Compruebe que el qtree se ha creado con la ruta de unión que desee:

   `volume qtree show -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `}`

Ejemplo

En el ejemplo siguiente se crea un qtree llamado qt01 ubicado en la SVM vs1.example.com que tiene una ruta de unión `/vol/data1`:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style unix
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                    Security Style: unix
                       Oplock Mode: enable
                  Unix Permissions: ---rwxr-xr-x
                          Qtree Id: 2
                      Qtree Status: normal
                     Export Policy: default
        Is Export Policy Inherited: true
```

Acceso seguro a NFS mediante políticas de exportación

Obtenga información sobre cómo proteger el acceso a ONTAP NFS mediante políticas de exportación

Puede utilizar las políticas de exportación para restringir el acceso de NFS a volúmenes o qtrees a clientes que coincidan con parámetros específicos. Al aprovisionar almacenamiento nuevo, puede usar una política y reglas existentes, agregar reglas a una política existente o crear una nueva política y reglas. También puede comprobar la configuración de las políticas de exportación

> A partir de ONTAP 9.3, puede habilitar la comprobación de la configuración de la política de exportación como un trabajo en segundo plano que registra cualquier infracción de reglas en una lista de reglas de error. `vserver export-policy config-checker`Los comandos invocan el comprobador y muestran los resultados, que puede utilizar para verificar la configuración y eliminar reglas erróneas de la política.Los comandos solo validan la configuración de exportación para nombres de host, grupos de red y usuarios anónimos.

Administrar el orden de procesamiento de las reglas de exportación de ONTAP NFS

Puede utilizar `vserver export-policy rule setindex` el comando para definir manualmente el número de índice de una regla de exportación existente. Esto le permite especificar la prioridad mediante la cual ONTAP aplica reglas de exportación a las solicitudes de clientes.

Acerca de esta tarea

Si el nuevo número de índice ya está en uso, el comando inserta la regla en el punto especificado y vuelve a ordenar la lista en consecuencia.

Paso

1. Modifique el número de índice de una regla de exportación especificada:

   ```
   vserver export-policy rule setindex -vserver virtual_server_name -policyname
   policy_name -ruleindex integer -newruleindex integer
   ```

Ejemplo

El siguiente comando cambia el número de índice de una regla de exportación en el número de índice 3 al número de índice 2 de una política de exportación denominada r1 en la SVM denominada vs1:

```
vs1::> vserver export-policy rule setindex -vserver vs1
-policyname rs1 -ruleindex 3 -newruleindex 2
```

Asignar una política de exportación NFS de ONTAP a un volumen

Cada volumen incluido en la SVM debe estar asociado a una política de exportación que contenga reglas de exportación para que los clientes accedan a los datos del volumen.

Acerca de esta tarea

Es posible asociar una política de exportación a un volumen cuando se crea el volumen o en cualquier momento después de crearlo. Es posible asociar una política de exportación al volumen, aunque otra se puede asociar a muchos volúmenes.

Pasos

1. Si no se especificó una política de exportación cuando se creó el volumen, asigne una política de exportación al volumen:

   ```
   volume modify -vserver vserver_name -volume volume_name -policy
   export_policy_name
   ```

2. Compruebe que la política se haya asignado al volumen:

   ```
   volume show -volume volume_name -fields policy
   ```

Ejemplo

Los siguientes comandos asignan la política de exportación nfs_policy al volumen vol1 en la SVM vs1 y verifican la asignación:

```
cluster::> volume modify -v1server vs1 -volume vol1 -policy nfs_policy

cluster::>volume show -volume vol -fields policy
vserver volume       policy
------- ------------ ----------------
vs1     vol1         nfs_policy
```

Asignar una política de exportación NFS de ONTAP a un qtree

En lugar de exportar un volumen completo, también puede exportar un qtree concreto de un volumen para que los clientes puedan acceder a él directamente. Puede asignar una política de exportación a un qtree para exportarlo. Puede asignar la política de exportación al crear un qtree nuevo o al modificar un qtree existente.

Antes de empezar

Debe existir la política de exportación.

Acerca de esta tarea

De forma predeterminada, los qtrees heredan la política de exportación principal del volumen que contiene si no se especifica de otro modo en el momento de la creación.

Puede asociar una política de exportación a un qtree al crear el qtree o en cualquier momento después de crearlo. Puede asociar una política de exportación al qtree, aunque otra se puede asociar con muchos qtrees.

Pasos

1. Si no se especificó una política de exportación al crear el qtree, asigne una política de exportación al qtree:

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

2. Compruebe que la política se ha asignado al qtree:

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

Ejemplo

Los siguientes comandos asignan la política de exportación nfs_policy al qtree qt1 en la SVM vs1 y verifican la asignación:

```
cluster::> volume modify -v1server vs1 -qtree-path /vol/vol1/qt1 -policy
nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy
------- ------ ----- -------------
vs1     data1  qt01  nfs_policy
```

Verificar el acceso del cliente NFS de ONTAP desde el clúster

Para proporcionar acceso a un recurso compartido a clientes seleccionados, debe establecer permisos de archivo UNIX en un host de administración UNIX. Puede comprobar el acceso del cliente mediante `vserver export-policy check-access` el comando y ajustar las reglas de exportación según sea necesario.

Pasos

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

   El siguiente comando comprueba el acceso de lectura/escritura de un cliente NFSv3 con la dirección IP 1.2.3.4 en el volumen home2. El resultado del comando muestra que el volumen utiliza la política de exportación `exp-home-dir` y que el acceso es denegado.

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
-type read-write
                                    Policy    Policy     Rule
Path                    Policy      Owner     Owner Type Index  Access
----------------------- ----------- --------- ---------- ------
----------
/                       default     vs1_root  volume          1 read
/eng                    default     vs1_root  volume          1 read
/eng/home2              exp-home-dir home2    volume          1 denied

3 entries were displayed.
```

2. Examine el resultado para determinar si la política de exportación funciona según lo previsto y el acceso al cliente se comporta como se espera.

   Específicamente, debe comprobar qué política de exportación usa el volumen o el qtree y el tipo de acceso al cliente como resultado.

3. Si es necesario, vuelva a configurar las reglas de política de exportación.

Probar el acceso a ONTAP NFS desde los sistemas cliente

Después de verificar el acceso de NFS al nuevo objeto de almacenamiento, debe probar la configuración iniciando sesión en un host de administración NFS y leyendo datos desde y escribiendo datos en la SVM. A continuación, debe repetir el proceso como usuario que no sea raíz en un sistema cliente.

Antes de empezar

- El sistema cliente debe tener una dirección IP permitida por la regla de exportación especificada anteriormente.
- Debe tener la información de inicio de sesión para el usuario raíz.

Pasos

1. En el clúster, compruebe la dirección IP de la LIF que aloja el nuevo volumen:

   `network interface show –vserver` *`svm_name`*

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

2. Inicie sesión como usuario raíz en el sistema cliente host de administración.
3. Cambie el directorio a la carpeta de montaje:

   ```
   cd /mnt/
   ```

4. Cree y monte una nueva carpeta con la dirección IP de la SVM:

   a. Crear una nueva carpeta:
   `mkdir /mnt/folder`

   b. Monte el nuevo volumen en este nuevo directorio:
   `mount -t nfs -o hard IPAddress:/volume_name /mnt/folder`

   c. Cambie el directorio a la nueva carpeta:
   `cd folder`

   Los siguientes comandos crean una carpeta llamada test1, montan el volumen vol1 en la dirección IP 192.0.2.130 de la carpeta de montaje test1 y cambian al nuevo directorio test1:

   ```
   host# mkdir /mnt/test1
   host# mount -t nfs -o hard 192.0.2.130:/vol1 /mnt/test1
   host# cd /mnt/test1
   ```

5. Cree un archivo nuevo, compruebe que existe y escriba texto en él:

   a. Cree un archivo de prueba:
   `touch filename`

   b. Verifique que el archivo existe.:
   `ls -l filename`

   c. Introduzca:
   `cat > filename`

   Escriba algún texto y, a continuación, presione Ctrl+D para escribir texto en el archivo de prueba.

   d. Muestra el contenido del archivo de prueba.
   `cat filename`

   e. Elimine el archivo de prueba:
   `rm filename`

   f. Vuelva al directorio principal:
   `cd ..`

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

6. Como raíz, se pueden establecer los permisos y la propiedad de UNIX que se desee en el volumen montado.
7. En un sistema cliente UNIX identificado en las reglas de exportación, inicie sesión como uno de los usuarios autorizados que ahora tienen acceso al nuevo volumen y repita los procedimientos descritos en los pasos 3 a 5 para verificar que puede montar el volumen y crear un archivo.

Dónde encontrar información adicional sobre ONTAP NFS

Una vez que haya probado correctamente el acceso al cliente NFS, puede realizar una configuración de NFS adicional o añadir acceso SAN. Cuando se completa el acceso al protocolo, debe proteger el volumen raíz de la máquina virtual de almacenamiento (SVM).

Configuración de NFS

El acceso a NFS se puede configurar más utilizando la siguiente información e informes técnicos:

- "Gestión de NFS"

  Describe cómo configurar y gestionar el acceso a archivos mediante NFS.

- "Informe técnico de NetApp 4067: Guía de prácticas recomendadas e implementación de NFS"

  Sirve de guía de funcionamiento de NFSv3 y NFSv4 y ofrece una descripción general del sistema operativo de ONTAP haciendo hincapié en NFSv4.

- "Informe técnico de NetApp 4073: Autenticación unificada segura"

  Explica cómo configurar ONTAP para su uso con los servidores Kerberos versión 5 (krb5) basados en UNIX para la autenticación de almacenamiento NFS y Active Directory de Windows Server (AD) como proveedor de identidades KDC y Lightweight Directory Access Protocol (LDAP).

- "Informe técnico de NetApp 3580: Guía de mejoras y prácticas recomendadas de NFSv4: Implementación de Data ONTAP"

  Describe las prácticas recomendadas que se deben seguir mientras implementa componentes de NFSv4 en clientes AIX, Linux o Solaris conectados a sistemas que ejecutan ONTAP.

Configuración de redes

Además, puede configurar las funciones de red y los servicios de nombres mediante los siguientes informes técnicos e informati:

- "Gestión de NFS"

  Describe cómo configurar y gestionar las redes de ONTAP.

- "Informe técnico de NetApp 4182: Consideraciones de diseño y prácticas recomendadas de almacenamiento Ethernet para las configuraciones de Data ONTAP en clúster"

  Describe la implementación de las configuraciones de red de ONTAP, y proporciona escenarios comunes de puesta en marcha de redes y recomendaciones de prácticas recomendadas.

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

  Explica cómo configurar la configuración de LDAP, NIS, DNS y archivos locales con fines de autenticación.

Configuración del protocolo SAN

Si desea proporcionar o modificar el acceso SAN a la SVM nueva, puede usar la información de configuración de FC o iSCSI, que está disponible para varios sistemas operativos host.

Protección de volúmenes raíz

Después de configurar los protocolos en la SVM, debe asegurarse de que su volumen raíz esté protegido:

- "Protección de datos"

  Describe cómo crear un reflejo de uso compartido de carga para proteger el volumen raíz de SVM, que es una práctica recomendada por NetApp para SVM habilitadas para NAS. También describe cómo recuperarse rápidamente de fallos o pérdidas de volúmenes mediante la promoción del volumen raíz de SVM desde un reflejo de uso compartido de carga.

En qué se diferencian las exportaciones de ONTAP de las exportaciones de 7-Mode

En qué se diferencian las exportaciones de ONTAP de las exportaciones de 7-Mode

Si no conoce cómo implementa ONTAP las exportaciones de NFS, puede comparar las herramientas de configuración de exportación de ONTAP y 7-Mode, así como `/etc/exports` archivos de muestra de 7-Mode con reglas y políticas en clúster.

En ONTAP no hay `/etc/exports` ningún archivo ni `exportfs` comando. En su lugar, debe definir una política de exportación. Las políticas de exportación le permiten controlar el acceso de los clientes de la misma forma que en 7-Mode, pero le proporcionan funcionalidades adicionales como la capacidad de reutilizar la misma política de exportación para varios volúmenes.

Información relacionada

"Gestión de NFS"

"Informe técnico de NetApp 4067: Guía de prácticas recomendadas e implementación de NFS"

Obtenga información sobre las comparaciones de exportación de NFS de 7-Mode y ONTAP

Las exportaciones en ONTAP se definen y utilizan de forma diferente a las que se utilizan en entornos de 7-Mode.

Áreas de diferencia	7-Mode	ONTAP
Cómo se definen las exportaciones	Las exportaciones se definen en el `/etc/exports` archivo.	Las exportaciones se definen mediante la creación de una política de exportación dentro de una SVM. Una SVM puede incluir más de una política de exportación.
Ámbito de exportación	• Las exportaciones se aplican a una ruta de archivo o qtree especificados. • Debe crear una entrada separada en `/etc/exports` para cada ruta o qtree del archivo. • Las exportaciones son persistentes solo si están definidas en el `/etc/exports` archivo.	• Las políticas de exportación se aplican a un volumen completo, incluidos todos los qtrees y rutas de archivos contenidos en el volumen. • Las políticas de exportación se pueden aplicar a más de un volumen si se desea. • Todas las políticas de exportación son persistentes a través de reinicios del sistema.
Cercado (especificando un acceso diferente para clientes específicos a los mismos recursos)	Para proporcionar a clientes específicos un acceso diferente a un único recurso exportado, debe enumerar cada cliente y su acceso permitido en el `/etc/exports` archivo.	Las políticas de exportación están compuestas por varias reglas individuales de exportación. Cada regla de exportación define permisos de acceso específicos para un recurso y enumera los clientes que tienen dichos permisos. Para especificar un acceso diferente para clientes específicos, debe crear una regla de exportación para cada conjunto específico de permisos de acceso, enumerar los clientes que tienen esos permisos y, a continuación, agregar las reglas a la directiva de exportación.

Alias de nombre	Al definir una exportación, puede elegir que el nombre de la exportación sea diferente del nombre de la ruta de acceso del archivo. Debe utilizar el `-actual` parámetro al definir dicha exportación en el `/etc/exports` archivo.	Es posible optar por que el nombre del volumen exportado sea diferente del nombre del volumen real. Para ello, debe montar el volumen con un nombre de ruta de unión personalizado dentro del espacio de nombres de la SVM. De manera predeterminada, los volúmenes se montan con su nombre de volumen. Para personalizar el nombre de ruta de unión de un volumen, debe desmontarlo, cambiarle el nombre y, a continuación, volver a montarlo.

Conozca los ejemplos de políticas de exportación de NFS de ONTAP

Puede revisar el ejemplo de políticas de exportación para comprender mejor cómo funcionan las políticas de exportación en ONTAP.

Implementación de ONTAP de ejemplo para una exportación de 7-Mode

El siguiente ejemplo muestra una exportación de 7-Mode tal como aparece en el `/etc/export` archivo:

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

Para reproducir esta exportación como una política de exportación en clúster, debe crear una política de exportación con tres reglas de exportación y, a continuación, asignar la política de exportación al volumen vol1.

Regla	Elemento	Valor
Regla 1	`-clientmatch` (especificación del cliente)	`@readonly_netgroup`
`-ruleindex`(posición de la regla de exportación en la lista de reglas)	`1`	`-protocol`
`nfs`	`-rorule`(permitir acceso de sólo lectura)	`sys` (Cliente autenticado con AUTH_SYS)

Regla	Elemento	Valor
`-rwrule`(permitir acceso de lectura y escritura)	`never`	`-superuser`(permitir acceso de superusuario)
`none`(root *squashed* a anon)	Regla 2	`-clientmatch`
`@rootaccess_netgroup`	`-ruleindex`	`2`
`-protocol`	`nfs`	`-rorule`
`sys`	`-rwrule`	`sys`
`-superuser`	`sys`	Regla 3
`-clientmatch`	`@readwrite_netgroup1,@readwrite_netgroup2`	`-ruleindex`
`3`	`-protocol`	`nfs`
`-rorule`	`sys`	`-rwrule`
`sys`	`-superuser`	`none`

1. Cree una política de exportación denominada exp_vol1:

   ```
   vserver export-policy create -vserver NewSVM -policyname exp_vol1
   ```

2. Cree tres reglas con los siguientes parámetros en el comando base:
   - Comando base:
     `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1`
   - Parámetros de regla:
     `-clientmatch @readonly_netgroup -ruleindex 1 -protocol nfs -rorule sys -rwrule never -superuser none + + -clientmatch @rootaccess_netgroup -ruleindex 2 -protocol nfs -rorule sys -rwrule sys -superuser sys -clientmatch @readwrite_netgroup1,@readwrite_netgroup2 -ruleindex 3 -protocol nfs -rorule sys -rwrule sys -superuser none`
3. Asigne la política al volumen vol1:

   ```
   volume modify -vserver NewSVM -volume vol1 -policy exp_vol1
   ```

Consolidación de muestras de exportaciones de 7-Mode

En el siguiente ejemplo, se muestra `/etc/export` un archivo de 7-Mode con una línea para cada 10 qtrees:

```
/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s
```

En ONTAP, se necesita una de estas dos políticas para cada qtree: Una con una regla que incluya `-clientmatch host1519s`, o una con una regla que incluya `-clientmatch host2057s`.

1. Cree dos políticas de exportación llamadas exp_vol1q1 y exp_vol1q2:
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q1`
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q2`
2. Crear una regla para cada política:
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q1 -clientmatch host1519s -rwrule sys -superuser sys`
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q2 -clientmatch host1519s -rwrule sys -superuser sys`
3. Aplique las políticas a los qtrees:
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_1472 -export -policy exp_vol1q1`
   - [4 qtrees siguientes…]
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_2237 -export -policy exp_vol1q2`
   - [4 qtrees siguientes…]

Si posteriormente necesita añadir qtrees adicionales para esos hosts, deberá usar las mismas políticas de exportación.

Administrar NFS

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

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

Este procedimiento se realiza en las siguientes circunstancias:

- Desea comprender la gama de funcionalidades del protocolo NFS de ONTAP.

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

Comprender el acceso a archivos NAS

Espacios de nombres y puntos de unión

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

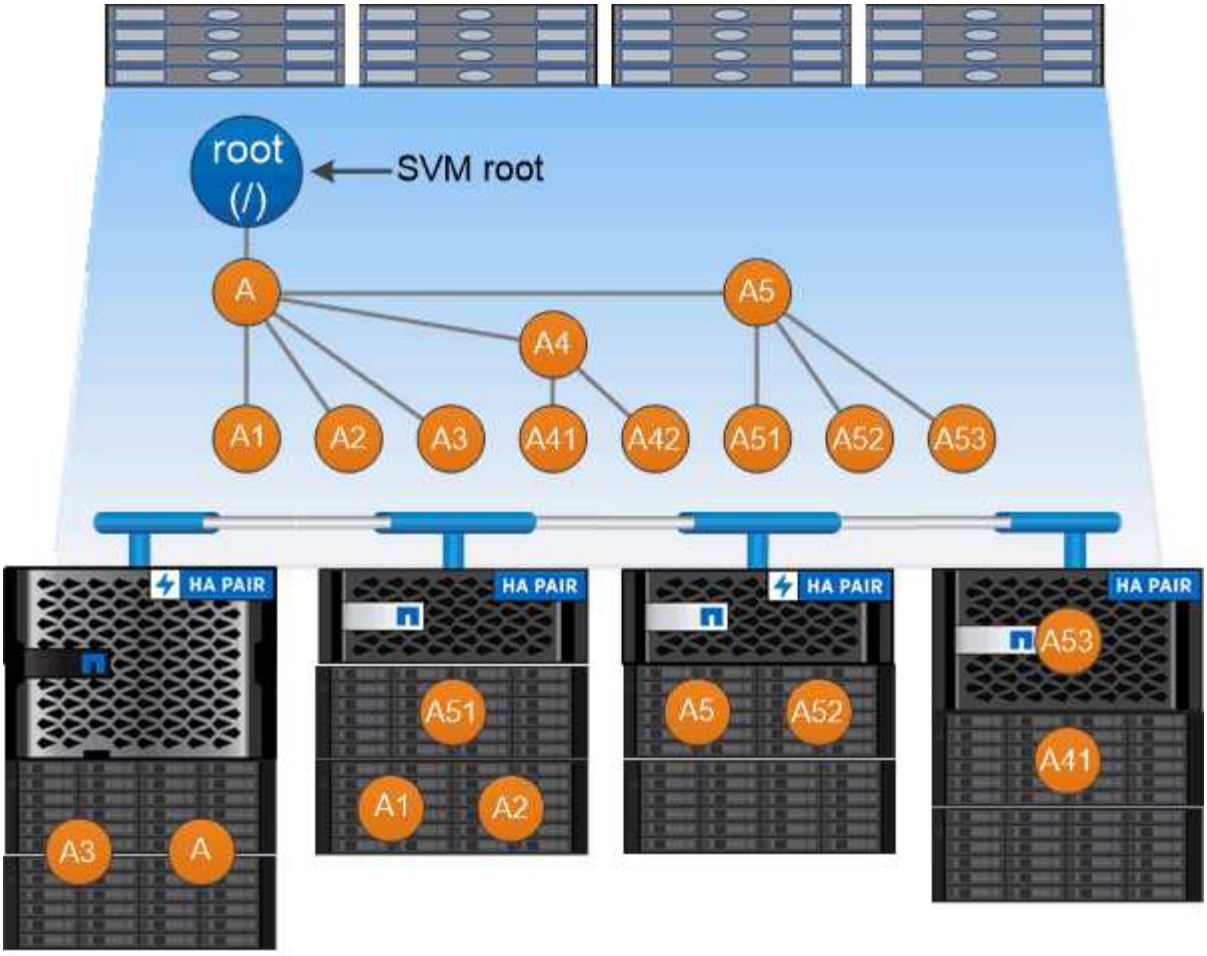
Un NAS *Namespace* es una agrupación lógica de volúmenes Unidos en *Junction points* para crear una única jerarquía de sistemas de archivos. Un cliente con permisos suficientes puede acceder a los archivos del espacio de nombres sin especificar la ubicación de los archivos en el almacenamiento. Los volúmenes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

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

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

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

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



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

Ejemplo

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

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

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

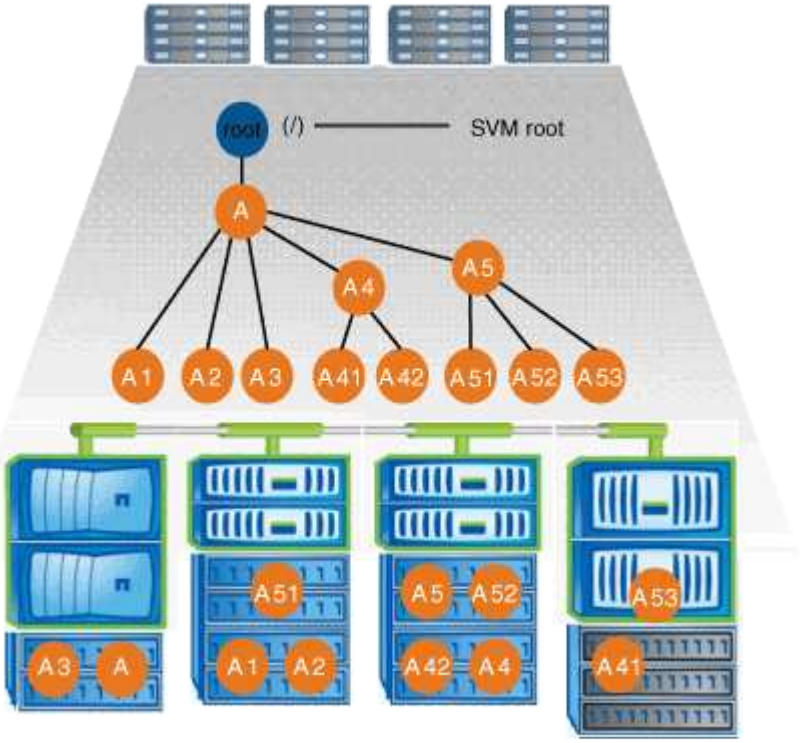
Existen varias arquitecturas de espacio de nombres NAS típicas que se pueden usar a medida que se crea el espacio de nombres de la SVM. Puede elegir la arquitectura de espacio de nombres que se ajuste a sus necesidades empresariales y de flujos de trabajo.

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

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

Espacio de nombres con árbol ramificado único

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

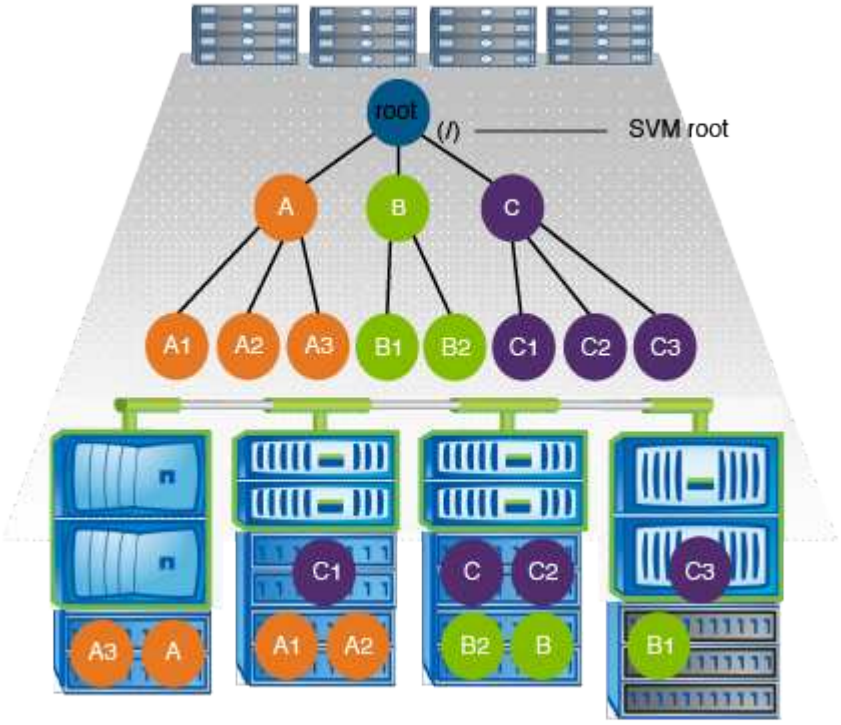


Por ejemplo, una configuración de unión de volúmenes típica con la arquitectura de espacio de nombres anterior podría tener el aspecto de la siguiente configuración, donde todos los volúmenes se unen por debajo del punto de inserción único, que es un directorio denominado «data»:

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

Espacio de nombres con varios árboles ramificados

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

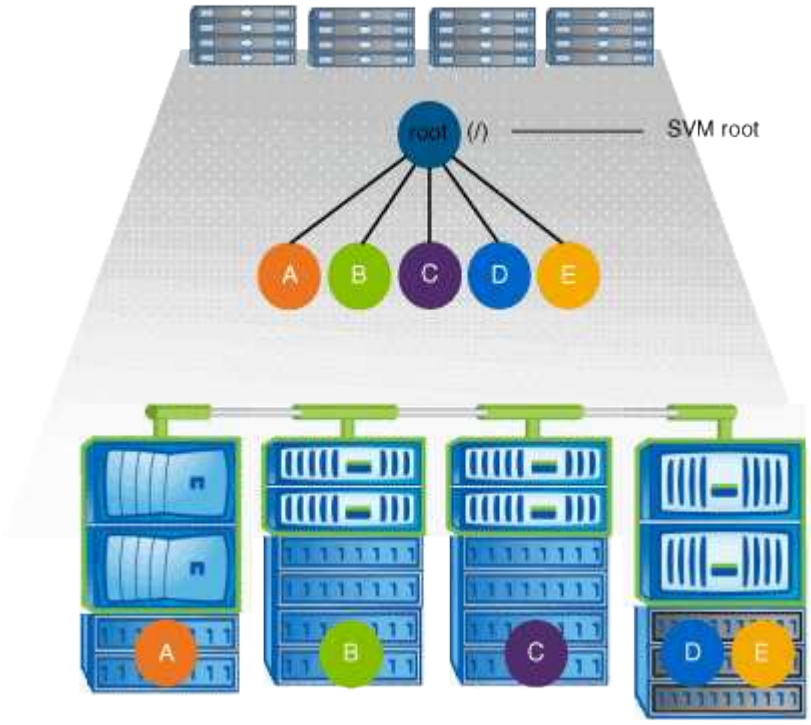


Por ejemplo, una configuración típica de unión de volúmenes con la arquitectura anterior del espacio de nombres puede parecer la siguiente configuración, donde hay tres puntos de inserción en el volumen raíz de la SVM. Dos puntos de inserción son directorios denominados «dé» y «proyectos». Un punto de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

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

Espacio de nombres con varios volúmenes independientes

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



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

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

Cómo ONTAP controla el acceso a los archivos

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

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

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

- Autenticación

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

- Autorización

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

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

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

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

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

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

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

tres niveles de seguridad.

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

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

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

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

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

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

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

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

Cómo gestiona ONTAP la autenticación del cliente NFS

Obtenga información sobre la autenticación ONTAP para clientes NAS

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

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

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

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

Descubra cómo ONTAP utiliza los servicios de nombres

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

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

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

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

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

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

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

Otorgar acceso a archivos SMB de ONTAP desde clientes NFS

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

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

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

Cómo funciona la caché de credenciales NFS de ONTAP

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

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

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

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

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

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

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

Cree y gestione volúmenes de datos en espacios de nombres NAS

Cree volúmenes NAS de ONTAP con puntos de unión específicos

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

Antes de empezar

- El agregado en el que desea crear el volumen ya debe existir.
- A partir de ONTAP 9.13.1, se pueden crear volúmenes con análisis de capacidad y seguimiento de actividades habilitados. Para activar la capacidad o el seguimiento de actividad, ejecute el `volume create` comando con `-analytics-state` o `-activity-tracking-state` establezca en `on`.

  Para obtener más información sobre el análisis de capacidad y el seguimiento de actividades, consulte "Active File System Analytics". Obtenga más información sobre `volume create` en el "Referencia de comandos del ONTAP".

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

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

Pasos

1. Cree el volumen con un punto de unión:

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

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

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

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

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

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

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

Ejemplo

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

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

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

Cree volúmenes NAS de ONTAP sin puntos de unión específicos

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

Antes de empezar

- El agregado en el que desea crear el volumen ya debe existir.
- A partir de ONTAP 9.13.1, se pueden crear volúmenes con análisis de capacidad y seguimiento de actividades habilitados. Para activar la capacidad o el seguimiento de actividad, ejecute el `volume create` comando con `-analytics-state` o `-activity-tracking-state` establezca en `on`.

  Para obtener más información sobre el análisis de capacidad y el seguimiento de actividades, consulte "Active File System Analytics". Obtenga más información sobre `volume create` en el "Referencia de comandos del ONTAP".

Pasos

1. Cree el volumen sin un punto de unión mediante el siguiente comando:

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

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

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

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

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

Ejemplo

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

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

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

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

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

Acerca de esta tarea

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

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

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

Pasos

1. Realice la acción deseada:

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

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

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

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

Ejemplos

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

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

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

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

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

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

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

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

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

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

Paso

1. Realice la acción deseada:

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

Ejemplos

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

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

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

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

Configurar estilos de seguridad

Cómo afectan los estilos de seguridad al acceso a los datos

Conozca los estilos de seguridad de ONTAP NAS

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

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

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

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

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

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

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

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

Información relacionada

- "Referencia de comandos del ONTAP"

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

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

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

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

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

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

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

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

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

Los estilos de seguridad se heredan de la siguiente manera:

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

Obtenga información sobre la conservación de permisos de ONTAP NFS UNIX

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

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

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

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

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

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

- Modificación de permisos de UNIX

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

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

- Cambiar los permisos de UNIX a los permisos NTFS

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

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

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

Configurar estilos de seguridad en volúmenes raíz SVM de ONTAP NFS

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

Pasos

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

estilo de seguridad.

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

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

   `vserver show -vserver` *`vserver_name`*

Configurar estilos de seguridad en volúmenes ONTAP NFS FlexVol

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

Pasos

1. Ejecute una de las siguientes acciones:

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

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

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

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

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

   `volume show -volume volume_name -instance`

Configurar estilos de seguridad en qtrees de ONTAP NFS

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

Pasos

1. Ejecute una de las siguientes acciones:

Si el qtree…	Usar el comando…

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

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

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

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

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

Configurar el acceso a archivos mediante NFS

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

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

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

1. Habilite el protocolo NFS en la SVM.

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

2. Cree un servidor NFS en la SVM.

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

3. Configure las políticas de exportación en la SVM.

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

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

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

Acceso seguro a NFS mediante políticas de exportación

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

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

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

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

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

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

Políticas de exportación predeterminadas para SVM NFS de ONTAP

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

Al crear una SVM, el sistema de almacenamiento crea automáticamente una política de exportación predeterminada denominada `default` para el volumen raíz de la SVM. Debe crear una o varias reglas para la política de exportación predeterminada para que los clientes puedan acceder a los datos de la SVM. También puede crear una política de exportación personalizada con reglas. Puede modificar y cambiar el nombre de la política de exportación predeterminada, pero no puede eliminar la política de exportación predeterminada.

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

Cómo funcionan las reglas de exportación de NFS de ONTAP

Las reglas de exportación son los elementos funcionales de una política de exportación. Las reglas de exportación coinciden con las solicitudes de acceso de los clientes a un volumen con los parámetros específicos que se configuran para determinar cómo se manejan las solicitudes de acceso de los clientes.

La política de exportación debe contener al menos una regla de exportación para permitir el acceso a los

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

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

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

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

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

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

> A partir de ONTAP 9.3, puede habilitar la comprobación de la configuración de la política de exportación como un trabajo en segundo plano que registra cualquier infracción de reglas en una lista de reglas de error. `vserver export-policy config-checker`Los comandos invocan al comprobador y muestran los resultados, que puede utilizar para verificar la configuración y eliminar reglas erróneas de la política.
>
> Los comandos solo validan la configuración de exportación para los nombres de host, grupos de red y usuarios anónimos.

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

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

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

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

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

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

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

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

Ejemplo

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

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

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

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

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

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

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

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

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

ID de usuario asignado a. `-anon`	**Tratamiento resultante de las solicitudes de acceso de los clientes**
`0 - 65533`	La solicitud de acceso de cliente se asigna al ID de usuario anónimo y obtiene acceso en función de los permisos configurados para este usuario.

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

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

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

Ejemplos

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

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

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

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

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

autentica con AUTH_SYS.

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

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

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

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

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

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

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

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

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

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

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

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

El tipo de seguridad con el que el cliente autenticado desempeña un rol especial en las reglas de exportación. Debe entender la manera en que el tipo de seguridad determina los niveles de acceso que el cliente obtiene a un volumen o un qtree.

Los tres niveles de acceso posibles son los siguientes:

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

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

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

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

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

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

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

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

Si el tipo de seguridad del cliente…	**A continuación, el cliente…**
Coincide con el especificado en el parámetro access.	Obtiene acceso para ese nivel con su propio ID de usuario.
No coincide con el especificado, pero el parámetro de acceso incluye la opción `none`.	Obtiene acceso para ese nivel pero como usuario anónimo con el ID de usuario especificado por el `-anon` parámetro.

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

Ejemplo

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

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

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

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

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

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

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

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

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

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

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

- `any`
- `none`

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

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

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

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

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

Ejemplo

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

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

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

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

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

El cliente #2 no obtiene acceso de superusuario. En su lugar, se asigna a Anonymous porque `-superuser`

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

Ejemplo

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Obtenga más información sobre los cachés de acceso NFS de ONTAP

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

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

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

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

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

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

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

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

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

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

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

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

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

Ejemplo

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

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

Eliminar políticas de exportación de qtrees de ONTAP NFS

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

Pasos

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

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

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

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

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

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

Acerca de esta tarea

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

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Ejecute una de las siguientes acciones:

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

3. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

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

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

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

Uso de Kerberos con NFS para una mayor seguridad

Compatibilidad de ONTAP NFS con Kerberos

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

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

- Autenticación Kerberos 5 con comprobación de integridad (krb5i)

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

- Autenticación Kerberos 5 con comprobación de privacidad (krb5p)

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

y también implica más carga.

- Cifrado AES de 128 bits y 256 bits

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

- Configuraciones en dominio de Kerberos a nivel de SVM

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

Requisitos para configurar Kerberos con ONTAP NFS

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

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

Primero deben configurarse los siguientes elementos:

Requisitos del entorno de red

- Kerberos

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

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

- Servicio de directorio

  Debe utilizar un servicio de directorio seguro en su entorno, como Active Directory u OpenLDAP, que esté configurado para usar LDAP sobre SSL/TLS.

- NTP

  Debe tener un servidor de tiempo de trabajo que ejecute NTP. Esto es necesario para evitar errores de autenticación de Kerberos debido a una desviación de tiempo.

- Resolución de nombres de dominio (DNS)

  Cada cliente UNIX y cada LIF de SVM deben tener un registro de servicio (SRV) adecuado registrado con el KDC en zonas de búsqueda inversa y de reenvío. Todos los participantes deben poder resolverse

correctamente a través de DNS.

- Cuentas de usuario

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

Requisitos del cliente NFS

- NFS

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

  Los clientes deben admitir RFC1964 y RFC2203.

- Kerberos

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

  - El cifrado para la comunicación TGS está activado.

    AES-256 para obtener la máxima seguridad.

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

    Al utilizar las credenciales de la máquina:

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

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

- DNS

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

- NTP

  Cada cliente debe sincronizarse con el servidor NTP.

- Información sobre el host y el dominio

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

- Archivos keytab

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

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

Requisitos del sistema de almacenamiento

- Licencia de NFS

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

- Licencia CIFS

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

- SVM

  Debe tener al menos una SVM configurada en el sistema.

- DNS en la SVM

  Debe haber configurado DNS en cada SVM.

- Servidor NFS

  Debe haber configurado NFS en la SVM.

- Cifrado AES

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

- Servidor SMB

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

- Volúmenes

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

- Volumen raíz

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

Nombre	Ajuste
Estilo de seguridad	UNIX

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

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

- Grupos UNIX

  La SVM debe tener configurados los siguientes grupos UNIX:

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

- Usuarios de UNIX

  La SVM debe tener configurados los siguientes usuarios de UNIX:

Nombre de usuario	ID de usuario	ID del grupo principal	Comentar
nfs	500	0	Necesario para la fase de INICIO DE GSS El primer componente del SPN de usuario del cliente NFS se utiliza como usuario.
pcuser	65534	65534	Necesario para el uso multiprotocolo de NFS y CIFS ONTAP lo crea y añade automáticamente al grupo pcuser cuando crea la SVM.
raíz	0	0	Necesario para el montaje

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

cliente NFS.

- Reglas y políticas de exportación

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

- Asignación de nombres Kerberos-UNIX

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

Información relacionada

"Informe técnico de NetApp 4073: Autenticación unificada segura"

"Herramienta de matriz de interoperabilidad de NetApp"

"Administración del sistema"

"Gestión de almacenamiento lógico"

Especifique el dominio de ID de usuario de ONTAP para NFSv4

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

Acerca de esta tarea

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

Paso

1. Introduzca el siguiente comando:

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

Configure los servicios de nombres

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

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

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

Tipos de base de datos

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

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

Tipos de origen

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

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

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

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

Especificar tipo de origen…	Para buscar información en…	Administrado por las familias de comandos…
dns	Servidores DNS externos como se especifica en la configuración de DNS de la SVM	`vserver services name-service dns`

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

Protocolos utilizados para acceder a fuentes externas

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

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

Ejemplo

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

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

Para buscar direcciones IP para hosts, ONTAP consulta primero los archivos de origen local. Si la consulta no devuelve ningún resultado, los servidores DNS se comprueban a continuación.

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

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

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

Información relacionada

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

Utilice LDAP

Obtenga más información sobre LDAP para SVM NFS de ONTAP

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

- Antes de configurar LDAP para ONTAP, debe verificar que la implementación del sitio cumple las prácticas recomendadas para la configuración del cliente y el servidor LDAP. En particular, deben cumplirse las siguientes condiciones:
  - El nombre de dominio del servidor LDAP debe coincidir con la entrada del cliente LDAP.
  - Los tipos hash de contraseña de usuario LDAP compatibles con el servidor LDAP deben incluir los compatibles con ONTAP:
    - CRIPTA (todos los tipos) y SHA-1 (SHA, SSHA).
    - A partir de los valores hash de ONTAP 9.8, SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, También se admiten SSHA-384 y SSHA-512).
  - Si el servidor LDAP requiere medidas de seguridad de la sesión, debe configurarlas en el cliente LDAP.

    Están disponibles las siguientes opciones de seguridad de la sesión:

    - La firma LDAP (proporciona comprobación de la integridad de los datos) y la firma y el sellado LDAP (proporciona cifrado y comprobación de la integridad de los datos).
    - INICIE TLS
    - LDAPS (LDAP sobre TLS o SSL)
  - Para habilitar consultas LDAP firmadas y selladas, se deben configurar los siguientes servicios:
    - Los servidores LDAP deben ser compatibles con el mecanismo SASL GSSAPI (Kerberos).
    - Los servidores LDAP deben tener registros DNS A/AAAA, así como registros PTR configurados en el servidor DNS.
    - Los servidores Kerberos deben tener registros SRV presentes en el servidor DNS.
  - Para habilitar el INICIO de TLS o LDAPS, se deben tener en cuenta los siguientes puntos.
    - Se trata de una práctica recomendada de NetApp para usar Start TLS en lugar de LDAPS.
    - Si se utiliza LDAPS, el servidor LDAP debe estar habilitado para TLS o para SSL en ONTAP 9.5 y versiones posteriores. SSL no es compatible con ONTAP 9.4 - 9.0.
    - Ya debe configurarse un servidor de certificados en el dominio.
  - Para habilitar la búsqueda de referencias LDAP (en ONTAP 9.5 y posterior), se deben cumplir las siguientes condiciones:
    - Ambos dominios deben configurarse con una de las siguientes relaciones de confianza:
      - Bidireccional

    - Unidireccional, donde la primaria confía en el dominio de referencia
    - Padre-hijo
  - El DNS debe configurarse de modo que resuelva todos los nombres de servidor a los que se hace referencia.
  - Las contraseñas de dominio deben ser las mismas para autenticarse cuando `--bind-as-cifs-server` se definen en TRUE.

> Las siguientes configuraciones no son compatibles con la búsqueda de referencias LDAP.
>
> - Para todas las versiones de ONTAP:
> - Clientes LDAP en una SVM de administrador
> - Para ONTAP 9.8 y versiones anteriores (se admiten en la versión 9.9.1 y posteriores):
> - Firma y sellado LDAP (`-session-security`opción)
> - Conexiones TLS cifradas (la `-use-start-tls` opción)
> - Comunicaciones a través del puerto LDAPS 636 (la `-use-ldaps-for-ad-ldap` opción)

- A partir de ONTAP 9.11,1, puede usar "Utilice el enlace rápido LDAP para la autenticación nsswitch para SVM NFS de ONTAP."
- Debe introducir un esquema de LDAP al configurar el cliente LDAP en la SVM.

  En la mayoría de los casos, uno de los esquemas ONTAP predeterminados será apropiado. Sin embargo, si el esquema LDAP del entorno difiere de éste, debe crear un nuevo esquema de cliente LDAP para ONTAP antes de crear el cliente LDAP. Consulte a su administrador LDAP sobre los requisitos de su entorno.

- No se admite el uso de LDAP para la resolución del nombre de host.

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

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

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

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

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

Obtenga más información sobre LDAPS para SVM NFS de ONTAP

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

Terminología

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

- **LDAP**

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

- **SSL**

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

- **TLS**

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

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

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

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

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

- **Iniciar TLS**

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

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

Cómo utiliza ONTAP LDAPS

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

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

ONTAP admite lo siguiente:

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

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

- Certificados de CA raíz autofirmados

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

De forma predeterminada, LDAPS está desactivado.

Habilitar la compatibilidad con LDAP RFC2307bis para SVM NFS de ONTAP

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

Antes de empezar

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

Acerca de esta tarea

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

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

De forma predeterminada, la compatibilidad con RFC2307bis está desactivada.

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

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

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

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

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

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

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

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

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

5. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Opciones de configuración de ONTAP NFS para búsquedas en directorios LDAP

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

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

Valores de búsqueda base y ámbito predeterminados

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

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

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

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

Valores de búsqueda de base y ámbito personalizados

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

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

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

Varios valores DN base personalizados

Si su estructura de directorios LDAP es más compleja, puede ser necesario especificar varios DNS base para buscar varias partes del directorio LDAP para cierta información. Puede especificar varios DNS para los parámetros de DN de usuario, grupo y grupo de red separándolos con punto y coma (;) y encerrando toda la

lista de búsqueda de DN con comillas dobles ("). Si un DN contiene un punto y coma, debe agregar un carácter de escape (\) inmediatamente antes del punto y coma en el DN.

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

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

Filtros de búsqueda LDAP personalizados

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

Un ejemplo de filtros válidos son:

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

Más información sobre "Cómo configurar LDAP en ONTAP".

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

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

Antes de empezar

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

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

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

Acerca de esta tarea

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

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

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

Pasos

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

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

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

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

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

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

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

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

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

Ejemplo

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

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

Después de terminar

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

Información relacionada

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

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

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

Acerca de esta tarea

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

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

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

"Aprenda sobre el uso de FAST BIND."

Antes de empezar

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

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

- Los usuarios del administrador de ONTAP deben estar configurados en un servidor LDAP que admita el enlace rápido.
- La SVM de ONTAP debe configurarse para LDAP en la base de datos de switches de servicios de nombres (nsswitch).
- Las cuentas de usuario y de grupo admin de ONTAP deben configurarse para la autenticación nsswitch mediante fast bind.
- El número UID y el número GID del administrador deben estar rellenados y ser consultables para que la vinculación rápida tenga éxito.

Pasos

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

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

      `vserver services name-service ldap client show`

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

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

      `vserver services name-service ns-switch show`

   "Más información sobre la configuración de nsswitch."

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

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

      `-authentication-method nsswitch`

      `-is-ldap-fastbind true`

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

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

Mostrar estadísticas LDAP para SVM NFS de ONTAP

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

Antes de empezar

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

Paso

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

   `statistics show`

Ejemplos

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

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

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

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

Información relacionada

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

Configurar las asignaciones de nombres

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

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

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

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

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

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

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

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

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

- Para la asignación de Windows a UNIX

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

- De asignación de UNIX a Windows

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

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

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

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

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

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

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

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

- *Confianza bidireccional*

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

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

- *Confianza saliente*

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

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

- *Confianza entrante*

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

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

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

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

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

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

Cómo se realizan las búsquedas de nombres multidominio

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

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

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

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

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

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

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

como en el `sed` programa UNIX.

Crear asignaciones de nombres para SVM de ONTAP NAS

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

Acerca de esta tarea

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

Paso

1. Crear una asignación de nombres:

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

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

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

Ejemplos

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

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

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

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

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

Windows ENG\ john$OPS al usuario UNIX john_OPS.

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

Configurar el usuario predeterminado para las SVM de ONTAP NAS

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

Acerca de esta tarea

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

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

Paso

1. Ejecute una de las siguientes acciones:

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

Comandos ONTAP para administrar asignaciones de nombres NFS

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

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

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

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

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

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

Acerca de esta tarea

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

Antes de empezar

Debe estar habilitado NFSv3 en la SVM.

Pasos

1. Habilitar la compatibilidad con clientes de Windows NFSv3:

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

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

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

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

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

Esto es necesario para garantizar montajes fiables.

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

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

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

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

Ejemplo

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

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

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

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

Gestione el acceso a archivos mediante NFS

Habilitar o deshabilitar NFSv3 para SVM de ONTAP

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

Paso

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el comando…
Habilitar NFSv3	`vserver nfs modify -vserver vserver_name -v3 enabled`

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

Habilitar o deshabilitar NFSv4.0 para SVM de ONTAP

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

Paso

1. Ejecute una de las siguientes acciones:

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

Habilitar o deshabilitar NFSv4.1 para SVM de ONTAP

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

Paso

1. Ejecute una de las siguientes acciones:

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

Administrar los límites del grupo de almacenamiento de ONTAP NFSv4

A partir de ONTAP 9,13, los administradores pueden permitir que sus servidores NFSv4 denieguen recursos a NFSv4 clientes cuando hayan alcanzado los límites de recursos por cada pool de clientes. Cuando los clientes consumen demasiados recursos de la agrupación de almacenamiento NFSv4, esto puede provocar que otros clientes NFSv4

se bloqueen debido a la falta de disponibilidad de los recursos de la agrupación de almacenamiento NFSv4.

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

Ver los recursos del almacén consumidos

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

Paso

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

Ejemplo

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

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

Node: node1

Vserver: vs1

Data-Ip: 10.0.1.1

Client-Ip Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount

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

10.0.2.1          nfs4.1     true    2 1 0 4

10.0.2.2          nfs4.2     true    2 1 0 4

2 entries were displayed.
```

Activar o desactivar los controles de límite de grupo de almacenamiento

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

Paso

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

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

Ver una lista de clientes bloqueados

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

Pasos

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

Eliminar un cliente de la lista de clientes bloqueados

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

Pasos

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

Ejemplo

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

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

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

Node: node1

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

1 entries were displayed.
```

Habilitar o deshabilitar pNFS para SVM de ONTAP

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

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

Antes de empezar

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

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

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

Paso

1. Ejecute una de las siguientes acciones:

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

Información relacionada

- Descripción general de trunking NFS

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

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

Acerca de esta tarea

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

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

Paso

1. Ejecute una de las siguientes acciones:

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

Controlar solicitudes NFS desde puertos no reservados para SVM de ONTAP

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

Acerca de esta tarea

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

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

Estas opciones no se aplican al procedimiento NULL.

Paso

1. Ejecute una de las siguientes acciones:

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

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

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

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

Antes de empezar

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

Acerca de esta tarea

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

- Denegar el acceso a usuarios UNIX desconocidos.

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

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

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

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Ejecute una de las siguientes acciones:

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

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

3. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

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

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

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

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

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

Acerca de esta tarea

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

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

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

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

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Realice la acción deseada:

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

3. Configure el nivel de privilegio en admin:

   ```
   set -privilege admin
   ```

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

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

Antes de empezar

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

Acerca de esta tarea

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

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

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Desactivar el acceso a NFS:

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

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

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

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

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

4. Habilitar el acceso a NFS:

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

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

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

6. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Ejemplo

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

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

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

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

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

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

Comandos de ONTAP para gestionar servidores NFS

Hay comandos ONTAP específicos para gestionar los servidores NFS.

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

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

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

Solucionar problemas de servicio de nombres para SVM NAS de ONTAP

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

Acerca de esta tarea

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

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

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

Pasos

1. Ejecute una de las siguientes acciones:

Para recuperar…	Usar el comando…

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

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

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

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

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

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

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

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

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

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

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

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

Información relacionada

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

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

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

Acerca de esta tarea

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

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

Paso

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

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

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

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

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

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

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

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

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

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

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

Información relacionada

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

Comandos ONTAP para administrar la caché del servicio de nombres NAS

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

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

Información relacionada

"Referencia de comandos del ONTAP"

Comandos ONTAP para administrar asignaciones de nombres NFS

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

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

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

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

Comandos ONTAP para administrar usuarios locales de UNIX en NAS

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

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

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

Comandos ONTAP para administrar grupos locales de UNIX NAS

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

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

Eliminar un usuario de un grupo UNIX local	`vserver services name-service unix-group deluser`
Elimine un grupo UNIX local	`vserver services name-service unix-group delete`

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

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

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

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

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

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

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

Acerca de esta tarea

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

Paso

1. Ejecute una de las siguientes acciones:

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

Si desea…	Usar el comando…
Modificar los límites de usuarios UNIX locales	`vserver services unix-user max-limit modify`
Modificar los límites de grupos UNIX locales	`vserver services unix-group max-limit modify`

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

Comandos ONTAP para administrar grupos de redes locales NFS

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

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

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

Comandos ONTAP para administrar configuraciones de dominios NIS NFS

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

Si desea…	Se usa este comando…
Cree una configuración de dominio NIS	`vserver services name-service nis-domain create`
Mostrar configuraciones de dominio NIS	`vserver services name-service nis-domain show`
Mostrar el estado de enlace de una configuración de dominio NIS	`vserver services name-service nis-domain show-bound`

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

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

Comandos ONTAP para administrar configuraciones de cliente LDAP NFS

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

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

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

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

Comandos ONTAP para administrar configuraciones LDAP de NFS

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

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

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

Comandos ONTAP para administrar plantillas de esquema de cliente LDAP NFS

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

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

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

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

Comandos ONTAP para administrar configuraciones de interfaz Kerberos de NFS

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

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

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

Comandos ONTAP para administrar configuraciones de dominio Kerberos de NFS

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

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

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

Comandos de ONTAP para gestionar políticas de exportación

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

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

Copiar una política de exportación	`vserver export-policy copy`
Eliminar una política de exportación	`vserver export-policy delete`

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

Comandos de ONTAP para administrar reglas de exportación

Hay comandos ONTAP específicos para gestionar las reglas de exportación.

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

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

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

Configure la caché de credenciales NFS

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

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

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

Razones

Considere cambiar el TTL predeterminado en las siguientes circunstancias:

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

Consecuencias

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

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

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

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

Acerca de esta tarea

Estos parámetros están disponibles en el nivel de privilegios avanzado.

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Realice la acción deseada:

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

3. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Gestione las cachés de la política de exportación

Vaciar cachés de políticas de exportación para SVM de ONTAP NAS

ONTAP usa varios cachés de políticas de exportación para almacenar información relacionada con las políticas de exportación para agilizar el acceso. Vaciar las cachés de política de exportación manualmente (`vserver export-policy cache flush`)

Elimina la información potencialmente obsoleta y obliga a ONTAP a recuperar la información actual de los recursos externos correspondientes. Esto puede ayudar a resolver diversos problemas relacionados con el acceso de clientes a exportaciones NFS.

Acerca de esta tarea

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

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

Pasos

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

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

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

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

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

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

Paso

1. Ejecute una de las siguientes acciones:

Para mostrar el grupo de red de la directiva de exportación…	Introduzca el comando…
Cola	`vserver export-policy netgroup queue show`
Almacenamiento en caché	`vserver export-policy netgroup cache show -vserver vserver_name`

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

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

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

Acerca de esta tarea

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

Paso

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

   El comando puede mostrar los siguientes resultados:

   - El cliente es un miembro del netgroup.

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

   - El cliente es un miembro del netgroup.

     Se encontró en la caché de netgroup de ONTAP.

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

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

Ejemplo

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

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

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

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

Acerca de esta tarea

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

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

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

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

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

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Realice la acción deseada:

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

3. Compruebe la nueva configuración de parámetros:

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

4. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Administrar bloqueos de archivos

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

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

ONTAP bloquea los archivos depende del protocolo del cliente.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Para evitar problemas causados por el cambio de nombre de los componentes de la ruta de acceso, puede aplicar la configuración de seguridad Lista de control de acceso (ACL) de Windows que impide que los usuarios o aplicaciones cambien el nombre de los directorios críticos.

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

Mostrar información sobre bloqueos para SVM NFS de ONTAP

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

Acerca de esta tarea

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

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

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

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

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

Paso

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

Ejemplos

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

```
cluster1::> vserver locks show

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

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

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

                  Vserver: vs1
                   Volume: data2_2
        Logical Interface: lif2
              Object Path: /data2/data2_2/intro.pptx
                Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
            Lock Protocol: cifs
```

```
                 Lock Type: share-level
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                   Vserver: vs1
                    Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/test.pptx
                 Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
             Lock Protocol: cifs
                 Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Romper bloqueos de archivos para SVMs NFS de ONTAP

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

Acerca de esta tarea

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

Pasos

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

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

2. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

3. Ejecute una de las siguientes acciones:

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

4. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

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

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

En NFS, el cliente realiza operaciones de I/o en un archivo mediante la recuperación de su gestor. Este

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

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

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

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

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

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

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

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

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

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

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

Acerca de esta tarea

Los valores predeterminados de las tres opciones son los siguientes:

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

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Ejecute una de las siguientes acciones:

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

3. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Gestione las ACL de NFSv4

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

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

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

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

Obtenga información sobre las ACL de NFSv4 para SVM de ONTAP

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

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

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

  Una ACL principal se hereda incluso si `-v4.0-acl` se establece en `off`.

- Si la solicitud incluye sólo permisos de acceso estándar a archivos UNIX y el directorio principal no tiene una ACL, el modo de archivo de cliente se utiliza para establecer permisos de acceso estándar a archivos UNIX.
- Si la solicitud incluye sólo permisos de acceso estándar a archivos UNIX y el directorio primario tiene una ACL no heredable, el nuevo objeto se crea sólo con bits de modo.

Si el `-chown-mode` parámetro se ha establecido en `restricted` con comandos en `vserver nfs` `vserver export-policy rule` las familias o, la propiedad del archivo solo puede ser cambiada por el superusuario, incluso si los permisos en disco establecidos con NFSv4 ACL permiten a un usuario que no sea root cambiar la propiedad del archivo. Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

Habilitar o deshabilitar la modificación de ACL de NFSv4 para SVM de ONTAP

Cuando ONTAP recibe un `chmod` comando para un archivo o directorio con una ACL, de forma predeterminada, la ACL se conserva y se modifica para reflejar el cambio de bits de modo. Puede desactivar el `-v4-acl-preserve` parámetro para cambiar el comportamiento si desea que se borre la ACL en su lugar.

Acerca de esta tarea

Cuando se utiliza un estilo de seguridad unificado, este parámetro también especifica si los permisos de archivo NTFS se conservan o se borran cuando un cliente envía un comando chmod, chgroup o chown para un archivo o directorio.

El valor predeterminado de este parámetro es Enabled.

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el siguiente comando…
Habilitación de la retención y modificación de las ACL de NFSv4 existentes (predeterminado)	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
Deshabilite la retención y borre las ACL de NFSv4 cuando cambie los bits de modo	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

3. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Descubra cómo ONTAP utiliza las ACL de NFSv4 para determinar si puede eliminar archivos

Para determinar si puede eliminar un archivo, ONTAP utiliza una combinación del bit DE ELIMINACIÓN del archivo y el bit DELETE_CHILD del directorio que lo contiene. Para obtener más información, consulte NFS 4.1 RFC 5661.

Habilitar o deshabilitar las ACL de NFSv4 para las SVM de ONTAP

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

Acerca de esta tarea

```
`-v4.0-acl` `-v4.1-acl`La opción o controla la configuración y
visualización de las ACL de NFSv4; no controla la aplicación de estas ACL
para la comprobación de acceso.
```

Paso

1. Ejecute una de las siguientes acciones:

Si desea…	Realice lo siguiente…
Habilite las ACL de NFSv4.0	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
Deshabilitar las ACL de NFSv4.0	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`

Habilite las ACL de NFSv4.1	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`
Deshabilitar las ACL de NFSv4.1	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

Modificar el límite máximo de ACE para las ACL de NFSv4 para las SVM de ONTAP

Puede modificar el Núm. Máximo de ACE permitidos para cada ACL NFSv4 modificando el parámetro `-v4-acl-max-aces`. De forma predeterminada, el límite se establece en 400 ACE para cada ACL. El aumento de este límite puede ayudar a garantizar una correcta migración de datos con ACL que contengan más de 400 ACE en sistemas de almacenamiento que ejecuten ONTAP.

Acerca de esta tarea

Si aumenta este límite, el rendimiento de los clientes que acceden a archivos con ACL de NFSv4.

Pasos

1. Configure el nivel de privilegio en Advanced:

   `set -privilege advanced`

2. Modifique el límite máximo de ACE para ACL de NFSv4:

   `vserver nfs modify -v4-acl-max-aces max_ace_limit`

   El rango válido de

   `max_ace_limit` es a. `192` `1024.`

3. Vuelva al nivel de privilegio de administrador:

   `set -privilege admin`

Gestione las delegaciones de archivos NFSv4

Habilitar o deshabilitar las delegaciones de archivos de lectura NFSv4 para SVM de ONTAP

Para habilitar o deshabilitar las delegaciones de archivos de lectura de NFSv4, puede modificar `-v4.0-read-delegation`la opción o. Al activar las delegaciones de archivos de lectura, puede eliminar gran parte de la sobrecarga de mensajes asociada con la apertura y el cierre de archivos.

Acerca de esta tarea

De forma predeterminada, las delegaciones de archivos de lectura están deshabilitadas.

La desventaja de habilitar las delegaciones de archivos de lectura es que el servidor y sus clientes deben recuperar las delegaciones una vez que se reinicia o reinicia el servidor, se reinicia o reinicia un cliente o se produce una partición de red.

Paso

1. Ejecute una de las siguientes acciones:

Si desea…	Realice lo siguiente…
Habilitar las delegaciones de archivos de lectura de NFSv4	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled`
Habilitar las delegaciones de archivos de lectura de NFSv4.1	Introduzca el siguiente comando: + `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled`
Deshabilitar las delegaciones de archivos de lectura de NFSv4	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled`
Deshabilitar las delegaciones de archivos de lectura de NFSv4.1	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled`

Resultado

Las opciones de delegación de archivos surten efecto tan pronto como se cambien. No es necesario reiniciar o reiniciar NFS.

Habilitar o deshabilitar las delegaciones de archivos de escritura NFSv4 para SVM de ONTAP

Para habilitar o deshabilitar las delegaciones de archivos de escritura, puede modificar `-v4.0-write-delegation`la opción o. Al habilitar las delegaciones de archivos de escritura, puede eliminar gran parte de la sobrecarga de mensajes asociada con el bloqueo de archivos y registros, además de abrir y cerrar archivos.

Acerca de esta tarea

De forma predeterminada, las delegaciones de archivos de escritura están deshabilitadas.

La desventaja de habilitar las delegaciones de archivos de escritura es que el servidor y sus clientes deben realizar tareas adicionales para recuperar delegaciones una vez que se reinicia o reinicia el servidor, un cliente se reinicia o reinicia, o se produce una partición de red.

Paso

1. Ejecute una de las siguientes acciones:

Si desea…	Realice lo siguiente…
Habilite las delegaciones de archivos de escritura de NFSv4	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled`
Habilite las delegaciones de archivos de escritura de NFSv4,1	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled`
Deshabilitar las delegaciones de archivos de escritura de NFSv4	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled`
Deshabilitar las delegaciones de archivos de escritura de NFSv4.1	Introduzca el siguiente comando: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled`

Resultado

Las opciones de delegación de archivos surten efecto tan pronto como se cambien. No es necesario reiniciar o reiniciar NFS.

Configure el bloqueo de archivos y registros de NFSv4

Obtenga información sobre el bloqueo de archivos y registros NFSv4 para SVM de ONTAP

En el caso de los clientes NFSv4, ONTAP admite el mecanismo de bloqueo de archivos NFSv4 y mantiene el estado de todos los bloqueos de archivos bajo un modelo basado en arrendamiento.

"Informe técnico de NetApp 3580: Guía de mejoras y prácticas recomendadas de NFSv4: Implementación de Data ONTAP"

Especifique el período de concesión de bloqueo de NFSv4 para las SVM de ONTAP

Para especificar el periodo de concesión de bloqueo NFSv4 (es decir, el período en el que ONTAP otorga un bloqueo de forma irrevocable a un cliente), puede modificar `-v4 -lease-seconds` la opción. Los periodos de concesión más breves aceleran la recuperación del servidor, a la vez que los periodos de concesión más largos son beneficiosos para los servidores que gestionan una gran cantidad de clientes.

Acerca de esta tarea

De forma predeterminada, esta opción se establece en `30`. El valor mínimo para esta opción es `10`. El valor máximo de esta opción es el período de gracia de bloqueo, que se puede definir con la `locking.lease_seconds` opción.

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Introduzca el siguiente comando:

   ```
   vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
   ```

3. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Especifique el período de gracia de bloqueo de NFSv4 para las SVM de ONTAP

Para especificar el período de gracia de bloqueo NFSv4 (es decir, el período de tiempo en el que los clientes intentan reclamar su estado de bloqueo de ONTAP durante la recuperación del servidor), puede modificar la `-v4-grace-seconds` opción.

Acerca de esta tarea

De forma predeterminada, esta opción se establece en `45`.

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Introduzca el siguiente comando:

   ```
   vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
   ```

3. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Obtenga información sobre las referencias de NFSv4 para SVM de ONTAP

Al activar las referencias de NFSv4, ONTAP proporciona referencias «'intra-SVM» a los clientes de NFSv4. La referencia dentro de SVM se produce cuando un nodo de clúster que recibe la solicitud NFSv4 hace referencia al cliente NFSv4 a otra interfaz lógica (LIF) de la máquina virtual de almacenamiento (SVM).

El cliente NFSv4 debe acceder a la ruta que ha recibido la referencia en la LIF de destino desde ese punto. El nodo de clúster original proporciona una referencia de este tipo cuando determina que hay una LIF en la SVM que reside en el nodo de clúster en el que reside el volumen de datos, lo cual permite que los clientes accedan más rápido a los datos y eviten una comunicación adicional del clúster.

Habilitar o deshabilitar referencias NFSv4 para SVM de ONTAP

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

`-referralso`. La habilitación de las referencias A NFSV4 puede resultar en un acceso más rápido a los datos para los clientes de NFSv4 que admiten esta función.

Antes de empezar

Si desea habilitar las referencias NFS, primero debe deshabilitar NFS paralelo. No puede habilitar ambos a la vez.

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el comando…
Activar NFSv4 referencias	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled`
Deshabilitar las referencias de NFSv4	`vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled`
Activar NFSv4,1 referencias	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled`
Deshabilitar las referencias de NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled`

3. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Mostrar estadísticas para SVM de ONTAP NFS

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

Pasos

1. Utilice `statistics catalog object show` el comando para identificar los objetos NFS desde los que puede ver los datos.

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

2. Utilice `statistics start` `statistics stop` los comandos opcionales y para recopilar una muestra de datos de uno o más objetos.

3. Utilice `statistics show` el comando para ver los datos de ejemplo.

Ejemplo: Supervisión del rendimiento de NFSv3

El siguiente ejemplo muestra datos de rendimiento para el protocolo NFSv3.

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

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

El siguiente comando muestra datos de la muestra especificando contadores que muestran el número de solicitudes de lectura y escritura correctas, en comparación con el número total de solicitudes de lectura y escritura:

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                     Value
    --------------------------- ----------------------------
    read_success                                40042
    read_total                                  40042
    write_success                              1492052
    write_total                                1492052
```

Información relacionada

- "Configuración de supervisión del rendimiento"
- "Catálogo de estadísticas de objetos mostrados"
- "Las estadísticas muestran"
- "Las estadísticas comienzan"
- "las estadísticas se detienen"

Mostrar estadísticas de DNS para SVM NFS de ONTAP

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

Pasos

1. Utilice `statistics catalog object show` el comando para identificar los objetos DNS desde los que puede ver datos.

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

2. Use `statistics start` `statistics stop` los comandos y para recopilar una muestra de datos de uno o más objetos.
3. Utilice `statistics show` el comando para ver los datos de ejemplo.

Supervisar las estadísticas de DNS

Los siguientes ejemplos muestran datos de rendimiento para las consultas DNS. Los siguientes comandos inician la recopilación de datos de una nueva muestra:

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

El siguiente comando muestra datos de la muestra especificando contadores que muestran el número de consultas DNS enviadas en comparación con el número de consultas DNS recibidas, con errores o con tiempo de espera agotado:

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            0
    num_requests_sent                                               1
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

El siguiente comando muestra los datos de la muestra especificando contadores que muestran el número de veces que se recibió un error específico para una consulta DNS en el servidor concreto:

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                             NXDOMAIN
    server_ip_address                                   10.72.219.109
3 entries were displayed.
```

Información relacionada

- "Configuración de supervisión del rendimiento"
- "Catálogo de estadísticas de objetos mostrados"
- "Las estadísticas muestran"
- "Las estadísticas comienzan"
- "las estadísticas se detienen"

Mostrar estadísticas NIS para SVM NFS de ONTAP

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

Pasos

1. Utilice el `statistics catalog object show` comando para identificar los objetos NIS desde los que puede ver los datos.

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

2. Use `statistics start` `statistics stop` los comandos y para recopilar una muestra de datos de uno o más objetos.
3. Utilice `statistics show` el comando para ver los datos de ejemplo.

Supervisar las estadísticas de NIS

Los siguientes ejemplos muestran datos de rendimiento para consultas NIS. Los siguientes comandos inician la recopilación de datos de una nueva muestra:

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

El siguiente comando muestra los datos de la muestra especificando contadores que muestran el número de consultas NIS enviadas en comparación con el número de consultas NIS recibidas, fallidas o con el tiempo de espera agotado:

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                        0
    num_request_failures                                           1
    num_requests_sent                                              2
    num_responses_received                                         1
    num_successful_responses                                       1
    num_timeouts                                                   0
6 entries were displayed.
```

El siguiente comando muestra los datos de la muestra especificando contadores que muestran el número de veces que se recibió un error específico para una consulta NIS en el servidor concreto:

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                           YP_NOTFOUND
    server_ip_address                                    10.227.13.221
3 entries were displayed.
```

Información relacionada

- "Configuración de supervisión del rendimiento"
- "Catálogo de estadísticas de objetos mostrados"
- "Las estadísticas muestran"
- "Las estadísticas comienzan"
- "las estadísticas se detienen"

Obtenga información sobre la compatibilidad con VMware vStorage sobre ONTAP NFS

ONTAP admite ciertas funciones de VMware vStorage APIs for Array Integration (VAAI) en un entorno NFS.

Funciones admitidas

Se admiten las siguientes funciones:

- Descarga de copias

  Permite que un host ESXi copie máquinas virtuales o discos de máquinas virtuales (VMDK) directamente entre la ubicación de almacén de datos de origen y destino sin implicar al host. Esto ahorra ciclos de CPU del host ESXi y ancho de banda de red. La descarga de copia preserva la eficiencia del espacio si el volumen de origen es escaso.

- Reserva de espacio

  Garantiza espacio de almacenamiento para un archivo VMDK reservando espacio para él.

Limitaciones

VMware vStorage over NFS tiene las siguientes limitaciones:

- Las operaciones de descarga de copia pueden fallar en las siguientes situaciones:
  - Mientras se ejecuta waiflron en el volumen de origen o de destino porque desconecta temporalmente el volumen
  - Al mover el volumen de origen o el de destino
  - Al mover las LIF de origen o de destino
  - Al realizar operaciones de toma de control o devolución del retorno al nodo primario
  - Al mismo tiempo que realiza operaciones de conmutación de sitios o conmutación de estado
- La copia del servidor puede fallar debido a diferencias de formato de gestión de archivos en el siguiente escenario:

  Se intentan copiar datos de las SVM que tienen actualmente o habían exportado qtrees anteriormente a las SVM que nunca han exportado qtrees. Para solucionar esta limitación, puede exportar al menos un qtree en la SVM de destino.

Información relacionada

"¿Qué operaciones de VAAI descargados son compatibles con Data ONTAP?"

Habilitar o deshabilitar VMware vStorage sobre ONTAP NFS

Puede habilitar o deshabilitar la compatibilidad con VMware vStorage over NFS en máquinas virtuales de almacenamiento (SVM) mediante `vserver nfs modify` el comando.

Acerca de esta tarea

De forma predeterminada, la compatibilidad con VMware vStorage over NFS está deshabilitada.

Pasos

1. Mostrar el estado actual de soporte de vStorage para las SVM:

   ```
   vserver nfs show -vserver vserver_name -instance
   ```

2. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el siguiente comando…
Activar la compatibilidad con VMware vStorage	`vserver nfs modify -vserver vserver_name -vstorage enabled`
Desactivar la compatibilidad con VMware vStorage	`vserver nfs modify -vserver vserver_name -vstorage disabled`

Después de terminar

Para poder utilizar esta funcionalidad, es necesario instalar el plugin de NFS para VMware VAAI. Para obtener más información, consulte *Installing the NetApp NFS Plug-in for VMware VAAI*.

Información relacionada

"Documentación de NetApp: Plugin de NetApp NFS para VMware VAAI"

Habilitar o deshabilitar la compatibilidad con rquota en SVM NFS de ONTAP

El protocolo de cuota remota (rquota) permite a los clientes NFS obtener información de cuotas para los usuarios de un equipo remoto. La compatibilidad con las versiones rquota varía según la versión de ONTAP.

- Rquota v1 es compatible con ONTAP 9 y versiones posteriores.
- Rquota v2 es compatible con ONTAP 9.12.1 y versiones posteriores.

  Si actualiza de rquota v1 a rquota v2, es posible que observe un cambio inesperado en el límite de cuota de usuario. Este cambio se debe a la diferencia en la forma en que se calcula la cuota entre rquota v1 y rquota v2. Para obtener más información, consulte la"Base de conocimientos de NetApp : ¿Por qué el límite de cuota de usuario cambió inesperadamente?" .

Acerca de esta tarea

De forma predeterminada, rquota está desactivado.

Paso

1. Habilitar o deshabilitar rquota:

Si desea…	Introduzca el siguiente comando…
Habilite la compatibilidad de rquota para SVM	`vserver nfs modify -vserver vserver_name -rquota enable`
Deshabilite el soporte rquota para SVM	`vserver nfs modify -vserver vserver_name -rquota disable`

Para obtener más información sobre las cuotas, consulte "Gestión de almacenamiento lógico".

Obtenga información sobre las mejoras de rendimiento de NFSv3 y NFSv4 y el tamaño de transferencia TCP para SVM de ONTAP

Puede mejorar el rendimiento de los clientes NFSv3 y NFSv4 que se conectan a los sistemas de almacenamiento a través de una red de alta latencia al modificar el tamaño máximo de transferencia de TCP.

Cuando los clientes acceden a los sistemas de almacenamiento a través de una red de alta latencia, como una red de área extensa (WAN) o una red de área metropolitana (MAN) con una latencia superior a 10 milisegundos, es posible que pueda mejorar el rendimiento de la conexión modificando el tamaño máximo de transferencia de TCP. Los clientes que acceden a sistemas de almacenamiento en una red de baja latencia, como una red de área local (LAN), pueden esperar muy poco o ningún beneficio de la modificación de estos parámetros. Si la mejora del rendimiento no supera el impacto en la latencia, no debe usar estos parámetros.

Para determinar si su entorno de almacenamiento se beneficiaría de la modificación de estos parámetros, primero debe realizar una evaluación completa del rendimiento de un cliente NFS de bajo rendimiento. Revise

si el bajo rendimiento se debe a una latencia excesiva de ida y vuelta y una solicitud pequeña en el cliente. En estas condiciones, el cliente y el servidor no pueden utilizar por completo el ancho de banda disponible porque gastan la mayoría de sus ciclos de servicio esperando a que pequeñas solicitudes y respuestas se transmitan a través de la conexión.

Al aumentar el tamaño de las solicitudes de NFSv3 y NFSv4, el cliente y el servidor pueden utilizar el ancho de banda disponible de forma más eficaz para mover más datos por unidad y, de este modo, aumentar la eficiencia general de la conexión.

Tenga en cuenta que la configuración entre el sistema de almacenamiento y el cliente puede variar. El sistema de almacenamiento y el cliente admiten un tamaño máximo de 1 MB para las operaciones de transferencia. Sin embargo, si configura el sistema de almacenamiento para que admita un tamaño de transferencia máximo de 1 MB pero el cliente solo admita 64 KB, el tamaño de transferencia de montaje estará limitado a 64 KB o menos.

Antes de modificar estos parámetros, debe tener en cuenta que genera un consumo adicional de memoria en el sistema de almacenamiento durante el período de tiempo necesario para ensamblar y transmitir una gran respuesta. Cuanto más conexiones de alta latencia tenga con el sistema de almacenamiento, mayor será el consumo de memoria adicional. Los sistemas de almacenamiento con una gran capacidad de memoria pueden experimentar un efecto muy reducido a partir de este cambio. Los sistemas de almacenamiento con baja capacidad de memoria pueden experimentar una degradación considerable del rendimiento.

El uso correcto de este parámetro depende de la capacidad de recuperar datos de varios nodos de un clúster. La latencia inherente de la red de clúster podría aumentar la latencia general de la respuesta. La latencia general tiende a aumentar cuando se usa estos parámetros. Como resultado, las cargas de trabajo sensibles a la latencia pueden mostrar un impacto negativo.

Modificar el tamaño máximo de transferencia TCP de NFSv3 y NFSv4 para SVM de ONTAP

Puede modificar `-tcp-max-xfer-size` la opción de configurar tamaños de transferencia máximos para todas las conexiones TCP mediante los protocolos NFSv3 y NFSv4.x.

Acerca de esta tarea

Puede modificar estas opciones de forma individual para cada máquina virtual de almacenamiento (SVM).

A partir de ONTAP 9, las `v3-tcp-max-read-size` `v3-tcp-max-write-size` opciones y están obsoletas. `-tcp-max-xfer-size`En su lugar, debe usar la opción.

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el comando…
Modifique el tamaño de transferencia máximo de TCP de NFSv3 o NFSv4	`vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size`

Opción	Rango	Predeterminado
`-tcp-max-xfer-size`	de 8192 a 1048576 bytes	65536 bytes

> El tamaño de transferencia máximo introducido debe ser un múltiplo de 4 KB (4096 bytes). Las solicitudes que no están alineadas correctamente afectan negativamente al rendimiento.

3. Utilice `vserver nfs show -fields tcp-max-xfer-size` el comando para verificar los cambios.
4. Si alguno de los clientes utiliza montajes estáticos, desmonte y vuelva a montar para que el nuevo tamaño de parámetro entre en vigor.

Ejemplo

El siguiente comando establece el tamaño de transferencia máximo de TCP de NFSv3 y NFSv4.x en 1048576 bytes de la SVM llamada vs1:

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

Configurar la cantidad de ID de grupo permitidos para usuarios de NFS para SVM de ONTAP

De forma predeterminada, ONTAP admite hasta 32 identificadores de grupo al gestionar credenciales de usuario de NFS mediante la autenticación Kerberos (RPCSEC_GSS). Cuando se utiliza la autenticación AUTH_SYS, el número máximo predeterminado de ID de grupo es 16, tal como se define en RFC 5531. Puede aumentar el máximo hasta 1,024 si tiene usuarios que son miembros de más del número predeterminado de grupos.

Acerca de esta tarea

Si un usuario tiene más de la cantidad predeterminada de identificadores de grupo en sus credenciales, los ID de grupo restantes se truncarán y el usuario podría recibir errores al intentar acceder a los archivos desde el sistema de almacenamiento. Debe establecer el número máximo de grupos, por SVM, en un número que represente los grupos máximos en su entorno.

> Para comprender los requisitos previos de autenticación AUTH_SYS para habilitar grupos extendidos(`-auth-sys-extended-groups`) que utilizan identificadores de grupo más allá del máximo predeterminado de 16, consulte la"Base de conocimientos de NetApp : ¿Cuáles son los requisitos previos para habilitar auth-sys-extended-groups?"

La siguiente tabla muestra los dos parámetros del `vserver nfs modify` comando que determinan el número máximo de ID de grupo en tres configuraciones de ejemplo:

Parámetros	Configuración	Límite de ID de grupo resultante

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`32`
	
	`disabled`
	
	Esta es la configuración predeterminada.
		RPCSEC_GSS: 32
		
		AUTH_SYS: 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`256`
	
	`disabled`
		RPCSEC_GSS: 256
		
		AUTH_SYS: 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`512`
	
	`enabled`
		RPCSEC_GSS: 512
		
		AUTH_SYS: 512

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Realice la acción deseada:

Si desea establecer el número máximo de grupos auxiliares permitidos…	Introduzca el comando…
Sólo para RPCSEC_GSS y deje AUTH_SYS establecido en el valor predeterminado de 16	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled`
Para RPCSEC_GSS y AUTH_SYS	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled`

3. Verifique el `-extended-groups-limit` valor y verifique si AUTH_SYS está utilizando grupos extendidos: `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`
4. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Ejemplo

En el ejemplo siguiente se habilitan grupos extendidos para la autenticación AUTH_SYS y se establece el número máximo de grupos extendidos en 512 para la autenticación AUTH_SYS y RPCSEC_GSS. Estos cambios se realizan solo para los clientes que acceden al SVM denominado vs1:

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

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
------- ------------------------ --------------------
vs1     enabled                  512

vs1::*> set -privilege admin
```

Información relacionada

- "Base de conocimientos de NetApp : Cambios en los grupos extendidos AUTH_SYS para la autenticación NFS para ONTAP 9"

Controlar el acceso del usuario root a los datos de estilo de seguridad NTFS para SVM de ONTAP

Puede configurar ONTAP para permitir que los clientes NFS accedan a datos de estilo de seguridad NTFS y a clientes NTFS para acceder a los datos de estilo de seguridad NFS. Cuando se utiliza un estilo de seguridad NTFS en un almacén de datos NFS, se debe decidir cómo tratar el acceso por parte del usuario raíz y configurar la máquina virtual de almacenamiento (SVM) según corresponda.

Acerca de esta tarea

Cuando un usuario raíz accede a datos de estilo de seguridad NTFS, tiene dos opciones:

- Asignar el usuario raíz a un usuario de Windows como cualquier otro usuario NFS y gestionar el acceso según ACL de NTFS.
- Ignorar las ACL de NTFS y proporcionar acceso completo a la raíz.

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Realice la acción deseada:

Si desea que el usuario raíz…	Introduzca el comando…
Estar asignado a un usuario de Windows	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled`

Omitir la comprobación de ACL de NT	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled`

De manera predeterminada, este parámetro está deshabilitado.

Si este parámetro está habilitado pero no hay ninguna asignación de nombres para el usuario raíz, ONTAP utiliza una credencial de administrador de SMB predeterminada para la auditoría.

3. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Admiten versiones y clientes NFS

Obtenga información sobre las versiones y los clientes NFS de ONTAP compatibles

Antes de poder utilizar NFS en la red, debe saber qué versiones de NFS y clientes admite ONTAP.

Esta tabla indica si las versiones de protocolo NFS principales y secundarias son compatibles de forma predeterminada con ONTAP. La compatibilidad de forma predeterminada no indica que esta es la versión más antigua de ONTAP compatible con ese protocolo NFS.

Versión	Compatible	Introducido
NFSv3	Sí	Todos los lanzamientos de ONTAP
NFSv4.0	Sí	ONTAP 8
NFSv4.1	Sí	ONTAP 8,1
NFSv4.2	Sí	ONTAP 9,8
PNFs	Sí	ONTAP 8,1

Para obtener la información más reciente sobre la compatibilidad con ONTAP para clientes NFS, consulte la matriz de interoperabilidad.

"Herramienta de matriz de interoperabilidad de NetApp"

Obtenga información sobre la compatibilidad de ONTAP con la funcionalidad NFSv4.0

ONTAP admite todas las funciones obligatorias de NFSv4.0 excepto los mecanismos de seguridad SPKM3 y LIPKEY.

Se admiten las siguientes funciones DE NFSV4:

- **COMPUESTO**

Permite a un cliente solicitar varias operaciones de archivo en una única solicitud de llamada a procedimiento remoto (RPC).

- **Delegación de archivos**

  Permite al servidor delegar el control de archivos en algunos tipos de clientes para el acceso de lectura y escritura.

- **Pseudofs**

  Los servidores NFSv4 los utilizan para determinar los puntos de montaje del sistema de almacenamiento. No existe ningún protocolo de montaje en NFSv4.

- **Bloqueo**

  Basado en arrendamiento. No hay protocolos NLM (Network Lock Manager) o NSM (Network Status Monitor) separados en NFSv4.

Para obtener más información acerca del protocolo NFSv4.0, consulte RFC 3530.

Conozca las limitaciones de compatibilidad de ONTAP para NFSv4

Debe conocer varias limitaciones del soporte de ONTAP para NFSv4.

- La función de delegación no es compatible con todos los tipos de cliente.
- En ONTAP 9.4 y versiones anteriores, el sistema de almacenamiento rechaza los nombres con caracteres no ASCII en volúmenes distintos a UTF8.

  En ONTAP 9.5 y versiones posteriores, los volúmenes creados con la configuración de idioma utf8mb4 y montados con NFS v4 ya no están sujetos a esta restricción.

- Todos los identificadores de archivos son persistentes; el servidor no proporciona identificadores de archivos volátiles.
- No se admiten la migración ni la replicación.
- Los clientes NFSv4 no son compatibles con los reflejos de uso compartido de carga de solo lectura.

  ONTAP enruta los clientes NFSv4 al origen de la duplicación de uso compartido de la carga para obtener acceso directo de lectura y escritura.

- No se admiten los atributos con nombre.
- Se admiten todos los atributos recomendados, excepto los siguientes:
  - `archive`
  - `hidden`
  - `homogeneous`
  - `mimetype`
  - `quota_avail_hard`
  - `quota_avail_soft`
  - `quota_used`

- system
- time_backup

> Aunque no admite los `quota*` atributos, ONTAP admite cuotas de usuarios y grupos a través del protocolo de banda lateral RQUOTA.

Obtenga más información sobre la compatibilidad de ONTAP con NFSv4.1

A partir de ONTAP 9.8, la funcionalidad nconnect está disponible de forma predeterminada con NFSv4.1 habilitado.

En las implementaciones anteriores de clientes NFS solo se utiliza una única conexión TCP con un montaje. En ONTAP, una única conexión TCP puede convertirse en un cuello de botella que aumenta las IOPS.

nconnect mejora el rendimiento del cliente NFS al permitir múltiples conexiones TCP (hasta 16) para un solo montaje, lo que ayuda a superar el cuello de botella de rendimiento que puede ocurrir con una sola conexión TCP a medida que aumentan las IOPS.

NFSv4.1 está habilitado de forma predeterminada en ONTAP 9.9.1 y posteriores. En versiones anteriores, puede habilitarla especificando `-v4.1` la opción y configurándola en `enabled` al crear un servidor NFS en la máquina virtual de almacenamiento (SVM).

ONTAP no es compatible con las delegaciones a nivel de archivo y directorio de NFSv4.1.

Información relacionada

"Obtenga información sobre nconnect para el rendimiento de NFS".

Obtenga más información sobre la compatibilidad de ONTAP con NFSv4.2

A partir de ONTAP 9,8, ONTAP admite el protocolo NFSv4,2 para permitir acceso a clientes habilitados para NFSv4,2.

NFSv4.2 está habilitado de forma predeterminada en ONTAP 9.9.1 y versiones posteriores. En ONTAP 9.8, es necesario habilitar manualmente la versión 4.2 especificando el `-v4.2` opción y configurarla en `enabled` al crear un servidor NFS en la máquina virtual de almacenamiento (SVM). Habilitar NFSv4.1 también permite a los clientes usar las características de NFSv4.1 mientras están montados como v4.2.

Las versiones sucesivas de ONTAP amplían la compatibilidad de NFSv4,2 funciones opcionales.

Empezando por…	NFSv4,2 características opcionales incluyen…
ONTAP 9.12.1	• Atributos NFS extendidos • Archivos dispersos • Reservas de espacio
ONTAP 9.9.1	El control de acceso obligatorio (MAC) tiene la etiqueta NFS

Etiquetas de seguridad de NFS v4,2

A partir de ONTAP 9.9.1, se pueden habilitar las etiquetas de seguridad NFS. Están desactivadas de forma predeterminada.

Con etiquetas de seguridad NFS v4.2, los servidores NFS de ONTAP tienen en cuenta el control de acceso obligatorio (MAC), al almacenar y recuperar atributos sec_label enviados por los clientes.

Para obtener más información, consulte "RFC 7240".

A partir de ONTAP 9.12.1, las etiquetas de seguridad v4.2 de NFS son compatibles con las operaciones de volcado NDMP. Si las etiquetas de seguridad se encuentran en archivos o directorios en versiones anteriores, el volcado falla.

Pasos

1. Cambie la configuración del privilegio a avanzado:

```
set -privilege advanced
```

2. Habilitar etiquetas de seguridad:

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel enabled
```

Atributos NFS extendidos

A partir de ONTAP 9.12.1, los atributos extendidos de NFS (xattrs) están habilitados de forma predeterminada.

Los atributos ampliados son atributos estándar de NFS definidos "RFC 8276" y activados en los clientes NFS modernos. Se pueden utilizar para adjuntar metadatos definidos por el usuario a objetos del sistema de archivos, y son de interés en implementaciones de seguridad avanzadas.

Los atributos extendidos de NFS no se admiten actualmente para las operaciones de volcado de NDMP. Si se encuentran atributos extendidos en archivos o directorios, el volcado se realiza pero no realiza una copia de seguridad de los atributos extendidos en esos archivos o directorios.

Si necesita deshabilitar los atributos ampliados, utilice `vserver nfs modify -v4.2-xattrs disabled` el comando.

Obtenga información sobre nconnect para el rendimiento de NFS

A partir de ONTAP 9.8, la funcionalidad nconnect está disponible de forma predeterminada cuando NFSv4.1 está habilitado. nconnect mejora el rendimiento del cliente NFS al permitir múltiples conexiones TCP para un único montaje.

Cómo funciona nconnect

En las implementaciones anteriores de clientes NFS solo se utiliza una única conexión TCP con un montaje. En ONTAP, una única conexión TCP puede convertirse en un cuello de botella que aumenta las IOPS.

Un cliente compatible con nconnect puede tener múltiples conexiones TCP (hasta 16) asociadas a un único

montaje NFS. nconnect utiliza una sola dirección IP y establece múltiples conexiones TCP a través de esa única IP para montar la exportación NFS. El cliente NFS distribuye las operaciones de archivos en múltiples conexiones TCP de forma rotativa, obteniendo un mayor rendimiento del ancho de banda de red disponible.

Versiones de NFS compatibles

- Se recomienda usar nconnect para montajes NFSv3, NFSv4.2 y NFSv4.1.
- No se recomienda usar nconnect para montajes NFSv4.0.

> Para un rendimiento óptimo, NetApp recomienda usar NFSv4.1 con nconnect en lugar de NFSv4.0. Si bien NFSv4.0 admite múltiples conexiones, NFSv4.1 con nconnect proporciona una mejor distribución de la carga y un rendimiento mejorado.

Soporte al cliente

Consulte su documentación de cliente NFS para confirmar si nconnect es compatible con su versión de cliente.

Información relacionada

- "Obtenga más información sobre la compatibilidad de ONTAP con NFSv4.1"
- "Obtenga más información sobre la compatibilidad de ONTAP con NFSv4.2"

Obtenga información sobre la compatibilidad de ONTAP con NFS paralelo

ONTAP es compatible con NFS paralelo (pNFS). El protocolo pNFS ofrece mejoras en el rendimiento al proporcionar a los clientes acceso directo a los datos de un conjunto de archivos distribuidos por varios nodos de un clúster. Ayuda a los clientes a localizar la ruta óptima para un volumen.

Obtenga más información sobre los montajes duros de NFS de ONTAP

Al solucionar los problemas de montaje, debe asegurarse de utilizar el tipo de montaje correcto. NFS admite dos tipos de montaje: Montajes soft y montajes hard. Solo debe utilizar montajes hard por motivos de fiabilidad.

No debería utilizar montajes soft, especialmente cuando hay una posibilidad de tiempos de espera de NFS frecuentes. Las condiciones de carrera pueden producirse como resultado de estos tiempos de espera, que pueden provocar daños en los datos.

NFS paralelo

Introducción

Obtenga más información sobre NFS paralelo (pNFS) en ONTAP

NFS paralelo se introdujo como estándar RFC en enero de 2010 bajo RFC-5661 para permitir que los clientes accedan directamente a los datos de archivos en servidores NFSv4.1 separando las rutas de metadatos y datos. Ese acceso directo ofrece beneficios de rendimiento en términos de localización de datos, eficiencia de la CPU y

paralelización de operaciones. En 2018 se redactó un RFC posterior que cubre los tipos de diseño pNFS (RFC-8434) y define estándares para diseños de archivos, bloques y objetos. ONTAP aprovecha el tipo de diseño de archivo para operaciones pNFS.

> A partir de julio de 2024, el contenido de los informes técnicos publicados anteriormente en formato PDF se integrará con la documentación del producto ONTAP . La documentación de administración de almacenamiento NFS de ONTAP ahora incluye contenido de *TR-4063: Sistema de archivos de red paralelos (pNFS) en NetApp ONTAP*.

Durante años, NFSv3 fue la versión estándar del protocolo NFS que se utilizó para casi todos los casos de uso. Sin embargo, el protocolo tenía limitaciones, como la falta de estado, un modelo de permisos rudimentario y capacidades de bloqueo básicas. NFSv4.0 (RFC 7530) introdujo una serie de mejoras respecto de NFSv3 y se mejoró aún más con las versiones posteriores NFSv4.1 (RFC 5661) y NFSv4.2 (RFC 7862), que agregaron características como NFS paralelo (pNFS).

Beneficios de NFSv4.x

NFSv4.x ofrece los siguientes beneficios sobre NFSv3:

- Compatible con firewall porque NFSv4 usa solo un puerto (2049) para sus operaciones
- Gestión de caché avanzada y agresiva, como las delegaciones en NFSv4.x
- Opciones de seguridad RPC sólidas que emplean criptografía
- Internacionalización de personajes
- Operaciones compuestas
- Funciona sólo con TCP
- Protocolo con estado (no sin estado como NFSv3)
- Integración completa de Kerberos para mecanismos de autenticación eficientes
- Referencias de NFS
- Soporte de control de acceso compatible con UNIX y Windows
- Identificadores de usuarios y grupos basados en cadenas
- pNFS (NFSv4.1)
- Atributos extendidos (NFSv4.2)
- Etiquetas de seguridad (NFSv4.2)
- Operaciones de archivos dispersos (FALLOCATE) (NFSv4.2)

Para obtener más información sobre NFSv4.x general, incluidas las mejores prácticas y detalles sobre las características, consulte "Informe técnico de NetApp 4067: Guía de prácticas recomendadas e implementación de NFS".

Información relacionada

- "Información general de la configuración DE NFS"
- "Descripción general de la gestión de NFS"
- "Gestión de volúmenes de FlexGroup"
- "Descripción general de trunking NFS"
- https://www.netapp.com/pdf.html?item=/media/19370-tr-4523.pdf

- "Informe técnico de NetApp 4616: Kerberos de NFS en ONTAP con Microsoft Active Directory"

Aprenda sobre la arquitectura pNFS en ONTAP

La arquitectura pNFS se compone de tres componentes principales: un cliente NFS que admite pNFS, un servidor de metadatos que proporciona una ruta dedicada para operaciones de metadatos y un servidor de datos que proporciona rutas localizadas a los archivos.

El acceso del cliente a pNFS necesita conectividad de red a las rutas de datos y metadatos disponibles en el servidor NFS. Si el servidor NFS contiene interfaces de red a las que los clientes no pueden acceder, es posible que el servidor anuncie al cliente rutas de datos que no son accesibles, lo que puede provocar interrupciones.

Servidor de metadatos

El servidor de metadatos en pNFS se establece cuando un cliente inicia un montaje utilizando NFSv4.1 o posterior cuando pNFS está habilitado en el servidor NFS. Una vez hecho esto, todo el tráfico de metadatos se envía a través de esta conexión y permanece en ella mientras dura el montaje, incluso si la interfaz se migra a otro nodo.

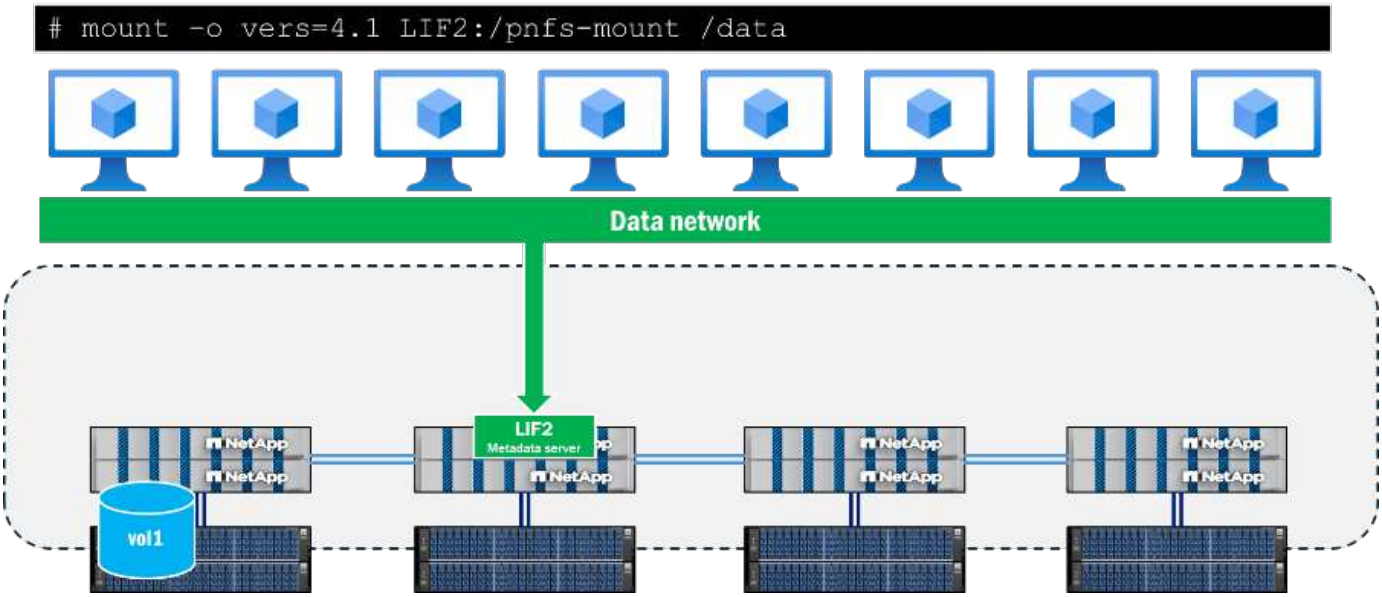


Figura 1. Establecer el servidor de metadatos en pNFS en ONTAP

La compatibilidad de pNFS se determina durante la llamada de montaje, específicamente en las llamadas EXCHANGE_ID. Esto se puede ver en una captura de paquetes debajo de las operaciones NFS como una bandera. Cuando las banderas pNFS `EXCHGID4_FLAG_USE_PNFS_DS` y `EXCHGID4_FLAG_USE_PNFS_MDS` se establecen en 1, entonces la interfaz es elegible para operaciones de datos y metadatos en pNFS.

```
Operations (count: 1)
  Opcode: EXCHANGE_ID (42)
      Status: NFS4_OK (0)
      clientid: 0x004050a97100001c
      seqid: 0x00000001
    flags: 0x00060100, EXCHGID4_FLAG_USE_PNFS_DS, EXCHGID4_FLAG_USE_PNFS_MDS, EXCHGID4_FLAG_BIND_PRINC
        0... .... .... .... .... .... .... .... = EXCHGID4_FLAG_CONFIRMED_R: Not set
        .0.. .... .... .... .... .... .... .... = EXCHGID4_FLAG_UPD_CONFIRMED_REC_A: Not set
        .... .... .... .1.. .... .... .... .... = EXCHGID4_FLAG_USE_PNFS_DS: Set
        .... .... .... ..1. .... .... .... .... = EXCHGID4_FLAG_USE_PNFS_MDS: Set
        .... .... .... ...0 .... .... .... .... = EXCHGID4_FLAG_USE_NON_PNFS: Not set
        .... .... .... .... .... ...1 .... .... = EXCHGID4_FLAG_BIND_PRINC_STATEID: Set
        .... .... .... .... .... .... .... ..0. = EXCHGID4_FLAG_SUPP_MOVED_MIGR: Not set
        .... .... .... .... .... .... .... ...0 = EXCHGID4_FLAG_SUPP_MOVED_REFER: Not set
```

Figura 2. Captura de paquetes para montaje pNFS

Los metadatos en NFS generalmente consisten en atributos de archivos y carpetas, como identificadores de archivos, permisos, tiempos de acceso y modificación e información de propiedad. Los metadatos también pueden incluir crear y eliminar llamadas, vincular y desvincular llamadas y cambiar nombres.

En pNFS, también hay un subconjunto de llamadas de metadatos específicas para la función pNFS y se tratan con más detalle en "RFC 5661". Estas llamadas se utilizan para ayudar a determinar dispositivos elegibles para pNFS, asignaciones de dispositivos a conjuntos de datos y otra información requerida. La siguiente tabla muestra una lista de estas operaciones de metadatos específicas de pNFS.

Funcionamiento	Descripción
DISEÑO	Obtiene el mapa del servidor de datos del servidor de metadatos.
COMPROMISO DE DISEÑO	Los servidores confirman el diseño y actualizan los mapas de metadatos.
DISEÑO RETORNO	Devuelve el diseño o el nuevo diseño si se modifican los datos.
OBTENER INFORMACIÓN DEL DISPOSITIVO	El cliente obtiene información actualizada sobre un servidor de datos en el clúster de almacenamiento.
OBTENERLISTADEDISPOSITIVOS	El cliente solicita la lista de todos los servidores de datos que participan en el clúster de almacenamiento.
CB_RECUPERACIÓN DE DISEÑO	El servidor recupera el diseño de datos de un cliente si se detectan conflictos.
CB_RECALL_ANY	Devuelve cualquier diseño al servidor de metadatos.
CB_NOTIFY_ID_DE DISPOSITIVO	Notifica cualquier cambio de ID del dispositivo.

Información de la ruta de datos

Una vez establecido el servidor de metadatos y comienzan las operaciones de datos, ONTAP comienza a rastrear los ID de dispositivos elegibles para operaciones de lectura y escritura de pNFS, así como las asignaciones de dispositivos, que asocian los volúmenes en el clúster con las interfaces de red local. Este proceso ocurre cuando se realiza una operación de lectura o escritura en el montaje. Llamadas de metadatos, como `GETATTR`. no activará estas asignaciones de dispositivos. Como tal, ejecutar una `ls` El comando dentro del punto de montaje no actualizará las asignaciones.

Los dispositivos y las asignaciones se pueden ver usando la CLI de ONTAP con privilegios avanzados, como se muestra a continuación.

```
::*> pnfs devices show -vserver DEMO
  (vserver nfs pnfs devices show)
Vserver Name     Mapping ID      Volume MSID     Mapping Status
Generation
---------------  --------------- --------------- ---------------
-------------
DEMO             16              2157024470      available       1

::*> pnfs devices mappings show -vserver SVM
  (vserver nfs pnfs devices mappings show)
Vserver Name    Mapping ID      Dsid            LIF IP
--------------  --------------- --------------- --------------------
DEMO            16              2488            10.193.67.211
```

En estos comandos, los nombres de los volúmenes no están presentes. En su lugar, se utilizan los identificadores numéricos asociados a esos volúmenes: el identificador del conjunto maestro (MSID) y el identificador del conjunto de datos (DSID). Para encontrar los volúmenes asociados a las asignaciones, puede utilizar `volume show -dsid [dsid_numeric]` o `volume show -msid [msid_numeric]` en privilegio avanzado de la CLI de ONTAP .

Cuando un cliente intenta leer o escribir en un archivo ubicado en un nodo remoto a la conexión del servidor de metadatos, pNFS negociará las rutas de acceso apropiadas para garantizar la localidad de los datos para esas operaciones y el cliente lo redireccionará al dispositivo pNFS anunciado en lugar de intentar atravesar la red del clúster para acceder al archivo. Esto ayuda a reducir la sobrecarga de la CPU y la latencia de la red.

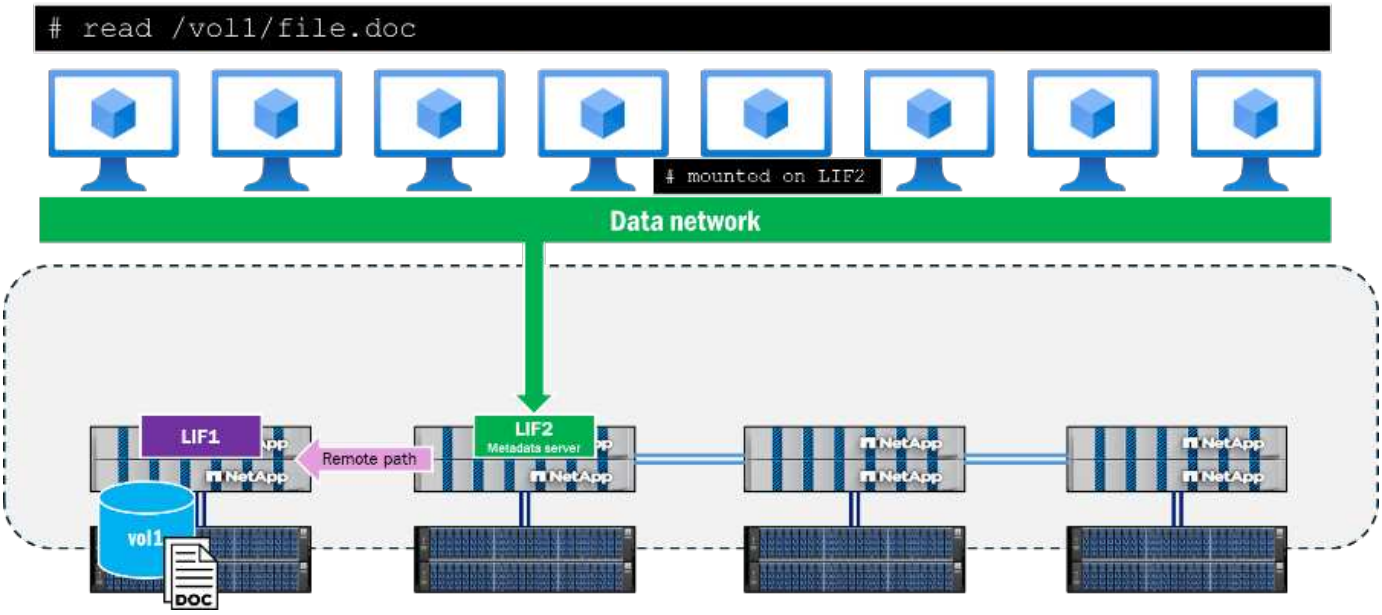


Figura 3. Ruta de lectura remota usando NFSv4.1 sin pNFS

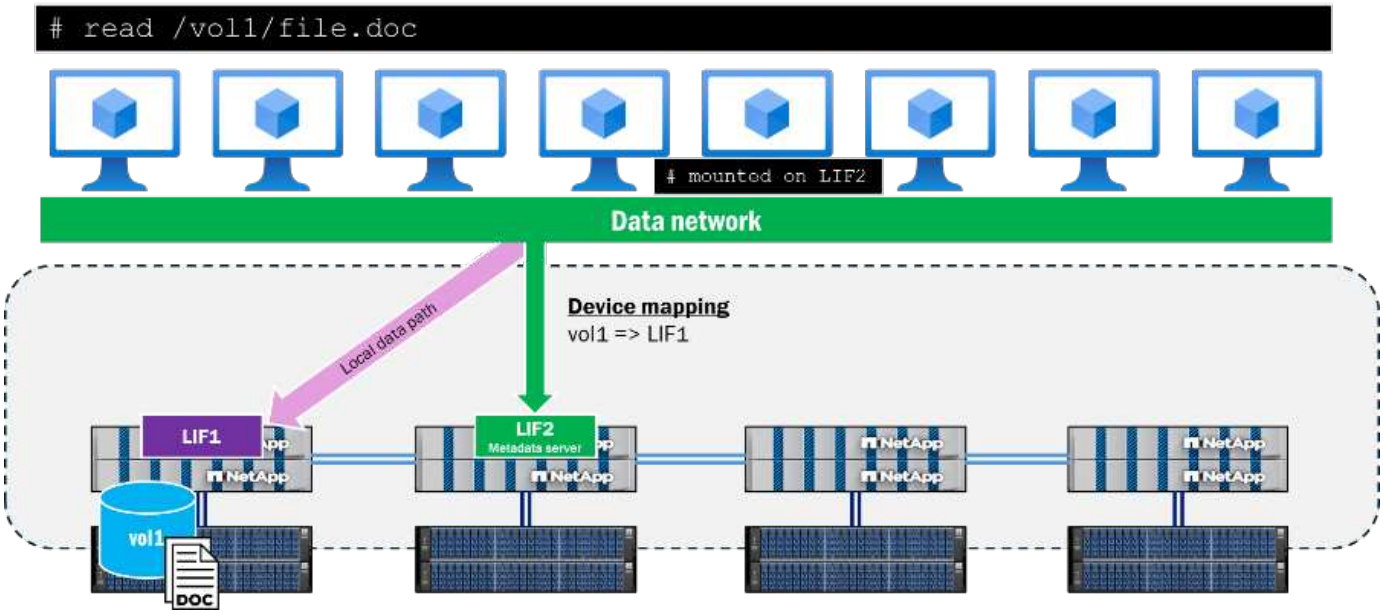


Figura 4. Ruta de lectura localizada mediante pNFS

Ruta de control pNFS

Además de los metadatos y las partes de datos de pNFS, también hay una ruta de control de pNFS. El servidor NFS utiliza la ruta de control para sincronizar la información del sistema de archivos. En un clúster ONTAP , la red del clúster backend se replica periódicamente para garantizar que todos los dispositivos pNFS y las asignaciones de dispositivos estén sincronizados.

Flujo de trabajo de población de dispositivos pNFS

A continuación se describe cómo se completa un dispositivo pNFS en ONTAP después de que un cliente realiza una solicitud para leer o escribir un archivo en un volumen.

1. El cliente solicita lectura o escritura; se realiza una operación OPEN y se recupera el identificador del archivo.
2. Una vez que se realiza la operación OPEN, el cliente envía el identificador de archivo al almacenamiento en una llamada LAYOUTGET a través de la conexión del servidor de metadatos.
3. LAYOUTGET devuelve al cliente información sobre el diseño del archivo, como el ID de estado, el tamaño de la banda, el segmento de archivo y el ID del dispositivo.
4. Luego, el cliente toma el ID del dispositivo y envía una llamada GETDEVINFO al servidor para recuperar la dirección IP asociada con el dispositivo.
5. El almacenamiento envía una respuesta con la lista de direcciones IP asociadas para el acceso local al dispositivo.
6. El cliente continúa la conversación NFS a través de la dirección IP local enviada desde el almacenamiento.

Interacción de pNFS con volúmenes FlexGroup

Los volúmenes FlexGroup en ONTAP presentan el almacenamiento como componentes de FlexVol volume que abarcan múltiples nodos en un clúster, lo que permite que una carga de trabajo aproveche múltiples recursos de hardware mientras mantiene un único punto de montaje. Debido a que varios nodos con múltiples interfaces de red interactúan con la carga de trabajo, es un resultado natural ver tráfico remoto atravesar la red del clúster backend en ONTAP.

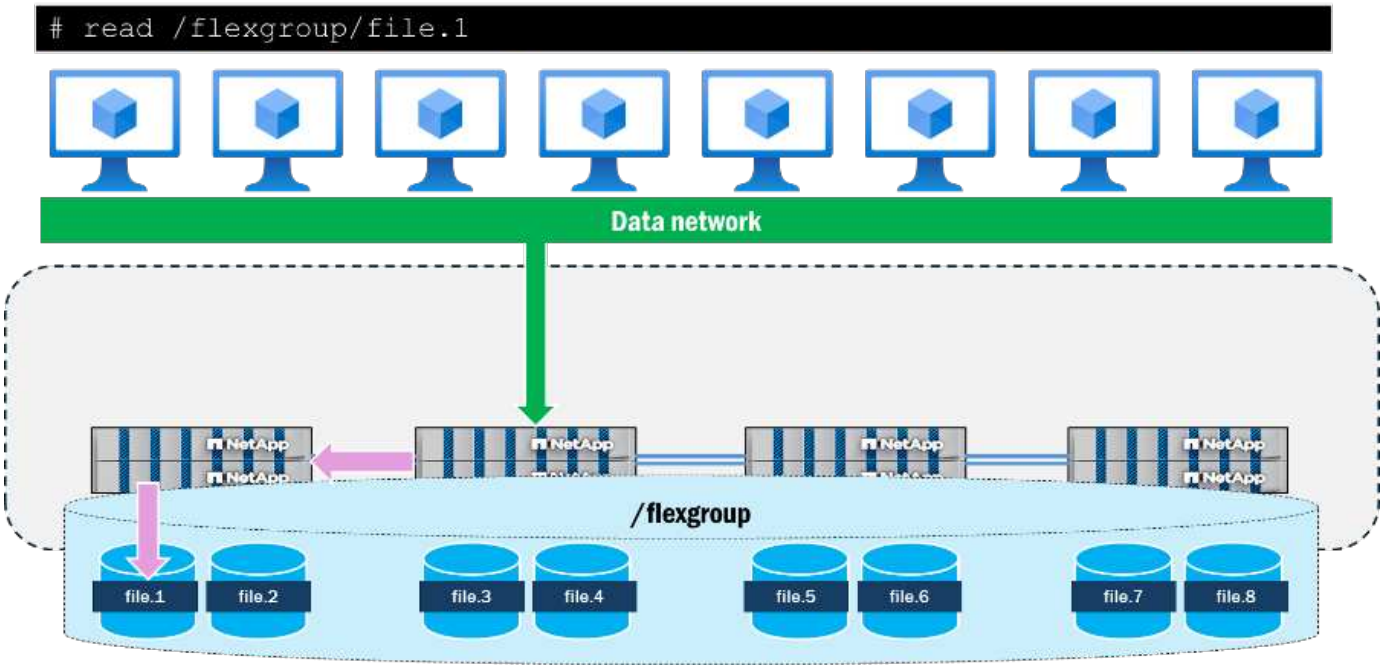


Figura 5. Acceso a un solo archivo en un volumen FlexGroup sin pNFS

Al utilizar pNFS, ONTAP realiza un seguimiento de los diseños de archivos y volúmenes del volumen FlexGroup y los asigna a las interfaces de datos locales en el clúster. Por ejemplo, si un volumen constituyente que contiene un archivo al que se accede reside en el nodo 1, entonces ONTAP notificará al cliente para redirigir el tráfico de datos a la interfaz de datos en el nodo 1.

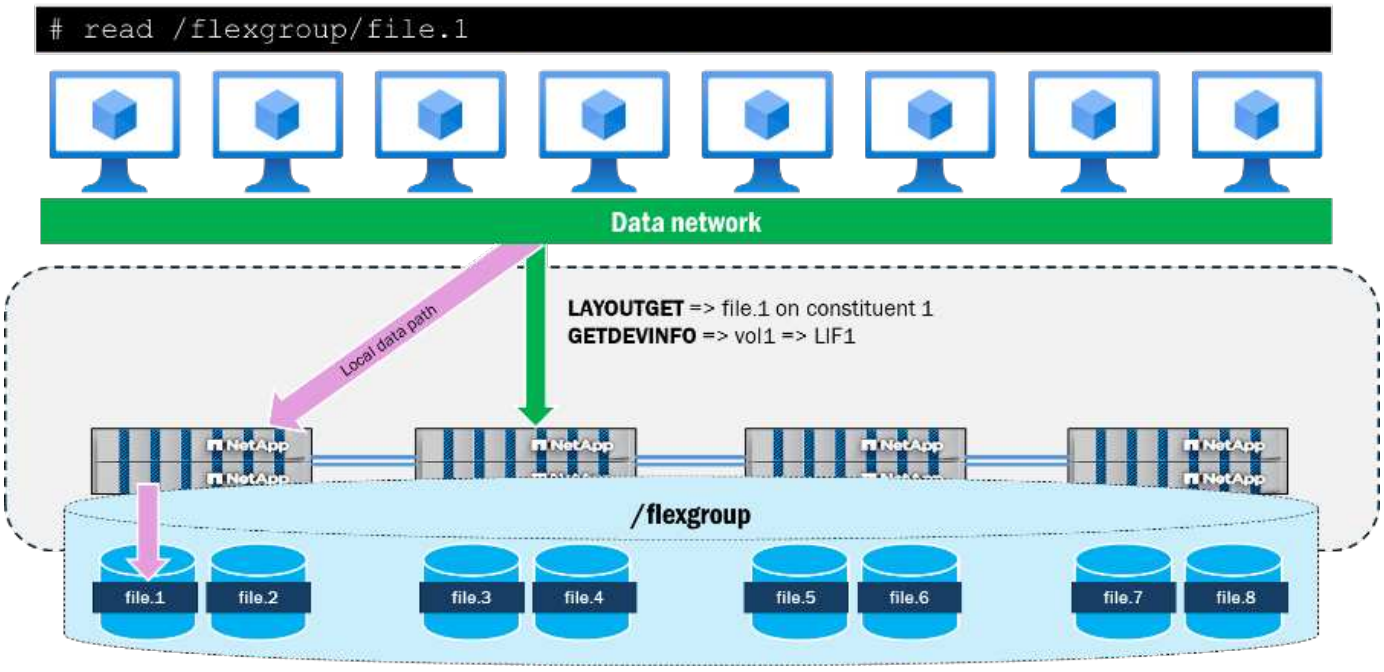


Figura 6. Acceso a un solo archivo en un volumen FlexGroup con pNFS

pNFS también permite la presentación de rutas de red paralelas a archivos desde un único cliente, algo que NFSv4.1 sin pNFS no proporciona. Por ejemplo, si un cliente desea acceder a cuatro archivos al mismo tiempo desde el mismo montaje usando NFSv4.1 sin pNFS, se utilizaría la misma ruta de red para todos los archivos y, en su lugar, el clúster ONTAP enviaría solicitudes remotas a esos archivos. La ruta de montaje puede convertirse en un cuello de botella para las operaciones, ya que todas siguen una única ruta y llegan a un único nodo y también atiende operaciones de metadatos junto con las operaciones de datos.

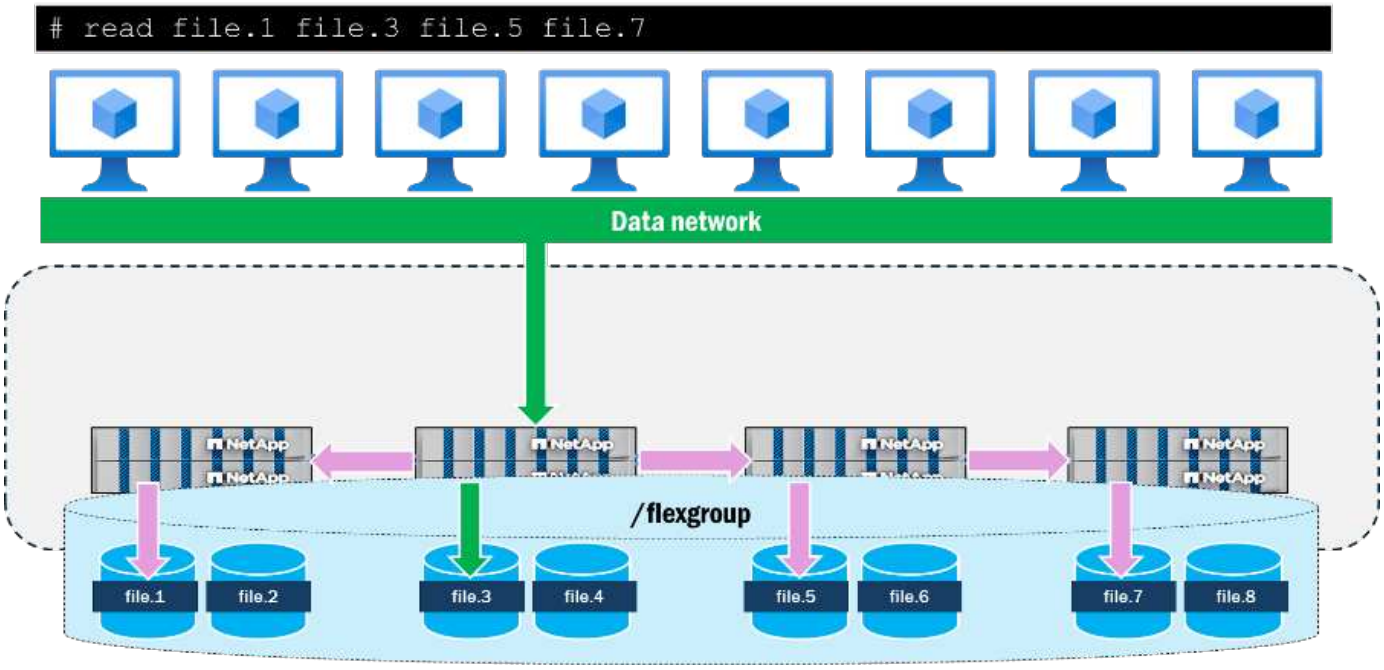


Figura 7. Acceso simultáneo a múltiples archivos en un volumen FlexGroup sin pNFS

Cuando se utiliza pNFS para acceder a los mismos cuatro archivos simultáneamente desde un solo cliente, el cliente y el servidor negocian rutas locales a cada nodo con los archivos y utilizan múltiples conexiones TCP para las operaciones de datos, mientras que la ruta de montaje actúa como la ubicación para todas las operaciones de metadatos. Esto proporciona beneficios de latencia al utilizar rutas locales a los archivos, pero también puede agregar beneficios de rendimiento mediante el uso de múltiples interfaces de red, siempre que los clientes puedan enviar suficientes datos para saturar la red.

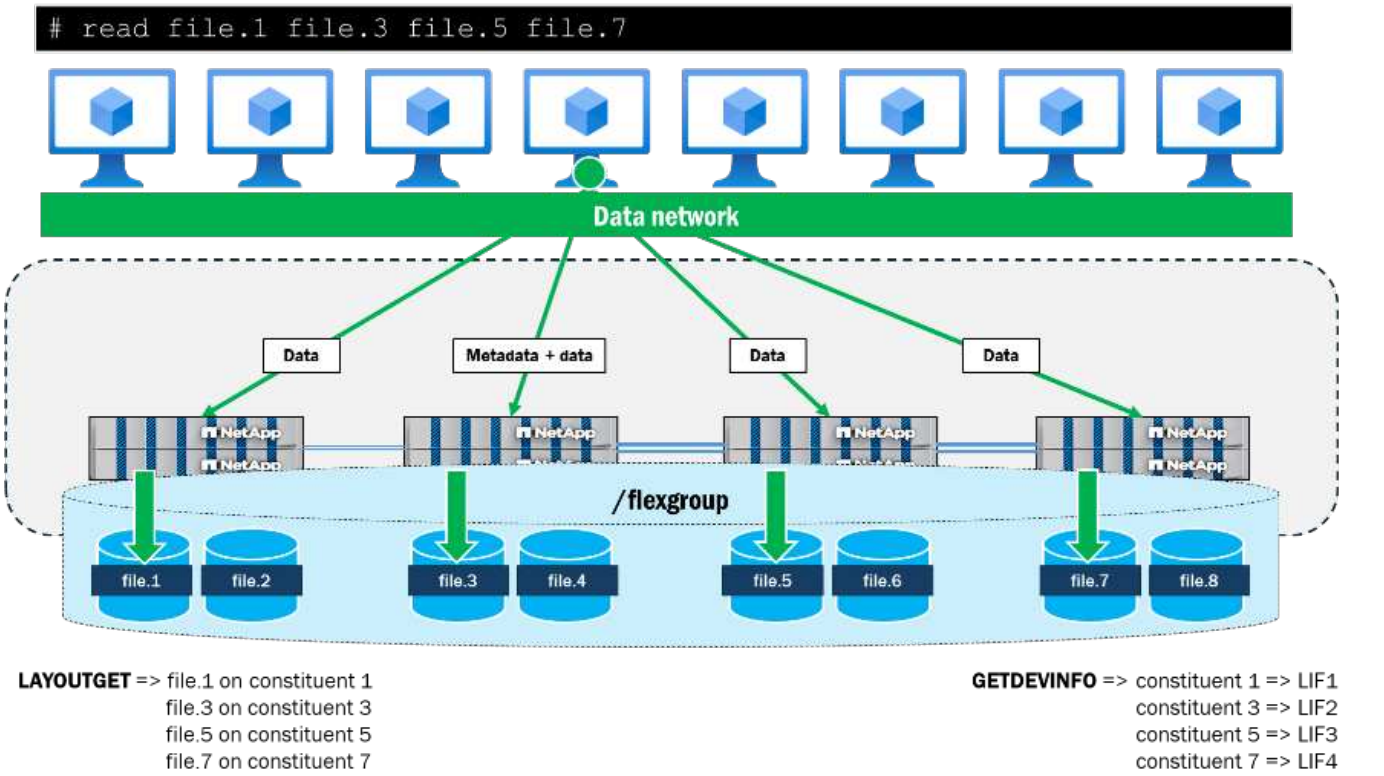


Figura 8. Acceso simultáneo a múltiples archivos en un volumen FlexGroup con pNFS

A continuación se muestran los resultados de una ejecución de prueba simple en un solo cliente RHEL 9.5

donde se leen en paralelo cuatro archivos de 10 GB (todos ellos residentes en diferentes volúmenes constituyentes en dos nodos del clúster ONTAP) mediante dd. Para cada archivo, se mejoró el rendimiento general y el tiempo de finalización al utilizar pNFS. Al usar NFSv4.1 sin pNFS, la diferencia de rendimiento entre los archivos que eran locales en el punto de montaje y los remotos era mayor que con pNFS.

Prueba	Rendimiento por archivo (MB/s)	Tiempo de finalización por archivo
NFSv4.1: sin pNFS	• Archivo.1–228 (local) • Archivo.2–227 (local) • Archivo.3–192 (remoto) • Archivo.4–192 (remoto)	• Archivo.1–46 (local) • Archivo.2–46.1 (local) • Archivo.3–54.5 (remoto) • Archivo.4–54.5 (remoto)
NFSv4.1: con pNFS	• Archivo.1–248 (local) • Archivo.2–246 (local) • Archivo .3–244 (local vía pNFS) • Archivo .4–244 (local vía pNFS)	• Archivo.1–42.3 (local) • Archivo.2–42.6 (local) • Archivo 3–43 (local vía pNFS) • Archivo 4–43 (local a través de pNFS)

Información relacionada

- "Gestión de volúmenes de FlexGroup"
- "Informe técnico 4571 de NetApp : Prácticas recomendadas de FlexGroup"

Casos de uso de pNFS en ONTAP

pNFS se puede utilizar con varias funciones de ONTAP para mejorar el rendimiento y proporcionar flexibilidad adicional para las cargas de trabajo NFS.

pNFS con nconnect

NFS introdujo una nueva opción de montaje con algunos clientes y servidores más recientes que proporciona una manera de entregar múltiples conexiones TCP mientras se monta una sola dirección IP. Esto proporciona un mecanismo para paralelizar mejor las operaciones, solucionar las limitaciones del servidor y del cliente NFS y, potencialmente, proporcionar un mayor rendimiento general para ciertas cargas de trabajo. nconnect es compatible con ONTAP 9.8 y versiones posteriores, siempre que el cliente admita nconnect.

Al usar nconnect con pNFS, las conexiones se paralelizarán usando la opción nconnect en cada dispositivo pNFS anunciado por el servidor NFS. Por ejemplo, si nconnect está configurado en cuatro y hay cuatro interfaces elegibles para pNFS, entonces la cantidad total de conexiones creadas será de hasta 16 por punto de montaje (4 nconnect x 4 direcciones IP).

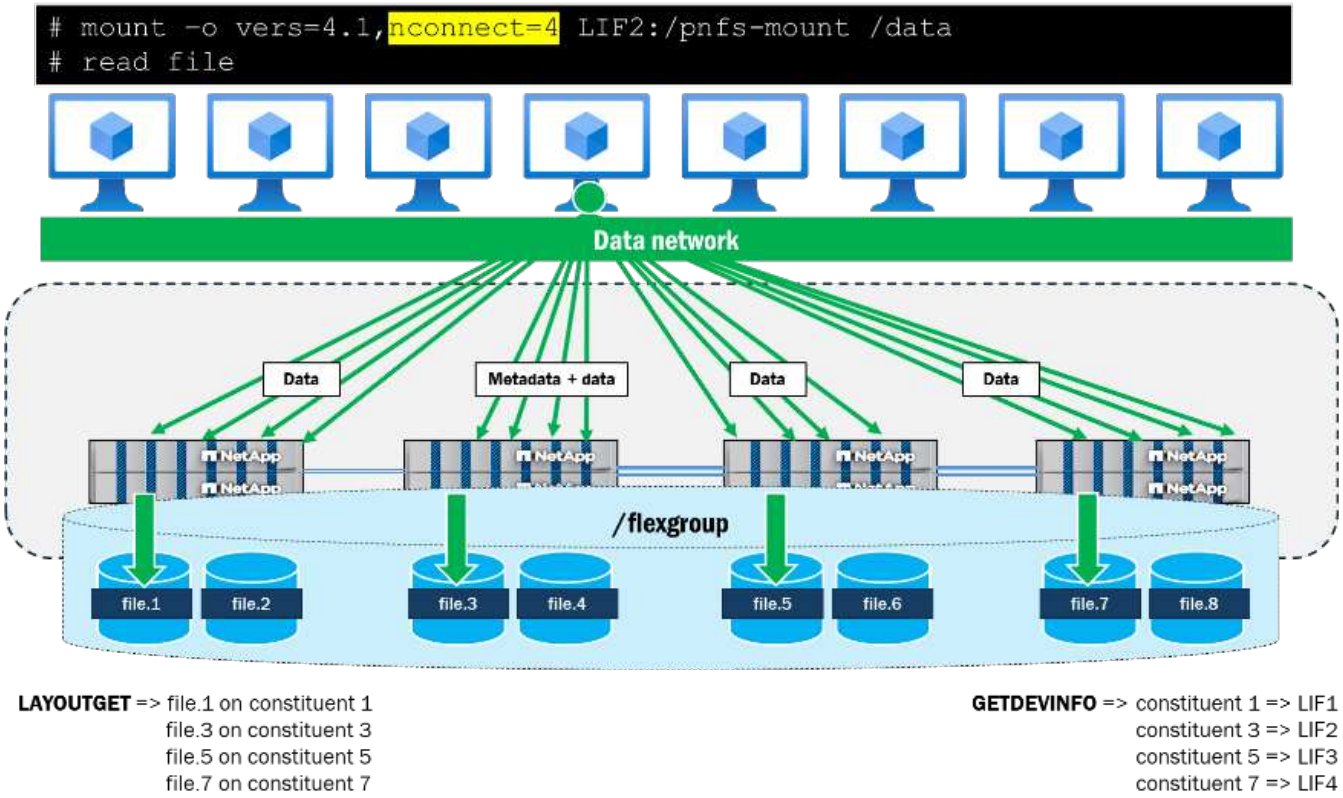


Figura 9. pNFS con nconnect establecido en 4

"Obtenga más información sobre la compatibilidad de ONTAP con NFSv4.1"

pNFS con enlace troncal de sesión NFSv4.1

Troncalización de sesión NFSv4.1 ("RFC 5661, sección 2.10.5") es el uso de múltiples conexiones TCP entre un cliente y un servidor para aumentar la velocidad de transferencia de datos. Se agregó soporte para troncalización de sesión NFSv4.1 a ONTAP 9.14.1 y debe usarse con clientes que también admitan troncalización de sesión.

En ONTAP, el enlace troncal de sesiones se puede utilizar en varios nodos de un clúster para proporcionar mayor rendimiento y redundancia en las conexiones.

La troncalización de sesiones se puede establecer de varias maneras:

- **Descubrir automáticamente a través de las opciones de montaje:** La troncalización de sesiones en la mayoría de los clientes NFS modernos se puede establecer a través de opciones de montaje (consulte la documentación del proveedor de su sistema operativo) que indican al servidor NFS que envíe información al cliente acerca de los troncales de sesión. Esta información aparece a través de un paquete NFS como un `fs_location4` llamar.

  La opción de montaje en uso depende de la versión del sistema operativo del cliente. Por ejemplo, las versiones de Ubuntu Linux generalmente usan `max_connect=n` para señalar que se debe utilizar un enlace troncal de sesión. En las distribuciones de Linux RHEL, el `trunkdiscovery` Se utiliza la opción de montaje.

  Ejemplo de Ubuntu

  ```
  mount -o vers=4.1,max_connect=8 10.10.10.10:/pNFS /mnt/pNFS
  ```

Ejemplo de RHEL

```
mount -o vers=4.1,trunkdiscovery 10.10.10.10:/pNFS /mnt/pNFS
```

Si intenta utilizar `max_connect` En las distribuciones RHEL, se tratará como nconnect y el enlace troncal de sesión no funcionará como se espera.

- **Establecer manualmente:** puede establecer la troncalización de sesiones manualmente montando cada dirección IP individual en la misma ruta de exportación y punto de montaje. Por ejemplo, si tiene dos direcciones IP en el mismo nodo (10.10.10.10 y 10.10.10.11) para una ruta de exportación de `/pNFS`, ejecuta el comando mount dos veces:

```
mount -o vers=4.1 10.10.10.10:/pNFS /mnt/pNFS
mount -o vers=4.1 10.10.10.11:/pNFS /mnt/pNFS
```

Repita este proceso en todas las interfaces que desee que participen en el enlace troncal.

Cada nodo obtiene su propio tronco de sesión. Los troncos no atraviesan los nodos.

Al utilizar pNFS, utilice únicamente el enlace troncal de sesión *o* nconnect. El uso de ambos generará un comportamiento no deseado, como por ejemplo que solo la conexión del servidor de metadatos obtenga los beneficios de nconnect mientras que los servidores de datos utilizan una única conexión.

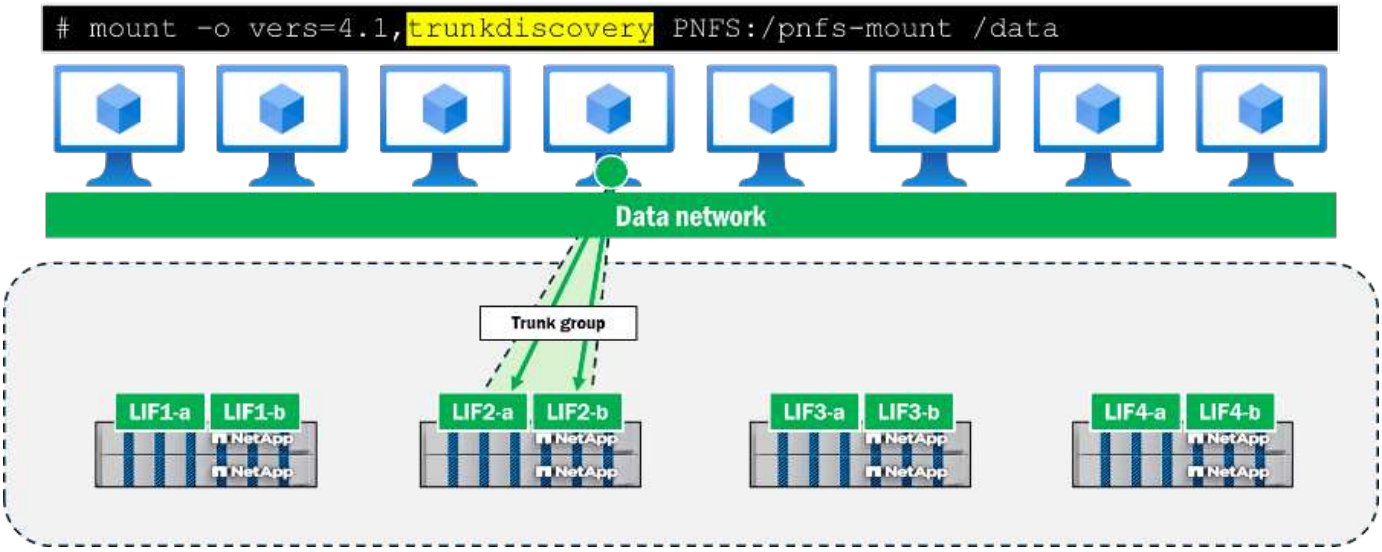
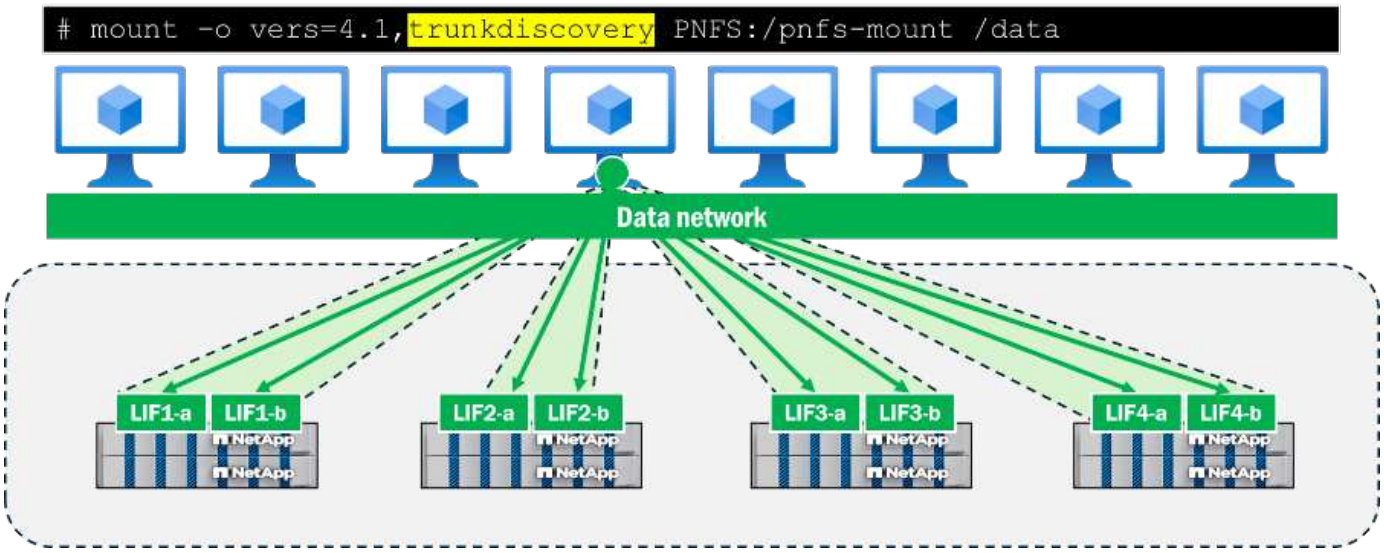


Figura 10. Troncalización de sesiones NFSv4.1 en ONTAP

pNFS puede proporcionar una ruta local a cada nodo participante en un clúster y, cuando se utiliza con troncalización de sesión, pNFS puede aprovechar un troncal de sesión por nodo para maximizar el rendimiento de todo el clúster.



Cuando `trunkdiscovery` se utiliza, se aprovecha una llamada GETATTR agregada (FS_Locations) para las interfaces troncales de sesión enumeradas en el nodo del servidor NFS donde se encuentra la interfaz de montaje. Una vez que se devuelven, se realizan montajes posteriores en las direcciones devueltas. Esto se puede ver en una captura de paquetes durante el montaje.

```
198 1.219372  [redacted]  [redacted]  NFS  246 V4 Call (Reply In 199) GETATTR FH: 0x787f5cf1
199 1.219579  [redacted]  [redacted]  NFS  238 V4 Reply (Call In 198) GETATTR

Opcode: SEQUENCE (53)
    Status: NFS4_OK (0)
    sessionid: 7100001e004090a90000000000000409
    seqid: 0x00000009
    slot id: 0
    high slot id: 63
    target high slot id: 63
  > status flags: 0x00000000
Opcode: PUTFH (22)
    Status: NFS4_OK (0)
Opcode: GETATTR (9)
    Status: NFS4_OK (0)
  Attr mask: 0x01000100 (FSID, FS_Locations)
    reqd_attr: FSID (8)
      fattr4_fsid
    reco_attr: FS_Locations (24)
      fattr4_fs_locations
          pathname components: 0
        fs_location4
            num: 1
          fs_location4
            servers
                num: 1
              server: [redacted]
                  length: 14
                  contents: [redacted]
                  fill bytes: opaque data
              pathname components: 0
```

Figura 11. Detección de troncos de sesión NFS durante el montaje: captura de paquetes

"Obtenga más información sobre los enlaces troncales NFS"

Referencias de pNFS versus NFSv4.1

Las referencias NFSv4.1 proporcionan un modo de redirección de ruta de montaje inicial que dirige a un cliente a la ubicación de los volúmenes cuando se produce una solicitud de montaje. Las referencias de NFSv4.1 funcionan dentro de una única SVM. Esta función intenta localizar el montaje NFS en una interfaz de red que reside en el mismo nodo que el volumen de datos. Si esa interfaz o volumen se mueve a otro nodo mientras está montado en un cliente, la ruta de datos ya no estará localizada hasta que se establezca un nuevo montaje.

pNFS no intenta localizar una ruta de montaje. En su lugar, establece un servidor de metadatos utilizando una ruta de montaje y luego localiza la ruta de datos dinámicamente según sea necesario.

Las referencias NFSv4.1 se pueden usar con pNFS, pero la funcionalidad es innecesaria. Habilitar referencias con pNFS no mostrará resultados notables.

"Habilitar o deshabilitar referencias NFSv4"

Interacción de pNFS con equilibrio de capacidad avanzado

"Equilibrado de capacidad avanzado" en ONTAP escribe porciones de datos de archivos en los volúmenes constituyentes de un volumen FlexGroup (no compatible con volúmenes FlexVol individuales). A medida que un archivo crece, ONTAP decide comenzar a escribir datos en un nuevo inodo multiparte en un volumen constituyente diferente, que puede estar en el mismo nodo o en uno diferente. Las operaciones de escritura, lectura y metadatos en estos archivos multi-inodo son transparentes y no interrumpen a los clientes. El equilibrio de capacidad avanzado mejora la gestión del espacio entre los volúmenes constituyentes de FlexGroup , lo que proporciona un rendimiento más consistente.

pNFS puede redirigir la E/S de datos a una ruta de red localizada dependiendo de la información de diseño de archivo almacenada en el servidor NFS. Cuando se crea un solo archivo grande en partes en múltiples volúmenes constituyentes que potencialmente pueden abarcar varios nodos en el clúster, pNFS en ONTAP aún puede proporcionar tráfico localizado a cada parte del archivo porque ONTAP también mantiene la información de diseño del archivo para todas las partes del archivo. Cuando se lee un archivo, la localidad de la ruta de datos cambiará según sea necesario.

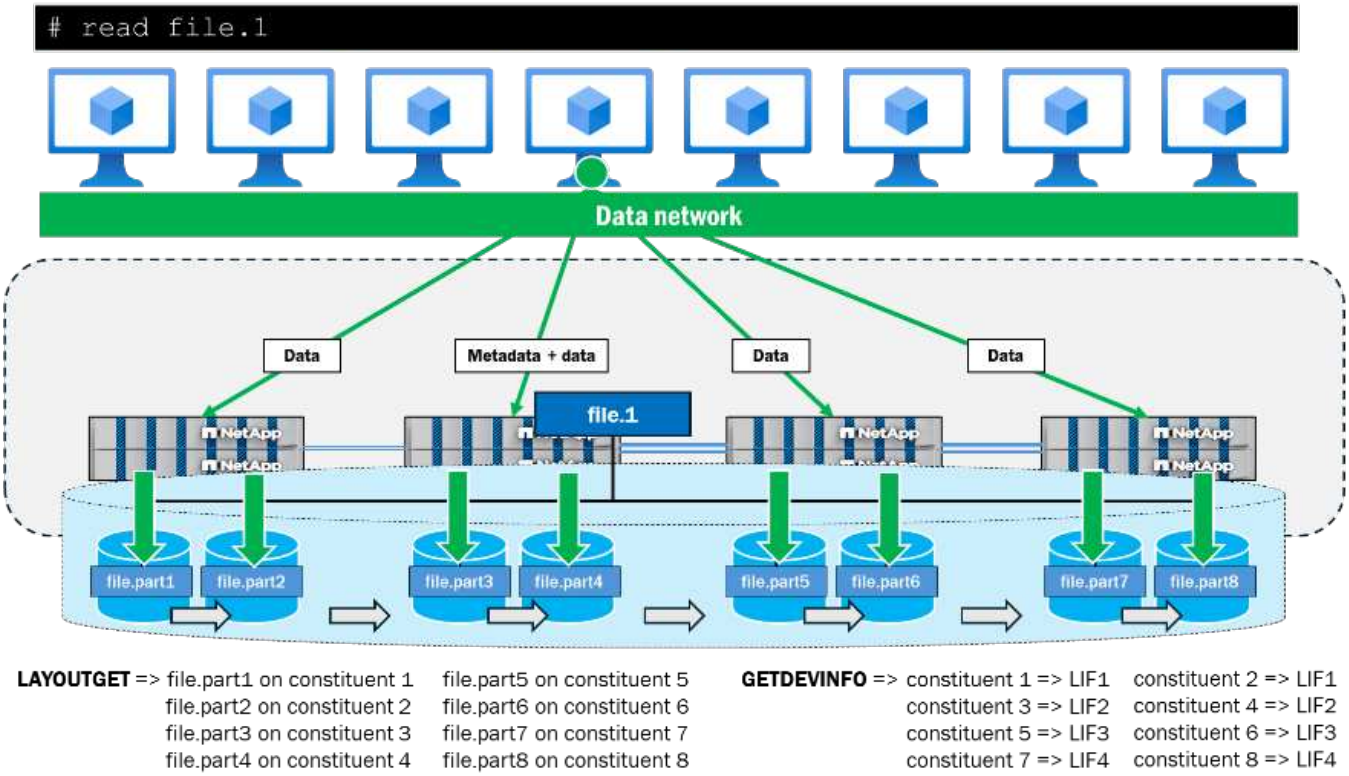


Figura 12. Equilibrio de capacidad avanzado con pNFS

Información relacionada

- "Configuración del volumen de FlexGroup"

Estrategia de implementación de pNFS en ONTAP

pNFS se introdujo para mejorar el NFS tradicional separando metadatos y rutas de datos, proporcionando localización de datos y permitiendo operaciones paralelas.

Desafíos del NFS tradicional y beneficios del pNFS

La siguiente tabla muestra los desafíos del NFS tradicional y explica cómo pNFS en ONTAP los aborda.

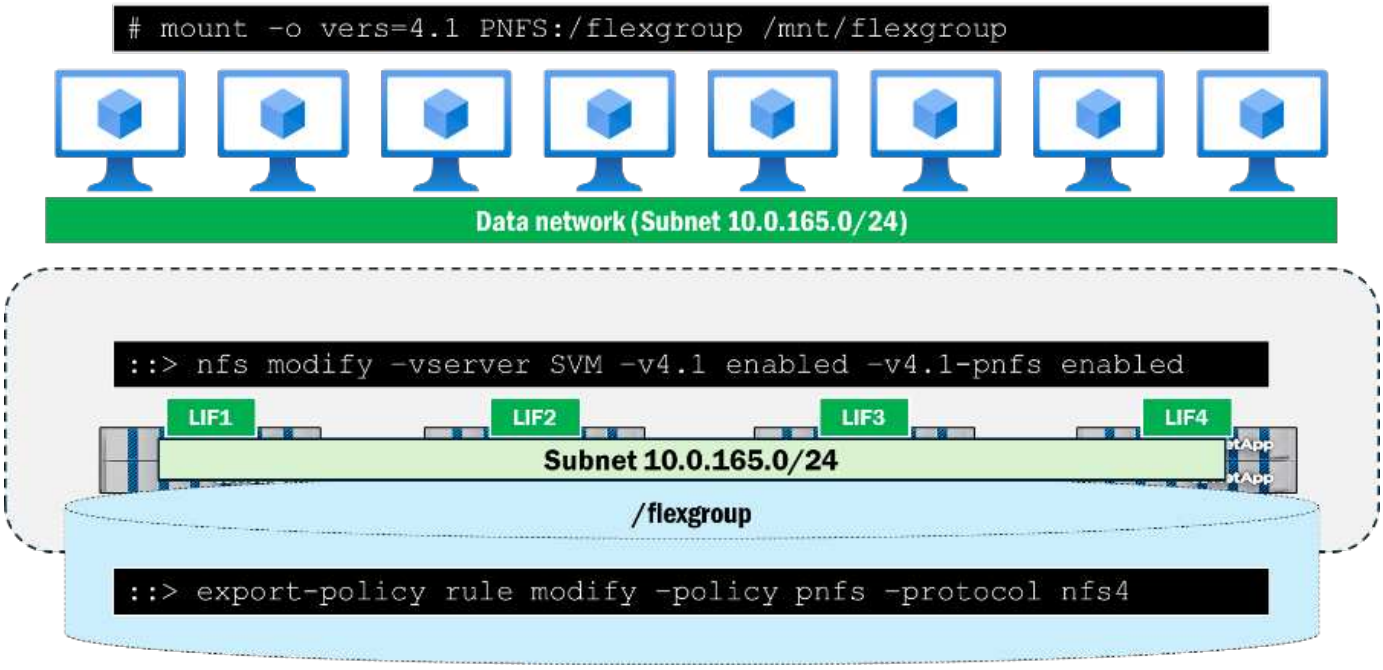
Desafío	beneficio de pNFS
La misma ruta para metadatos y datos En NFS tradicional, los metadatos y los datos recorren la misma ruta, lo que puede saturar tanto la red como la CPU, ya que una sola ruta se conectará a un solo nodo de hardware en el clúster. Esto se agrava cuando muchos usuarios intentan acceder a la misma exportación NFS.	**Las rutas de metadatos y datos están separadas, las rutas de datos están paralelizadas** Al separar las rutas de metadatos y datos para el tráfico NFS y proporcionar múltiples rutas de red para las rutas de datos, se maximizan los recursos de CPU y red en un clúster ONTAP , lo que proporciona una escala mejorada para las cargas de trabajo.

Desafío	beneficio de pNFS
Desafíos de la distribución de la carga de trabajo En un clúster NAS de ONTAP , puede tener hasta 24 nodos, cada uno de los cuales puede tener su propio conjunto de volúmenes de datos e interfaces de red. Cada volumen puede alojar su propia carga de trabajo, o un subconjunto de una carga de trabajo, y con un volumen FlexGroup esa carga de trabajo puede existir en múltiples nodos que acceden a un único espacio de nombres para mayor simplicidad. Cuando un cliente monta una exportación NFS, el tráfico de red se establecerá en un solo nodo. Cuando los datos a los que se accede residen en un nodo separado del clúster, se producirá tráfico remoto, lo que puede agregar latencia a la carga de trabajo y complejidad en la administración.	**Rutas locales y paralelas a las estructuras de datos** Debido a que pNFS separa las rutas de datos de los metadatos y proporciona múltiples rutas de datos paralelas según la localidad del volumen en el clúster, la latencia se puede reducir al reducir la distancia del tráfico de red en el clúster, además de aprovechar múltiples recursos de hardware en un clúster. Además, dado que pNFS en ONTAP redirige el tráfico de datos automáticamente, los administradores tienen menos necesidad de administrar múltiples rutas y ubicaciones de exportación.
Reubicación de puntos de montaje NFS Una vez establecido un punto de montaje, sería disruptivo desmontar y volver a montar el volumen. ONTAP ofrece la posibilidad de migrar interfaces de red entre nodos, pero eso agrega sobrecarga de administración y es perjudicial para las conexiones NFS con estado que utilizan NFSv4.x. Algunas de las razones para reubicar un punto de montaje están relacionadas con los desafíos de localidad de datos.	**Reubicación automática de rutas** Con pNFS, el servidor NFS mantiene una tabla de las ubicaciones de las interfaces y volúmenes de red. Cuando se solicita una estructura de datos a un cliente a través de la ruta de metadatos en pNFS, el servidor entregará una ruta de red optimizada al cliente, que luego utilizará esa ruta para operaciones de datos. Esto reduce drásticamente la sobrecarga de gestión de las cargas de trabajo y puede mejorar el rendimiento en algunos casos.

Requisitos de configuración

La configuración de pNFS en NetApp ONTAP requiere lo siguiente:

- Un cliente NFS que admita pNFS y esté montado con NFSv4.1 o posterior
- NFSv4.1 habilitado en el servidor NFS en ONTAP (`nfs modify -v4.1 enabled`; desactivado por defecto)
- pNFS habilitado en el servidor NFS en ONTAP (`nfs modify -v4.1-pnfs enabled`; deshabilitado por defecto)
- Al menos una interfaz de red por nodo, enrutable a los clientes NFS
- Volúmenes de datos en la SVM que tienen políticas y reglas de exportación que permiten NFSv4



Una vez cumplidos los requisitos de configuración anteriores, pNFS simplemente funcionará por sí solo.

Información relacionada

- "Configuración de NFS"
- "Compatibilidad de ONTAP con NFSv4.1"
- "Conectividad de interfaz de red para pNFS"

Planificación

Plan para la implementación de pNFS

Antes de implementar pNFS en su entorno, asegúrese de cumplir con los requisitos previos y comprender los requisitos de interoperabilidad y los límites de configuración.

Requisitos previos

Antes de habilitar y usar pNFS en ONTAP, asegúrese de que se cumplan los siguientes requisitos:

- NFSv4.1 o posterior está habilitado en el servidor NFS
- Al menos uno "Los datos LIF existen por nodo" en el clúster para el SVM que aloja el servidor NFS
- Todo "Los LIF de datos en el SVM son enrutables" a clientes NFS
- Los clientes NFS admiten pNFS (la mayoría de las distribuciones de Linux modernas a partir de 2014)
- La conectividad de red entre los clientes y todos los LIF de datos en la SVM es funcional
- La resolución de DNS (si se utilizan nombres de host) está configurada correctamente para todos los LIF de datos
- "Volúmenes de FlexGroup" están configurados (recomendado para obtener mejores resultados)
- "Coincidencia de dominios de identificación de NFSv4.x" entre clientes y ONTAP
- "NFS Kerberos" (si se utiliza) está habilitado en todos los LIF de datos en el SVM

Resumen de mejores prácticas

Al implementar pNFS en su entorno, siga estas prácticas recomendadas:

- Usar "Volúmenes de FlexGroup" Para un mejor rendimiento y escalamiento de capacidad
- Asegúrese de que todos "Las interfaces de red en el SVM son enrutables" a los clientes
- "Desactivar NFSv4,0" para garantizar que los clientes utilicen NFSv4.1 o posterior
- Distribuya los puntos de montaje en múltiples interfaces y nodos de red
- Utilice DNS round robin para "servidores de metadatos de equilibrio de carga"
- Verificar "Coincidencia de dominios de identificación de NFSv4.x" en clientes y servidores
- Conducta "migraciones de interfaz de red" y "conmutaciones por error de almacenamiento" durante las ventanas de mantenimiento
- Permitir "NFS Kerberos" en todos los LIF de datos si se utiliza seguridad Kerberos
- Evite usar "Referencias de NFSv4.1" al usar pNFS
- Prueba "Configuración de nconnect" con cuidado para evitar sobrepasar los límites de conexión TCP
- Considerar "troncalización de sesiones" como alternativa a "nconectar" (no utilice ambos juntos)
- Verificar "Soporte del proveedor del sistema operativo del cliente" para pNFS antes de la implementación

Interoperabilidad

pNFS en ONTAP está diseñado para funcionar con clientes NFS compatibles con RFC. Se aplican las siguientes consideraciones:

- El más moderno "Distribuciones de Linux de 2014 y posteriores" Admite pNFS (RHEL 6.4, Fedora 17 y posteriores)
- Verifique con el proveedor del sistema operativo de su cliente que pNFS sea compatible
- pNFS funciona tanto con FlexVol como con "Volúmenes de FlexGroup"
- pNFS es compatible con NFSv4.1 y "NFSv4.2"
- pNFS se puede utilizar con "NFS Kerberos" (krb5, krb5i, krb5p), pero el rendimiento podría verse afectado
- pNFS se puede utilizar junto con "nconectar" o "troncalización de sesiones" (pero no ambos simultáneamente)
- pNFS no funciona sobre "NFSv4.0"

Límites

Los siguientes límites se aplican a pNFS en ONTAP:

- "Límites de conexión TCP" por nodo varía según la plataforma (consulte NetApp Hardware Universe para conocer los límites específicos)
- Tamaño máximo de archivo: depende del tipo de volumen y la versión de ONTAP
- Cantidad máxima de archivos: hasta 200 mil millones de archivos con "Volúmenes de FlexGroup"
- Capacidad máxima: Hasta 60 PB con "Volúmenes de FlexGroup"
- "Recuento de interfaces de red":Se requiere al menos un LIF de datos por nodo; es posible que se necesiten más para equilibrar la carga

Al utilizar "Conéctese con pNFS"Tenga en cuenta que los recuentos de conexiones TCP se multiplican rápidamente:

- Cada montaje de cliente con nconnect crea múltiples conexiones TCP por LIF de datos
- Con muchos clientes que utilizan valores altos de nconnect, "Límites de conexión TCP" puede superarse
- Exceder los límites de conexión TCP impide nuevas conexiones hasta que se liberen las conexiones existentes

Información relacionada

- "Conectividad de interfaz de red para pNFS"
- "Habilitar o deshabilitar NFSv4.1"
- "Compatibilidad de ONTAP con NFSv4.1"
- "Compatibilidad de ONTAP con NFSv4.2"
- "NetApp Hardware Universe"

Mejores prácticas de rendimiento y ajuste de pNFS

Al utilizar pNFS en ONTAP, tenga en cuenta estas consideraciones y prácticas recomendadas para obtener mejores resultados.

Recomendaciones de tipo de volumen

pNFS en ONTAP funciona con volúmenes FlexVol y FlexGroup , pero para obtener los mejores resultados generales, utilice volúmenes FlexGroup .

Los volúmenes FlexGroup proporcionan:

- Un único punto de montaje que puede abarcar múltiples recursos de hardware en un clúster y al mismo tiempo permitir que pNFS localice el tráfico de datos
- Posibilidades de capacidad masiva (hasta 60 PB) y gran cantidad de archivos (hasta 200 mil millones de archivos)
- Compatibilidad con archivos multiparte para equilibrar la capacidad y obtener posibles beneficios de rendimiento
- Acceso paralelo a volúmenes y hardware que admiten una única carga de trabajo

"Obtenga más información sobre la gestión de volúmenes de FlexGroup"

Recomendaciones de clientes

No todos los clientes NFS admiten pNFS, pero la mayoría de los clientes modernos sí. RHEL 6.4 y Fedora 17 fueron los primeros clientes pNFS compatibles (aproximadamente en 2014), por lo que es razonable suponer que las versiones de cliente lanzadas en los últimos años son totalmente compatibles con esta función. La postura de soporte de NFS de ONTAP es la siguiente: "si el cliente admite la función y cumple con RFC, y nosotros admitimos la función, entonces la combinación es compatible". Sin embargo, es una buena práctica asegurarse de que el proveedor del sistema operativo del cliente admita pNFS.

El volumen se mueve

ONTAP brinda la capacidad de mover volúmenes sin interrupciones entre nodos o agregados en el mismo clúster para brindar flexibilidad de equilibrio de capacidad y rendimiento. Cuando se realiza un movimiento de

volumen en ONTAP, las asignaciones de dispositivos pNFS se actualizan automáticamente para informar a los clientes que utilicen la nueva relación de volumen a interfaz si es necesario.

"Aprenda a mover un volumen"

Migración de la interfaz de red

ONTAP proporciona la capacidad de mover interfaces de red entre nodos del mismo clúster para brindar equilibrio de rendimiento y flexibilidad de mantenimiento. Al igual que los movimientos de volumen, cuando se realiza una migración de interfaz de red en ONTAP, las asignaciones de dispositivos pNFS se actualizan automáticamente para informar a los clientes que utilicen la nueva relación de volumen a interfaz si es necesario.

Sin embargo, debido a que NFSv4.1 es un protocolo con estado, una migración de interfaz de red puede ser perjudicial para los clientes que utilizan activamente el montaje NFS. Es una buena práctica realizar migraciones de interfaz de red en una ventana de mantenimiento y notificar a los clientes sobre posibles interrupciones de la red.

Conmutaciones por error/devoluciones de almacenamiento

pNFS sigue las mismas consideraciones de conmutación por error de almacenamiento que NFSv4.1. Estos temas se tratan en detalle en "Informe técnico de NetApp 4067: Guía de prácticas recomendadas e implementación de NFS"En general, cualquier conmutación por error o devolución de almacenamiento que involucre pNFS debe realizarse en una ventana de mantenimiento, con posibles interrupciones de almacenamiento esperadas debido al estado del protocolo.

Cargas de trabajo de metadatos

Las operaciones de metadatos son de tamaño pequeño y pueden ser grandes en número según la carga de trabajo (¿Está creando una gran cantidad de archivos? ¿Está ejecutando comandos "buscar"?) y el recuento total de archivos. Como resultado, las cargas de trabajo con muchas llamadas de metadatos pueden sobrecargar la CPU del servidor NFS y potencialmente pueden generar un cuello de botella en una sola conexión. pNFS (y NFSv4.x en general) no es adecuado para cargas de trabajo con muchas llamadas de metadatos que dependen del rendimiento, ya que el estado, los mecanismos de bloqueo y algunas de las características de seguridad de la versión del protocolo pueden afectar negativamente la utilización y la latencia de la CPU. Estos tipos de carga de trabajo (como GETATTR o SETATTR altos) generalmente funcionan mejor con NFSv3.

Servidor de metadatos

El servidor de metadatos en pNFS se establece en el montaje inicial de una exportación NFS. Cuando se establece el punto de montaje, permanece en su lugar hasta que se vuelve a montar o se mueve la interfaz de datos. Por este motivo, es una buena práctica garantizar que varios clientes que acceden al mismo volumen se monten en diferentes nodos e interfaces de datos en toda la SVM. Este enfoque permite equilibrar la carga de los servidores de metadatos entre los nodos y los recursos de la CPU, al tiempo que maximiza las interfaces de red en el clúster. Una forma de lograr esto es establecer una configuración de DNS round robin, que se describe en "Informe técnico 4523 de NetApp : Equilibrio de carga de DNS en ONTAP".

Dominios de identificación de NFSv4.x

NFSv4.x proporciona funcionalidad de seguridad de muchas maneras (que se explican en detalle en "Informe técnico de NetApp 4067: Guía de prácticas recomendadas e implementación de NFS"). Los dominios de identificación de NFSv4.x son una de esas formas en las que un cliente y un servidor deben acordar los dominios de identificación cuando intentan autenticar usuarios y grupos en una exportación NFS. Uno de los efectos secundarios de una falta de coincidencia en el dominio de ID sería que el usuario o grupo apareciera

como un usuario anónimo (esencialmente aplastado) para evitar acceso no deseado. Con NFSv4.x (y también pNFS), es una buena práctica garantizar que los dominios de identificación de NFSv4.x coincidan en el cliente y el servidor.

nconectar

Como se mencionó anteriormente, nconnect en ONTAP puede ayudar a mejorar el rendimiento en algunas cargas de trabajo. Con pNFS, es importante entender que si bien nconnect puede mejorar el rendimiento al aumentar en gran medida la cantidad total de conexiones TCP al sistema de almacenamiento, también puede crear problemas cuando muchos clientes aprovechan la opción de montaje al saturar las conexiones TCP en el almacenamiento. El Hardware Universe de NetApp cubre los límites de conexión TCP por nodo.

Cuando se superan los límites de conexión TCP de un nodo, no se permiten nuevas conexiones TCP hasta que se liberen las conexiones existentes. Esto puede crear complicaciones en entornos que podrían experimentar fuertes tormentas.

La siguiente tabla muestra cómo pNFS con nconnect podría superar los límites de conexión TCP:

Número de clientes	valor de nconnect	Total de conexiones TCP potenciales por montaje, por nodo
1	4	4
100	4	400
1000	8	8000
10000	8	80000
10000	16	160000 [1]

[1] Supera la mayoría de los límites de conexión TCP de nodo único de ONTAP

Troncalización de sesión NFSv4,1

El enlace troncal de sesiones en ONTAP se puede utilizar para aumentar el rendimiento y la resiliencia de la ruta a los montajes NFSv4.x. Cuando se utiliza con pNFS, cada nodo de un clúster puede establecer un tronco de sesión. Sin embargo, los troncales de sesión requieren al menos dos interfaces por nodo, y pNFS requiere al menos una interfaz por nodo para funcionar según lo previsto. Además, todas las interfaces en la SVM deben ser enrutables a los clientes NFS. El enlace troncal de sesiones y pNFS no funcionan correctamente cuando también se aprovecha nconnect. Considere nconnect y el enlace troncal de sesiones como características mutuamente excluyentes.

"Obtenga más información sobre el enlace troncal NFS"

Conectividad de la interfaz de red

pNFS requiere una interfaz de red enrutable en cada nodo de un clúster para funcionar correctamente. Si existen otras interfaces de red que no se pueden enrutar a clientes NFS en el mismo SVM que el servidor NFS que aloja pNFS, ONTAP seguirá anunciando esas interfaces en la asignación de dispositivos a los clientes. Cuando el cliente NFS intenta acceder a los datos a través de las interfaces en una subred diferente, no podrá conectarse y se creará una interrupción. Se recomienda permitir únicamente interfaces de red en una SVM a las que los clientes puedan acceder cuando utilizan pNFS.

De forma predeterminada, pNFS requiere que cualquier LIF de datos en el SVM sea enrutable a las interfaces en los clientes NFS porque las listas de dispositivos pNFS se completarán con cualquier LIF de datos en el SVM. Como resultado, se podrían seleccionar LIF de datos no enrutables, lo que puede crear escenarios de interrupción. Como práctica recomendada, solo configure LIF de datos enrutables cuando utilice pNFS.

A partir de ONTAP 9.18.1 RC1 y versiones posteriores, puede especificar qué interfaces son elegibles para el tráfico pNFS por subred, lo que permite combinar interfaces enrutables y no enrutables. Comuníquese con el soporte de NetApp para obtener información sobre los comandos.

NFSv4.0

NFSv4.0 es una opción que se puede habilitar en un servidor NFS de ONTAP junto con NFSv4.1. Sin embargo, pNFS no funciona con NFSv4.0. Si NFSv4.0 está habilitado en el servidor NFS, los clientes podrían potencialmente montar sin saberlo esa versión del protocolo y no podrán aprovechar pNFS. Como resultado, es una buena práctica deshabilitar explícitamente NFSv4.0 al usar pNFS. NFSv4.1 aún debe estar habilitado y puede funcionar independientemente de NFSv4.0.

Referencias de NFSv4.1

Las referencias de NFSv4.1 localizarán la ruta de montaje desde un cliente a la interfaz de red en el nodo que posee un volumen. pNFS localiza la ruta de datos y la ruta de montaje se convierte en un servidor de metadatos.

Si bien las dos características se pueden usar juntas, el uso de referencias NFSv4.1 con pNFS puede generar el efecto no deseado de apilar múltiples servidores de metadatos en el mismo nodo y reducir la capacidad de distribuir servidores de metadatos entre múltiples nodos del clúster. Si los servidores de metadatos no se distribuyen de manera uniforme en un clúster cuando se usa pNFS, la CPU de un solo nodo puede verse sobrecargada con solicitudes de metadatos y crear un cuello de botella en el rendimiento.

Por ello, se recomienda evitar el uso de referencias NFSv4.1 al utilizar pNFS. En su lugar, distribuya los puntos de montaje en varias interfaces de red y nodos del clúster.

"Obtenga información sobre cómo habilitar o deshabilitar las referencias de NFSv4"

NFS Kerberos

Con NFS Kerberos, es posible cifrar la autenticación con krb5 y cifrar aún más los paquetes de datos con krb5i y krb5p. Esto se habilita en función de la interfaz por red en una SVM y se cubre con todo detalle en "Informe técnico de NetApp 4616: Kerberos de NFS en ONTAP con Microsoft Active Directory".

Dado que pNFS puede redirigir el tráfico de datos a través de nodos e interfaces de red en la SVM, NFS Kerberos debe estar habilitado y funcional en cada interfaz de red en la SVM. Si alguna interfaz de red en la SVM no está habilitada para Kerberos, entonces pNFS no podrá funcionar correctamente al intentar acceder a los volúmenes de datos en esas interfaces.

Por ejemplo, al ejecutar una prueba de lectura utilizando dd paralelo en un SVM habilitado para pNFS con dos interfaces de red (solo una habilitada para Kerberos), los archivos ubicados en la interfaz habilitada para Kerberos funcionaron bien, mientras que los archivos en el nodo con la interfaz sin Kerberos habilitado nunca pudieron completar sus lecturas. Cuando Kerberos se habilitó en ambas interfaces, todos los archivos pudieron funcionar como se esperaba.

Se puede utilizar NFS Kerberos con pNFS siempre que NFS Kerberos esté habilitado en todas las interfaces

de red en la SVM. Tenga en cuenta que NFS Kerberos puede incurrir en una penalización de rendimiento debido al cifrado/descifrado de los paquetes, por lo que es una buena práctica probar pNFS con NFS Kerberos exhaustivamente con sus cargas de trabajo para garantizar que cualquier impacto en el rendimiento no tenga un impacto excesivo en la carga de trabajo.

A continuación se muestra un ejemplo de rendimiento de lectura paralela al utilizar krb5 (autenticación) y krb5p (cifrado de extremo a extremo) con pNFS en un cliente RHEL 9.5. Krb5p vio una degradación del rendimiento del 70% en esta prueba.

Sabor Kerberos	MB/s	Tiempo de finalización
krb5	• File1-243 • File2-243 • File3-238 • File4-238	• File1-43 • File2-43,1 • File3-44 • File4-44,1
krb5p	• File1-72,9 • File2-72,8 • File3-71,4 • File4-71,2	• File1-143,9 • File2-144,1 • File3-146,9 • File4-147,3

"Obtenga más información sobre Kerberos con NFS para una seguridad sólida"

NFSv4.2

NFSv4.2 se agregó a ONTAP 9.8 y es la última versión de NFSv4.x disponible (RFC-7862). NFSv4.2 no tiene una opción explícita para habilitarlo/deshabilitarlo. En cambio, se habilita/deshabilita junto con NFSv4.1 (`-4.1 enabled`). Si un cliente admite NFSv4.2, negociará la versión más alta compatible de NFS durante el comando de montaje si no se especifica lo contrario con el `minorversion=2` Opción de montaje.

NFSv4.2 en ONTAP admite la siguiente funcionalidad:

- Etiquetas de seguridad (etiquetas MAC)
- Atributos ampliados
- Operaciones de archivos dispersos (FALLOCATE)

pNFS se introdujo con NFSv4.1, pero también es compatible con NFSv4.2, así como con sus características complementarias.

"Obtenga más información sobre la compatibilidad de ONTAP con NFSv4.2"

Comandos, estadísticas y registros de eventos de pNFS

Estos comandos CLI de ONTAP pertenecen específicamente a pNFS. Puede usarlos para configurar, solucionar problemas y recopilar estadísticas.

Habilitar NFSv4,1

```
nfs modify -vserver SVM -v4.1 enabled
```

Habilite pNFS

```
nfs modify -vserver SVM -v4.1-pnfs enabled
```

Mostrar dispositivos pNFS (privilegios avanzados)

```
pnfs devices show -vserver SVM
```

```
Vserver Name     Mapping ID      Volume MSID     Mapping Status
Generation
---------------  --------------- --------------- ---------------
-------------
SVM              17              2157024470      notavailable    2
SVM              18              2157024463      notavailable    2
SVM              19              2157024469      available       3
SVM              20              2157024465      available       4
SVM              21              2157024467      available       3
SVM              22              2157024462      available       1
```

Mostrar asignaciones de dispositivos pNFS (privilegios avanzados)

```
pnfs devices mappings show -vserver SVM
```

```
Vserver Name    Mapping ID      Dsid            LIF IP
--------------  --------------- --------------- --------------------
SVM             19              2449            10.x.x.x
SVM             20              2512            10.x.x.y
SVM             21              2447            10.x.x.x
SVM             22              2442            10.x.x.y
```

Capturar contadores de rendimiento específicos de pNFS (privilegios avanzados)

```
statistics start -object nfsv4_1 -vserver SVM -sample-id [optional-name]
```

Ver contadores de rendimiento específicos de pNFS (privilegios avanzados)

```
statistics show -object nfsv4_1 -vserver SVM
```

Ver la lista de contadores específicos de pNFS (privilegios avanzados)

```
statistics catalog counter show -object nfsv4_1 -counter *layout*|*device*
```

```
Object: nfsv4_1

Counter                      Description
---------------------------- ----------------------------------------------
getdeviceinfo_avg_latency    Average latency of NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_error          The number of failed NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_percent        Percentage of NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_success        The number of successful NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_total          Total number of NFSv4.1 GETDEVICEINFO
operations.
getdevicelist_avg_latency    Average latency of NFSv4.1 GETDEVICELIST
operations.
getdevicelist_error          The number of failed NFSv4.1 GETDEVICELIST
operations.
getdevicelist_percent        Percentage of NFSv4.1 GETDEVICELIST
operations.
getdevicelist_success        The number of successful NFSv4.1 GETDEVICELIST
operations.
getdevicelist_total          Total number of NFSv4.1 GETDEVICELIST
operations.
layoutcommit_avg_latency     Average latency of NFSv4.1 LAYOUTCOMMIT
operations.
layoutcommit_error           The number of failed NFSv4.1 LAYOUTCOMMIT
operations.
layoutcommit_percent         Percentage of NFSv4.1 LAYOUTCOMMIT operations.
layoutcommit_success         The number of successful NFSv4.1 LAYOUTCOMMIT
operations.
layoutcommit_total           Total number of NFSv4.1 LAYOUTCOMMIT
operations.
layoutget_avg_latency        Average latency of NFSv4.1 LAYOUTGET
operations.
layoutget_error              The number of failed NFSv4.1 LAYOUTGET
```

```
operations.
layoutget_percent           Percentage of NFSv4.1 LAYOUTGET operations.
layoutget_success           The number of successful NFSv4.1 LAYOUTGET
operations.
layoutget_total             Total number of NFSv4.1 LAYOUTGET operations.
layoutreturn_avg_latency    Average latency of NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_error          The number of failed NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_percent        Percentage of NFSv4.1 LAYOUTRETURN operations.
layoutreturn_success        The number of successful NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_total          Total number of NFSv4.1 LAYOUTRETURN
operations.
```

Ver conexiones de red activas para NFS

Puede verificar si se están realizando múltiples conexiones TCP al SVM con el `network connections active show` dominio.

Por ejemplo, si desea ver los troncales de sesión NFS, busque conexiones de los mismos clientes en diferentes interfaces por nodo:

```
cluster::*> network connections active show -node cluster-0* -vserver PNFS
              Vserver   Interface         Remote
      CID Ctx Name      Name:Local Port   Host:Port
Protocol/Service
--------- --- --------- ----------------- --------------------
----------------
Node: node-01
2304333128 14 PNFS      data1:2049        ubuntu22-224:740     TCP/nfs
2304333144 10 PNFS      data3:2049        ubuntu22-224:864     TCP/nfs
2304333151  5 PNFS      data1:2049        ubuntu22-226:848     TCP/nfs
2304333167 15 PNFS      data3:2049        ubuntu22-226:684     TCP/nfs
Node: node-02
2497668321 12 PNFS      data2:2049        ubuntu22-224:963     TCP/nfs
2497668337 18 PNFS      data4:2049        ubuntu22-224:859     TCP/nfs
2497668344 14 PNFS      data2:2049        ubuntu22-226:675     TCP/nfs
2497668360  7 PNFS      data4:2049        ubuntu22-226:903     TCP/nfs
```

Ver la información de la versión de NFS para los clientes conectados

También puede ver las conexiones NFS con el `nfs connected-clients show` dominio. Tenga en cuenta que la lista de clientes que se muestra son clientes que han tenido tráfico NFS activo en las últimas 48 horas. Es posible que los clientes NFS inactivos (incluso si aún están montados) no aparezcan hasta que se acceda al montaje. Puede filtrarlos para mostrar solo los clientes a los que accedió más recientemente especificando

el `-idle-time` característica.

Por ejemplo, para ver clientes con actividad en los últimos 10 minutos para el pNFS SVM:

```
cluster::*> nfs connected-clients show -vserver PNFS -idle-time <10m>

 Node: node-01

Vserver: PNFS Data-Ip: 10.x.x.x Local Remote Client-Ip Protocol Volume
Policy Idle-Time Reqs Reqs Trunking

10.x.x.a nfs4.2 PNFS_root default 9m 10s 0 149 false 10.x.x.a nfs4.2
FG_0001 default 9m 10s 135847 0 false 10.x.x.b nfs4.2 PNFS_root default 8m
12s 0 157 false 10.x.x.b nfs4.2 FG_0001 default 8m 12s 52111 0 false
```

Información relacionada

- "Obtenga más información sobre NFS paralelo (pNFS) en ONTAP"

Dependencias de nomenclatura de archivos y directorios NFS y SMB

Obtenga información sobre las dependencias de nombres de archivos y directorios de ONTAP NFS y SMB

Las convenciones de nomenclatura de archivos y directorios dependen tanto de los sistemas operativos de los clientes de red como de los protocolos de uso compartido de archivos, además de la configuración de idioma del clúster ONTAP y de los clientes.

El sistema operativo y los protocolos de uso compartido de archivos determinan lo siguiente:

- Caracteres que puede utilizar un nombre de archivo
- Distinción entre mayúsculas y minúsculas de un nombre de archivo

ONTAP admite caracteres de varios bytes en nombres de archivos, directorios y qtrees, según la versión de ONTAP.

Obtenga información sobre los caracteres válidos en diferentes sistemas operativos para SVM NFS de ONTAP

Si accede a un archivo o directorio desde clientes con sistemas operativos diferentes, debe utilizar caracteres válidos en ambos sistemas operativos.

Por ejemplo, si utiliza UNIX para crear un archivo o directorio, no utilice dos puntos (:) en el nombre porque no se permiten dos puntos en los nombres de archivos o directorios de MS-dos. Debido a que las restricciones de caracteres válidos varían de un sistema operativo a otro, consulte la documentación del sistema operativo cliente para obtener más información acerca de los caracteres prohibidos.

Obtenga información sobre la distinción entre mayúsculas y minúsculas de los nombres de archivos y directorios en un entorno multiprotocolo ONTAP NFS

Los nombres de archivo y directorio distinguen mayúsculas y minúsculas para los clientes NFS y no distinguen entre mayúsculas y minúsculas, pero sí lo hacen para los clientes SMB. Debe comprender las implicaciones que tiene en un entorno multiprotocolo y las acciones que podría tener que tomar al especificar la ruta al crear recursos compartidos de SMB y al acceder a datos dentro de los recursos compartidos.

Si un cliente SMB crea un directorio denominado `testdir`, los clientes SMB y NFS muestran el nombre del archivo como `testdir`. Sin embargo, si un usuario SMB intenta crear un nombre de directorio más adelante `TESTDIR` , el nombre no está permitido porque, para el cliente SMB, ese nombre existe actualmente. Si un usuario NFS crea posteriormente un directorio denominado `TESTDIR`, los clientes NFS y SMB muestran el nombre del directorio de forma diferente, de la siguiente manera:

- En los clientes NFS, puede ver los nombres de directorio a medida que se crearon, por ejemplo `testdir` y `TESTDIR`, porque los nombres de directorio distinguen entre mayúsculas y minúsculas.
- Los clientes SMB utilizan los nombres 8.3 para distinguir entre los dos directorios. Un directorio tiene el nombre del archivo base. A directorios adicionales se les asigna un nombre de archivo 8.3.
  - En clientes SMB, puede ver `testdir` y `TESTDI~1`.
  - ONTAP crea el `TESTDI~1` nombre del directorio para diferenciar los dos directorios.

    En este caso, debe usar el nombre 8.3 al especificar una ruta de recurso compartido mientras crea o modifica un recurso compartido en una máquina virtual de almacenamiento (SVM).

Del mismo modo para los archivos, si un cliente SMB lo crea `test.txt`, los clientes SMB y NFS muestran el nombre del archivo como `text.txt`. Sin embargo, si un usuario SMB intenta crear `Test.txt`, el nombre no está permitido porque, para el cliente SMB, ese nombre existe actualmente. Si un usuario NFS crea posteriormente un archivo denominado `Test.txt`, los clientes NFS y SMB muestran el nombre del archivo de forma diferente, de la siguiente manera:

- En los clientes NFS, verá los nombres de archivo a medida que se crearon y `test.txt` `Test.txt` , porque los nombres de archivo distinguen entre mayúsculas y minúsculas.
- Los clientes SMB utilizan los nombres 8.3 para distinguir entre los dos archivos. Un archivo tiene el nombre del archivo base. Se asigna un nombre de archivo 8.3 a archivos adicionales.
  - En clientes SMB, puede ver `test.txt` y `TEST~1.TXT`.
  - ONTAP crea el `TEST~1.TXT` nombre de archivo para diferenciar los dos archivos.

> Si se ha creado una asignación de caracteres con los comandos de asignación de caracteres CIFS de Vserver, una búsqueda de Windows que normalmente no distingue entre mayúsculas y minúsculas puede distinguir entre mayúsculas y minúsculas. Esto significa que las búsquedas de nombre de archivo solo serán sensibles a mayúsculas/minúsculas si se ha creado la asignación de caracteres y el nombre de archivo está utilizando esa asignación de caracteres.

Aprenda a crear nombres de archivos y directorios NFS de ONTAP

ONTAP crea y mantiene dos nombres para archivos o directorios en cualquier directorio que tenga acceso desde un cliente SMB: El nombre largo original y un nombre en

formato 8.3.

Para los nombres de archivos o directorios que excedan el nombre de ocho caracteres o el límite de extensión de tres caracteres (para archivos), ONTAP genera un nombre de formato de 8.3 de la siguiente manera:

- Trunca el nombre del archivo o directorio original a seis caracteres, si el nombre supera los seis.
- Agrega una tilde (~) y un número, de uno a cinco, a los nombres de archivo o directorio que ya no son únicos después de truncarse.

  Si se queda sin números porque hay más de cinco nombres similares, crea un nombre único que no tiene relación con el nombre original.

- En el caso de los archivos, trunca la extensión del nombre de archivo a tres caracteres.

Por ejemplo, si un cliente NFS crea un archivo llamado `specifications.html`, el nombre de archivo de formato 8,3 creado por ONTAP es `specif~1.htm`. Si este nombre ya existe, ONTAP utiliza un número diferente al final del nombre de archivo. Por ejemplo, si un cliente NFS crea otro archivo denominado `specifications_new.html`, el formato 8,3 de `specifications_new.html` es `specif~2.htm`.

Obtenga información sobre el manejo de nombres de archivos, directorios y qtree de múltiples bytes en ONTAP NFS

A partir de ONTAP 9.5, la compatibilidad con nombres codificados UTF-8 de 4 bytes permite la creación y visualización de nombres de archivos, directorios y árboles que incluyen caracteres complementarios Unicode fuera del plano multilingüe básico (BMP). En las versiones anteriores, estos caracteres complementarios no se mostraba correctamente en entornos multiprotocolo.

Para habilitar la compatibilidad con nombres codificados UTF-8 de 4 bytes, hay disponible un nuevo código de idioma *utf8mb4* para las `vserver volume` familias de comandos y.

- Debe crear un nuevo volumen de una de las siguientes maneras:
- Configuración `-language` explícita de la opción volume:

  ```
  volume create -language utf8mb4 {…}
  ```

- Heredar `-language` la opción de volumen de una SVM que se haya creado o modificado para la opción:

  ```
  vserver [create|modify] -language utf8mb4 {…}``volume create {…}
  ```

- Si utiliza ONTAP 9,6 y versiones anteriores, no podrá modificar los volúmenes existentes para admitir utf8mb4; debe crear un nuevo volumen listo para utf8mb4 y después migrar los datos con las herramientas de copia basadas en cliente.

  Si utiliza ONTAP 9.7P1 o una versión posterior, puede modificar los volúmenes existentes para utf8mb4 con una solicitud de soporte. Para obtener más información, consulte "¿Se puede cambiar el idioma del volumen después de crearlo en ONTAP?".

+ Puede actualizar SVM para soporte utf8mb4, pero los volúmenes existentes conservan sus códigos de idioma originales.

+

Los nombres de las LUN con caracteres UTF-8 de 4 bytes no se admiten actualmente.

- Los datos de caracteres Unicode se suelen representar en aplicaciones de sistemas de archivos Windows que utilizan el formato de transformación Unicode de 16 bits (UTF-16) y en sistemas de archivos NFS que utilizan el formato de transformación Unicode de 8 bits (UTF-8).

  En las versiones anteriores a ONTAP 9.5, los nombres incluidos los caracteres complementarios UTF-16 creados por los clientes de Windows se mostraban correctamente a otros clientes de Windows pero no se tradujeron correctamente a UTF-8 para los clientes NFS. Del mismo modo, los nombres con caracteres complementarios UTF-8 de los clientes NFS creados no se tradujeron correctamente a UTF-16 para los clientes Windows.

- Cuando se crean nombres de archivo en sistemas que ejecutan ONTAP 9.4 o una versión anterior que contienen caracteres complementarios válidos o no válidos, ONTAP rechaza el nombre de archivo y devuelve un error de nombre de archivo no válido.

  Para evitar este problema, utilice sólo los caracteres BMP en los nombres de archivo y evite utilizar caracteres complementarios, o actualice a ONTAP 9.5 o posterior.

Se permiten caracteres Unicode en nombres de qtree.

- Puede usar `volume qtree` la familia de comandos o System Manager para configurar o modificar los nombres de qtree.
- Los nombres de qtree pueden incluir caracteres de varios bytes en formato Unicode, como los caracteres japoneses y chinos.
- En versiones anteriores a ONTAP 9.5, sólo se admiten los caracteres BMP (es decir, los que podrían representarse en 3 bytes).

  En las versiones anteriores a ONTAP 9.5, la ruta de unión del volumen principal del qtree puede contener nombres de qtree y directorio con caracteres Unicode. El `volume show` comando muestra estos nombres correctamente cuando el volumen primario tiene una configuración de idioma UTF-8. Sin embargo, si el idioma del volumen principal no es uno de los valores de idioma UTF-8, algunas partes de la ruta de unión se muestran utilizando un nombre NFS alternativo numérico.

- En las versiones 9.5 y posteriores, se admiten caracteres de 4 bytes en nombres de qtree, siempre y cuando el qtree se encuentre en un volumen habilitado para utf8mb4.

Configurar la asignación de caracteres para la traducción de nombres de archivos SMB en volúmenes NFS de ONTAP

Los clientes NFS pueden crear nombres de archivo que contengan caracteres que no son válidos para los clientes SMB y ciertas aplicaciones Windows. Puede configurar la asignación de caracteres para la traducción de nombres de archivo en volúmenes para permitir que los clientes SMB accedan a archivos con nombres NFS que, de lo contrario, no serían válidos.

Acerca de esta tarea

Cuando los clientes SMB acceden a los archivos creados por los clientes NFS, ONTAP observa el nombre del archivo. Si el nombre no es un nombre de archivo SMB válido (por ejemplo, si tiene un carácter "':'" incrustado en dos puntos), ONTAP devuelve el nombre de archivo 8.3 que se mantiene para cada archivo. Sin embargo,

esto causa problemas para las aplicaciones que codifican información importante en nombres de archivos largos.

Por lo tanto, si comparte un archivo entre clientes en diferentes sistemas operativos, debe utilizar caracteres en los nombres de archivo válidos en ambos sistemas operativos.

Sin embargo, si tiene clientes NFS que crean nombres de archivo que contienen caracteres que no son nombres de archivo válidos para clientes SMB, puede definir un mapa que convierte los caracteres NFS no válidos en caracteres Unicode que tanto SMB como determinadas aplicaciones Windows aceptan. Por ejemplo, esta funcionalidad admite las aplicaciones CATIA MCAD y Mathematica, así como otras aplicaciones que tienen este requisito.

Puede configurar la asignación de caracteres de volumen a volumen.

Debe tener en cuenta lo siguiente al configurar la asignación de caracteres en un volumen:

- La asignación de caracteres no se aplica a través de puntos de unión.

  Debe configurar explícitamente la asignación de caracteres para cada volumen de unión.

- Debe asegurarse de que los caracteres Unicode que se utilizan para representar caracteres no válidos o ilegales son caracteres que normalmente no aparecen en los nombres de archivo; de lo contrario, se producen asignaciones no deseadas.

  Por ejemplo, si intenta asignar dos puntos (:) a un guión (-) pero el guión (-) se utilizó correctamente en el nombre del archivo, un cliente de Windows que intente acceder a un archivo denominado «'a-b'» tendría su solicitud asignada al nombre NFS de «'a:b'» (no al resultado deseado).

- Después de aplicar la asignación de caracteres, si la asignación aún contiene un carácter de Windows no válido, ONTAP vuelve a los nombres de archivo de Windows 8.3.
- En las notificaciones de FPolicy, los registros de auditoría de NAS y los mensajes de seguimiento de seguridad, se muestran los nombres de archivos asignados.
- Cuando se crea una relación de SnapMirror del tipo DP, la asignación de caracteres del volumen de origen no se replica en el volumen de DP de destino.
- Distinción entre mayúsculas y minúsculas: Debido a que los nombres de Windows asignados se convierten en nombres NFS, la búsqueda de los nombres sigue a la semántica NFS. Esto incluye el hecho de que las búsquedas de NFS distinguen mayúsculas de minúsculas. Esto significa que las aplicaciones que acceden a recursos compartidos asignados no deben depender de un comportamiento que no distingue mayúsculas y minúsculas de Windows. Sin embargo, el nombre 8.3 está disponible y no distingue mayúsculas y minúsculas.
- Asignaciones parciales o no válidas: Tras asignar un nombre para devolver a los clientes que realizan enumeración de directorios ("dir"), se comprueba la validez de Windows en el nombre Unicode resultante. Si ese nombre sigue teniendo caracteres no válidos, o si no es válido para Windows (p. ej., finaliza en "". o en blanco) se devuelve el nombre 8.3 en lugar del nombre no válido.

Paso

1. Configurar asignación de caracteres:

   ```
   vserver cifs character-mapping create -vserver vserver_name -volume
   volume_name -mapping mapping_text, ...
   ```

   El mapeo consta de una lista de pares de caracteres fuente-objetivo separados por "':'". Los caracteres son caracteres Unicode introducidos mediante dígitos hexadecimales. Por ejemplo: 3C:E03C.

El primer valor de cada `mapping_text` par que está separado por dos puntos es el valor hexadecimal del carácter NFS que desea traducir, y el segundo valor es el valor Unicode que utiliza SMB. Las parejas de asignación deben ser únicas (debe existir una asignación uno a uno).

- Asignación de origen

  La siguiente tabla muestra el conjunto de caracteres Unicode permisible para la asignación de origen:

Carácter Unicode	Carácter impreso	Descripción
0x01-0x19	No aplicable	Caracteres de control que no se imprimen
0x5C	\	Barra invertida
0x3A	:	Dos puntos
0x2A	*	Asterisco
0x3F	?	Signo de interrogación
0x22	"	Entre comillas
0x3C	<	Menor que
0x3E	>	Mayor que
0x7C		
Línea vertical	0xB1	±

- Asignación de objetivos

  Puede especificar caracteres de destino en el "'Área de uso privado'" de Unicode en el siguiente intervalo: U+E0000…U+F8FF.

Ejemplo

El siguiente comando crea una asignación de caracteres para un volumen denominado «data» en la máquina virtual de almacenamiento (SVM) vs1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  -----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

Comandos NFS de ONTAP para administrar asignaciones de caracteres para la traducción de nombres de archivos SMB

Puede gestionar la asignación de caracteres creando, modificando, mostrando información o eliminando asignaciones de caracteres de archivo utilizadas para la traducción del nombre del archivo SMB en volúmenes FlexVol.

Si desea…	Se usa este comando…
Cree nuevas asignaciones de caracteres de archivo	`vserver cifs character-mapping create`
Mostrar información acerca de las asignaciones de caracteres de archivo	`vserver cifs character-mapping show`
Modifique las asignaciones de caracteres de archivo existentes	`vserver cifs character-mapping modify`
Eliminar asignaciones de caracteres de archivo	`vserver cifs character-mapping delete`

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

Gestión de enlaces NFS

Obtenga más información sobre la conexión de enlaces NFS de ONTAP

A partir de ONTAP 9.14.1, los clientes NFSv4,1 pueden aprovechar la conexión de enlaces de sesión para abrir varias conexiones a diferentes LIF en el servidor NFS, lo que aumenta la velocidad de transferencia de datos y ofrece resiliencia a través de la multivía.

La conexión de enlaces proporciona ventajas para exportar volúmenes de FlexVol a clientes con capacidad de Trunking, en particular clientes VMware y Linux o para NFS a través de RDMA, TCP o pNFS.

En ONTAP 9.14.1, la conexión de enlaces se limita a las LIF en un único nodo; la conexión de enlaces no puede abarcar las LIF en varios nodos.

Los volúmenes FlexGroup se admiten para la conexión de enlaces. Aunque puede proporcionar un mejor rendimiento, el acceso multivía a un volumen FlexGroup solo puede configurarse en un único nodo.

En esta versión, solo se admite la conexión troncal de sesión para el acceso multivía.

Cómo utilizar trunking

Para aprovechar las ventajas de las rutas múltiples que ofrece la conexión de enlaces, necesita un conjunto de LIF, denominados *grupo de conexión troncal*, asociados a la SVM que contiene un servidor NFS habilitado para conexión de enlaces. Las LIF de un grupo de enlaces deben tener puertos iniciales en el mismo nodo del

clúster y deben residir en esos puertos iniciales. Es recomendable que todas las LIF de un grupo de enlaces sean miembros del mismo grupo de recuperación tras fallos.

ONTAP admite hasta 16 conexiones troncalizadas por nodo desde un cliente determinado.

Cuando un cliente monta exportaciones desde un servidor habilitado para conexión de enlaces, especifica una serie de direcciones IP para las LIF en un grupo de conexiones. Una vez que el cliente se conecta a la primera LIF, los LIF adicionales solo se agregan a la sesión NFSv4,1 y se usan para la conexión de enlaces si cumplen los requisitos de grupo de Trunking. A continuación, el cliente distribuye las operaciones de NFS a través de las múltiples conexiones basadas en su propio algoritmo (como round-robin).

Para obtener el mejor rendimiento, se debe configurar el enlace de enlaces en una SVM que se dedique a proporcionar exportaciones multivía, no de rutas únicas. Es decir, solo debe habilitar la conexión troncal en un servidor NFS en una SVM cuyas exportaciones se proporcionan únicamente a clientes habilitados para la conexión troncal.

Clientes admitidos

El servidor ONTAP NFSv4,1 admite la conexión troncal con cualquier cliente capaz de realizar una conexión troncal de sesión NFSv4,1.

Los siguientes clientes han sido probados con ONTAP 9.14.1:

- VMware: ESXi 7.0U3F y versiones posteriores
- Linux: Red Hat Enterprise Linux (RHEL) 8,8 y 9,3

> El cliente NFS de RHEL no volverá a establecer la conexión troncal si los LIF troncales se migran a otro nodo en un evento de conmutación por error (como una recuperación tras fallos de la controladora). Cuando las LIF se migran a otro nodo, se eliminan del grupo de enlaces. Si se migran todas las LIF del grupo de enlaces, el cliente NFS únicamente utilizará el primer LIF para continuar con las operaciones de I/O.

> Al habilitar la conexión troncal en un servidor NFS, los usuarios que acceden a recursos compartidos exportados en clientes NFS que no admiten la conexión troncal pueden ver una caída de rendimiento. Esto se debe a que solo se utiliza una única conexión TCP para varios montajes en las LIF de datos de SVM.

Diferencia entre la conexión de enlaces NFS y nconnect

A partir de ONTAP 9.8, la funcionalidad nconnect está disponible de forma predeterminada con NFSv4.1 habilitado. En clientes que admiten nconnect, un solo montaje NFS puede tener varias conexiones TCP (hasta 16) a través de un único LIF.

Por el contrario, la función de enlace es la funcionalidad *multipathing*, que proporciona varias conexiones TCP a través de varias LIF. Si tiene la capacidad de emplear NIC adicionales en su entorno, la troncalización proporciona un mayor paralelismo y rendimiento más allá de la capacidad de nconnect.

Más información sobre "nconectar".

Configurar un nuevo servidor NFS y exportar para trunking

Cree un servidor NFS habilitado para la conexión de enlaces en una SVM de ONTAP

A partir de ONTAP 9.14.1, se puede habilitar la conexión troncal en servidores NFS. NFSv4,1 está habilitado de forma predeterminada cuando se crean servidores NFS.

Antes de empezar

Para crear un servidor NFS habilitado para la conexión de enlaces, se requiere una SVM. La SVM debe ser:

- respaldado por suficiente almacenamiento para los requisitos de datos de cliente.
- Habilitado para NFS.

Puede utilizar una SVM existente; sin embargo, al habilitar la conexión troncal se deben volver a montar todos los clientes NFSv4.x, lo que puede causar interrupciones. Si no es posible volver a montar, cree una nueva SVM para el servidor NFS.

Pasos

1. Si no existe una SVM adecuada, cree una:

   ```
   vserver create -vserver svm_name -rootvolume root_volume_name -aggregate
   aggregate_name -rootvolume-security-style unix -language C.UTF-8
   ```

2. Compruebe la configuración y el estado de la SVM recién creada:

   ```
   vserver show -vserver svm_name
   ```

   Más información sobre "Creación de una SVM".

3. Cree el servidor NFS:

   ```
   vserver nfs create -vserver svm_name -v3 disabled -v4.0 disabled -v4.1 enabled
   -v4.1-trunking enabled -v4-id-domain my_domain.com
   ```

4. Compruebe que NFS está ejecutando:

   ```
   vserver nfs status -vserver svm_name
   ```

5. Compruebe que NFS está configurado como se desea:

   ```
   vserver nfs show -vserver svm_name
   ```

   Más información acerca de "Configuración del servidor NFS."

Después de terminar

Configure los siguientes servicios según sea necesario:

- "DNS"
- "LDAP"
- "Kerberos"

Prepare la red para la conexión de enlaces NFS de ONTAP

Para aprovechar la conexión de enlaces NFSv4,1, los LIF de un grupo de enlaces deben residir en el mismo nodo y tener puertos de inicio en el mismo nodo. Las LIF deben estar configuradas en un grupo de conmutación por error del mismo nodo.

Acerca de esta tarea

Una asignación uno a uno de LIF y NIC proporciona la mayor ganancia de rendimiento, pero no es necesaria para permitir la conexión de enlaces. Tener al menos dos NIC instaladas puede ofrecer un beneficio de rendimiento, pero no es necesario.

Todas las LIF del grupo de enlaces deben pertenecer al mismo grupo de conmutación al nodo de respaldo. Tenga en cuenta que cuando las LIF están configuradas en un grupo de conmutación por error en el mismo nodo, una recuperación tras fallos de controladora de ese nodo puede provocar que las LIF se desconecten. Si las LIF no están configuradas en un grupo de recuperación tras fallos en el mismo nodo y la recuperación tras fallos a otro nodo, la conexión de enlaces ya no funcionará.

Debe ajustar el grupo de conmutación por error de troncalización cada vez que agregue o elimine conexiones (y NIC subyacentes) de un grupo de conmutación por error.

Antes de empezar

- Debe conocer los nombres de puerto asociados a las NIC para crear un grupo de conmutación por error.
- Los puertos deben estar todos en el mismo nodo.

Pasos

1. Compruebe los nombres y el estado de los puertos de red que desea utilizar:

   ```
   network port show
   ```

2. Cree el grupo de failover:

   ```
   network interface failover-groups create -vserver <svm_name> -failover-group
   <failover_group_name> -targets <ports_list>
   ```

   No es un requisito tener un grupo de recuperación tras fallos, pero es muy recomendable.

   - `<svm_name>` Es el nombre de la SVM que contiene el servidor NFS.
   - `<ports_list>` es la lista de puertos que se agregarán al grupo de failover.

     Los puertos se agregan en el formato `<node_name>:<port_number>`, por ejemplo `node1:e0c`: .

     El siguiente comando crea el grupo de conmutación al nodo de respaldo FG3 para SVM VS1 y añade tres puertos:

     ```
     network interface failover-groups create -vserver vs1 -failover-group fg3
     -targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
     ```

     Más información acerca de "grupos de conmutación por error."

   Obtenga más información sobre `network interface failover-groups create` en el "Referencia

de comandos del ONTAP".

3. Si es necesario, cree LIF para los miembros del grupo de enlaces:

   `network interface create -vserver <svm_name> -lif <lif_name> -home-node <node_name> -home-port <port_name> -address <IP_address> -netmask <IP_address> [-service-policy <policy>] [-auto-revert <true|false>]`

   - `-home-node` - El nodo al que regresa la LIF cuando se ejecuta el comando network interface revert en la LIF.

     También puede especificar si el LIF debe volver automáticamente al nodo de inicio y al puerto de inicio con `-auto-revert` la opción.

   - `-home-port` Es el puerto físico o lógico al que devuelve la LIF cuando el comando de reversión de la interfaz de red se ejecuta en la LIF.
   - Puede especificar una dirección IP con las `-address -netmask` opciones y, no con `-subnet` la opción.
   - Al asignar direcciones IP, es posible que deba configurar una ruta predeterminada a una puerta de enlace si hay clientes o controladores de dominio en una subred IP diferente. Obtenga más información sobre `network route create` y cómo crear una ruta estática dentro de una SVM en el "Referencia de comandos del ONTAP".
   - `-service-policy` - La política de servicio para la LIF. Si no se especifica ninguna política, se asignará automáticamente una política predeterminada. Utilice `network interface service-policy show` el comando para revisar las políticas de servicio disponibles.
   - `-auto-revert` - Especificar si una LIF de datos se revierte automáticamente a su nodo de inicio en circunstancias como el inicio, cambios en el estado de la base de datos de administración, o cuando se realiza la conexión de red. La configuración predeterminada es false, pero puede establecerla en true en función de las políticas de gestión de red del entorno.

     Repita este paso para cada LIF del grupo de enlaces.

     El siguiente comando crea `lif-A` para la SVM `vs1`, en el puerto `e0c` del nodo `cluster1_01`:

     ```
     network interface create -vserver vs1 -lif lif-A -service-policy default-intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
     ```

   Más información acerca de "Creación de LIF."

4. Comprobar que se han creado las LIF:

   ```
   network interface show
   ```

5. Compruebe que se pueda acceder a la dirección IP configurada:

Para verificar una…	Usar…
Dirección IPv4	`network ping`
Dirección IPv6	`network ping6`

Información relacionada

- "ping de red"
- "interfaz de red"
- "muestra el puerto de red"

Cree una política de exportación de volúmenes de ONTAP

Para ofrecer al cliente acceso a recursos compartidos de datos, debe crear uno o varios volúmenes y el volumen debe tener políticas de exportación con al menos una regla.

Requisitos de exportación del cliente:

- Los clientes de Linux deben tener un montaje independiente y un punto de montaje independiente para cada conexión de Trunking (es decir, para cada LIF).
- Los clientes de VMware solo requieren un único punto de montaje para un volumen exportado, con varias LIF especificadas.

  Los clientes de VMware requieren acceso raíz en la política de exportación.

Pasos

1. Cree una política de exportación:

   ```
   vserver export-policy create -vserver svm_name -policyname policy_name
   ```

   El nombre de la política puede tener hasta 256 caracteres.

2. Compruebe que se ha creado la política de exportación:

   ```
   vserver export-policy show -policyname policy_name
   ```

   Ejemplo

   Los siguientes comandos crean y verifican la creación de una política de exportación llamada exp1 en la SVM llamada vs1:

   ```
   vs1::> vserver export-policy create -vserver vs1 -policyname exp1
   ```

3. Cree una regla de exportación y añádala a una política de exportación existente:

   ```
   vserver export-policy rule create -vserver svm_name -policyname policy_name
   -ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,…" }
   -rorule security_type -rwrule security_type -superuser security_type -anon
   user_ID
   ```

   ```
   `-clientmatch`El parámetro debe identificar los clientes Linux o VMware
   compatibles con la conexión de enlaces que montarán la exportación.
   ```

   Más información acerca de "creación de reglas de exportación."

4. Cree el volumen con un punto de unión:

```
volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
-size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
-group group_name_or_number -junction-path junction_path -policy
export_policy_name
```

Más información sobre "creando volúmenes."

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

```
volume show -vserver svm_name -volume volume_name -junction-path
```

Montaje de volúmenes de ONTAP o recursos compartidos de datos para la conexión de enlaces NFS

Los clientes de Linux y VMware compatibles con la conexión de enlaces pueden montar volúmenes o recursos compartidos de datos desde un servidor ONTAP NFSv4,1 que esté habilitado para la conexión de enlaces.

Obtenga más información "clientes admitidos"sobre .

Requisitos del cliente Linux

Si utiliza ONTAP 9.16.1 o posterior y Red Hat Enterprise Linux versión 8,7 o posterior (para RHEL 8) o 9,2 o posterior (para RHEL 9) como cliente Linux, solo se necesita un punto de montaje para el grupo de enlaces. Monte los volúmenes exportados con este comando con `trunkdiscovery` la opción:

```
mount <lif_ip>:<volume_name> </mount_path> -o trunkdiscovery,vers=4.1
```

De lo contrario, se necesita un punto de montaje independiente para cada conexión del grupo de troncalización. Monte el volumen exportado con comandos similares a los siguientes, con la `max_connect` opción:

```
mount <lif1_ip>:<volume_name> </mount_path1> -o vers=4.1,max_connect=16
```

```
mount <lif2_ip>:<volume_name> </mount_path2> -o vers=4.1,max_connect=16
```

(`vers`El valor version) debe ser `4.1` o posterior.

El `max_connect` valor corresponde al número de conexiones del grupo de troncalización.

Requisitos del cliente de VMware

Se necesita una sentencia mount que incluya una dirección IP para cada conexión del grupo de enlaces.

Monte el almacén de datos exportado con un comando similar al siguiente:

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

```
`-H`Los valores corresponden a las conexiones del grupo de
troncalización.
```

Adapte las exportaciones NFS existentes para la conexión de enlaces

Adapte las exportaciones de ruta única para la conexión de enlaces NFS de ONTAP

Puede adaptar una exportación NFSv4,1 de ruta única existente (no troncalizada) para utilizar troncalización. Los clientes compatibles con trunking pueden aprovechar el rendimiento mejorado en cuanto se activa la troncalización en el servidor, siempre y cuando se cumplan los requisitos previos del servidor y del cliente.

La adaptación de una exportación de ruta única para la conexión de enlaces le permite mantener conjuntos de datos exportados en sus volúmenes y SVM existentes. Para ello, debe habilitar la conexión troncal en el servidor NFS, actualizar la configuración de redes y exportación y volver a montar el recurso compartido exportado en los clientes.

La activación de la conexión troncal tiene el efecto de reiniciar el servidor. Luego, los clientes de VMware deben volver a montar los almacenes de datos exportados; los clientes Linux deben volver a montar los volúmenes exportados con `max_connect` la opción.

Habilite la conexión troncal en un servidor NFS de ONTAP

La conexión troncal debe estar explícitamente habilitada en los servidores NFS. NFSv4,1 está habilitado de forma predeterminada cuando se crean servidores NFS.

Después de activar la conexión troncal, verifique que los siguientes servicios estén configurados según sea necesario.

- "DNS"
- "LDAP"
- "Kerberos"

Pasos

1. Active la conexión troncal y asegúrese de que NFSv4,1 está activado:

   ```
   vserver nfs create -vserver svm_name -v4.1 enabled -v4.1-trunking enabled
   ```

2. Compruebe que NFS se está ejecutando:
   `vserver nfs status -vserver svm_name`
3. Compruebe que NFS está configurado como se desea:

   ```
   vserver nfs show -vserver svm_name
   ```

   Más información sobre "Configuración del servidor NFS.".. Si ofrece servicio a clientes de Windows desde esta SVM, mueva los recursos compartidos y elimine el servidor.
   `vserver cifs show -vserver svm_name`

   +
   `vserver cifs delete -vserver svm_name`

Actualice la red para la conexión de enlaces NFS de ONTAP

Para aprovechar la conexión de enlaces NFSv4,1, los LIF de un grupo de enlaces deben residir en el mismo nodo y tener puertos de inicio en el mismo nodo. Las LIF deben estar configuradas en un grupo de conmutación por error del mismo nodo.

Acerca de esta tarea

Una asignación uno a uno de LIF y NIC proporciona la mayor ganancia de rendimiento, pero no es necesaria para permitir la conexión de enlaces. Tener al menos dos NIC instaladas puede ofrecer un beneficio de rendimiento, pero no es necesario.

Todas las LIF del grupo de enlaces deben pertenecer al mismo grupo de conmutación al nodo de respaldo. Tenga en cuenta que cuando las LIF están configuradas en un grupo de conmutación por error en el mismo nodo, una recuperación tras fallos de controladora de ese nodo puede provocar que las LIF se desconecten. Si las LIF no están configuradas en un grupo de recuperación tras fallos en el mismo nodo y la recuperación tras fallos a otro nodo, la conexión de enlaces ya no funcionará.

Debe ajustar el grupo de conmutación por error de troncalización cada vez que agregue o elimine conexiones (y NIC subyacentes) de un grupo de conmutación por error.

Antes de empezar

- Debe conocer los nombres de puerto asociados a las NIC para crear un grupo de conmutación por error.
- Los puertos deben estar todos en el mismo nodo.

Pasos

1. Compruebe los nombres y el estado de los puertos de red que desea utilizar:

   ```
   network port show
   ```

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

2. Cree un grupo de failover de trunking o modifique uno existente para trunking:

   ```
   network interface failover-groups create -vserver <svm_name> -failover-group
   <failover_group_name> -targets <ports_list>
   ```

   ```
   network interface failover-groups modify -vserver <svm_name> -failover-group
   <failover_group_name> -targets <ports_list>
   ```

   No es un requisito tener un grupo de recuperación tras fallos, pero es muy recomendable.

   - `<svm_name>` Es el nombre de la SVM que contiene el servidor NFS.
   - `<ports_list>` es la lista de puertos que se agregarán al grupo de failover.

     Los puertos se agregan en el formato `<node_name>:<port_number>`, por ejemplo, `node1:e0c`.

     El siguiente comando crea un grupo de conmutación al nodo de respaldo `fg3` para la SVM VS1 y añade tres puertos:

     ```
     network interface failover-groups create -vserver vs1 -failover-group fg3
     -targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
     ```

   Más información acerca de "grupos de conmutación por error."

3. Cree LIF adicionales para los miembros del grupo de enlaces según sea necesario:

   ```
   network interface create -vserver <svm_name> -lif <lif_name> -home-node
   <node_name> -home-port <port_name> -address <IP_address> -netmask <IP_address>
   [-service-policy <policy>] [-auto-revert <true|false>]
   ```

   - `-home-node` - El nodo al que regresa la LIF cuando se ejecuta el comando network interface revert en la LIF.

     Puede especificar si la LIF debe revertir automáticamente al nodo raíz y al puerto de inicio con la `-auto-revert` opción.

   - `-home-port` Es el puerto físico o lógico al que devuelve la LIF cuando el comando de reversión de la interfaz de red se ejecuta en la LIF.

- Puede especificar una dirección IP con las `-address -netmask` opciones y.
- Cuando se asignan direcciones IP manualmente (sin utilizar una subred), es posible que deba configurar una ruta predeterminada a una puerta de enlace si existen clientes o controladores de dominio en una subred IP diferente. `network route create`La página de comandos contiene información acerca de la creación de una ruta estática dentro de una SVM. Obtenga más información sobre `network route create` en el "Referencia de comandos del ONTAP".
- `-service-policy` - La política de servicio para la LIF. Si no se especifica ninguna política, se asignará automáticamente una política predeterminada. Utilice `network interface service-policy show` el comando para revisar las políticas de servicio disponibles.

  Obtenga más información sobre `network interface service-policy show` en el "Referencia de comandos del ONTAP".

- `-auto-revert` - Especificar si una LIF de datos se revierte automáticamente a su nodo de inicio en circunstancias como el inicio, cambios en el estado de la base de datos de administración, o cuando se realiza la conexión de red. **La configuración predeterminada es false**, pero puedes configurarla en true dependiendo de las políticas de administración de red de tu entorno.

  Repita este paso con cada LIF adicional necesario en el grupo de enlaces.

  El siguiente comando crea `lif-A` para la SVM `vs1`, en el puerto `e0c` del nodo `cluster1_01`:

  ```
  network interface create -vserver vs1 -lif lif-A -service-policy default-intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
  ```

Más información acerca de "Creación de LIF."

4. Compruebe que las LIF se han creado:

   ```
   network interface show
   ```

5. Compruebe que se pueda acceder a la dirección IP configurada:

Para verificar una…	Usar…
Dirección IPv4	`network ping`
Dirección IPv6	`network ping6`

Información relacionada

- "ping de red"
- "interfaz de red"

Modifique las políticas de exportación de volúmenes ONTAP

Para que los clientes puedan aprovechar la conexión de enlaces para los recursos compartidos de datos existentes, es posible que deba modificar las políticas y reglas de exportación y los volúmenes a los que están asociados. Hay diversos requisitos de

exportación para los clientes Linux y los almacenes de datos VMware.

Requisitos de exportación del cliente:

- Los clientes de Linux deben tener un montaje independiente y un punto de montaje independiente para cada conexión de Trunking (es decir, para cada LIF).

  Si va a actualizar a ONTAP 9.14.1 y ya ha exportado un volumen, puede seguir usando ese volumen en un grupo de enlaces.

- Los clientes de VMware solo requieren un único punto de montaje para un volumen exportado, con varias LIF especificadas.

  Los clientes de VMware requieren acceso raíz en la política de exportación.

Pasos

1. Compruebe que haya vigente una política de exportación existente:

   ```
   vserver export-policy show
   ```

2. Compruebe que las reglas de política de exportación existentes son adecuadas para la configuración de trunking:

   ```
   vserver export-policy rule show -policyname policy_name
   ```

   En concreto, compruebe que el `-clientmatch` parámetro identifica correctamente los clientes de Linux o VMware que admitirán la conexión en línea que montarán la exportación.

   Si es necesario realizar ajustes, modifique la regla con el `vserver export-policy rule modify` comando o cree una nueva regla:

   ```
   vserver export-policy rule create -vserver svm_name -policyname policy_name
   -ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,…" }
   -rorule security_type -rwrule security_type -superuser security_type -anon
   user_ID
   ```

   Más información acerca de "creación de reglas de exportación."

3. Verifique que los volúmenes exportados existentes estén en línea:

   ```
   volume show -vserver svm_name
   ```

Vuelva a montar volúmenes ONTAP o recursos compartidos de datos para la conexión de enlaces NFS

Para convertir conexiones de cliente no troncalizadas en conexiones troncales, los montajes existentes en clientes Linux y VMware deben desmontarse y volver a montarse utilizando la información acerca de las LIF.

Obtenga más información "clientes admitidos"sobre .

El desmontaje de los clientes de VMware provoca interrupciones en las máquinas virtuales del almacén de datos. Una alternativa sería crear un nuevo almacén de datos habilitado para trunking, y usar **storage vmotion** para mover sus VM del antiguo almacén de datos al nuevo. Consulte la documentación de VMware para más detalles.

Requisitos del cliente Linux

Si utiliza ONTAP 9.16.1 o posterior y Red Hat Enterprise Linux versión 8,7 o posterior (para RHEL 8) o 9,2 o posterior (para RHEL 9) como cliente Linux, solo se necesita un punto de montaje para el grupo de enlaces. Monte los volúmenes exportados con este comando con `trunkdiscovery` la opción:

```
mount <lif_ip>:<volume_name> </mount_path> -o trunkdiscovery,vers=4.1
```

De lo contrario, se necesita un punto de montaje independiente para cada conexión del grupo de troncalización. Monte los volúmenes exportados con comandos similares a los siguientes, con la `max_connect` opción:

```
mount <lif1_ip>:<volume_name> </mount_path1> -o vers=4.1,max_connect=16
```

```
mount <lif2_ip>:<volume_name> </mount_path2> -o vers=4.1,max_connect=16
```

(`vers`El valor `version ) debe ser `4.1` o posterior.

El `max_connect` valor corresponde al número de conexiones del grupo de troncalización.

Requisitos del cliente de VMware

Se necesita una sentencia mount que incluya una dirección IP para cada conexión del grupo de enlaces.

Monte el almacén de datos exportado con un comando similar al siguiente:

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

```
`-H`Los valores deben corresponder a las conexiones del grupo de
troncalización.
```

Gestione NFS a través de RDMA

Obtenga información sobre NFS sobre RDMA en ONTAP

NFS a través de RDMA utiliza adaptadores de red compatibles con RDMA, lo que permite copiar los datos directamente entre la memoria del sistema de almacenamiento y la memoria del sistema host, evitando así las interrupciones y los gastos generales de la CPU.

Las configuraciones de NFS sobre RDMA están diseñadas para clientes con cargas de trabajo sensibles a la latencia o de gran ancho de banda, como el aprendizaje automático y el análisis. NFS de ONTAP sobre RDMA puede utilizarse para cualquier carga de trabajo basada en NFS. Además, NVIDIA ha ampliado NFS a RDMA para permitir el almacenamiento directo GPU (GDS). GDS acelera aún más las cargas de trabajo habilitadas para GPU al omitir completamente la CPU y la memoria principal, mediante RDMA, que transfiere datos entre el sistema de almacenamiento y la memoria de la GPU directamente.

A partir de ONTAP 9.10.1, las configuraciones de NFS over RDMA son compatibles con el protocolo NFSv4,0. Las versiones posteriores de ONTAP introdujeron compatibilidad con versiones adicionales de NFS.

Requisitos

- Asegúrese de ejecutar la versión correcta de ONTAP para la versión de NFS que desea utilizar.

Versión de NFS	Soporte de ONTAP
NFSv4.0	ONTAP 9.10.1 y versiones posteriores
NFSv4.1	ONTAP 9.14.1 y versiones posteriores
NFSv3	ONTAP 9.15.1 y versiones posteriores

  - Es posible configurar NFS a través de RDMA con System Manager que empieza con ONTAP 9.12.1. En ONTAP 9.10.1 y 9.11.1, tiene que utilizar la CLI para configurar NFS sobre RDMA.
- Los dos nodos de la pareja de alta disponibilidad deben tener la misma versión.
- Las controladoras de los sistemas de almacenamiento deben admitir RDMA:

Iniciando con ONTAP…	Las siguientes controladoras admiten RDMA…
9.10.1 y posterior	• AFF A400 • AFF A700 • AFF A800
ONTAP 9.14.1 y versiones posteriores	• AFF C-Series • AFF A900
ONTAP 9.15.1 y versiones posteriores	• AFF A1K • AFF A90 • AFF A70
ONTAP 9.16.1 y versiones posteriores	• AFF A50 • AFF A30 • AFF A20

- Deben configurarse los LIF de datos para que sean compatibles con RDMA.
- Para obtener información sobre el soporte RNIC de destino, consulte la "NetApp Hardware Universe".
- Para obtener información sobre los sistemas operativos cliente compatibles para NFS a través de RDMA, consulte "Matriz de interoperabilidad de NetApp (IMT)" el . Para obtener información sobre las RNIC compatibles con RoCE v2, consulte la documentación del proveedor de RNIC correspondiente.

Los grupos de interfaces no son compatibles con NFS sobre RDMA.

Siguientes pasos

- Configure las NIC para NFS a través de RDMA
- Configure LIF para NFS a través de RDMA
- Configuración de NFS para NFS sobre RDMA

Información relacionada

- "RDMA"
- Descripción general de trunking NFS
- "RFC 7530: Protocolo NFS versión 4"
- "RFC 8166: Transporte de acceso directo a memoria remota para llamada de procedimiento remoto versión 1"
- "RFC 8167: Llamada de procedimiento remoto bidireccional en transpuertos RPC a través de RDMA"
- "RFC 8267: Enlace de capa superior de NFS a RPC-over-RDMA versión 1"

Configure las NIC para NFS a través de RDMA

NFS a través de RDMA requiere la configuración de NIC tanto para el sistema cliente como para la plataforma de almacenamiento.

Configuración de la plataforma de almacenamiento

Para obtener información sobre el soporte RNIC de destino, consulte la "NetApp Hardware Universe".

Si se utiliza una configuración de alta disponibilidad (HA), ambos nodos deben usar la misma RNIC para admitir conmutación al nodo de respaldo RDMA. La NIC debe ser compatible con RoCE.

- A partir de ONTAP 9.10.1, es posible ver una lista de protocolos de descarga RDMA con el comando:

  ```
  network port show -rdma-protocols roce
  ```

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

- A partir de ONTAP 9.16.1, se recomienda utilizar el control de flujo de prioridad (PFC). Configure PFC con `network port modify` el comando:

  ```
  network port modify -node <nodename> -port <portname> -flowcontrol-admin
  pfc -pfc-queues-admin 3
  ```

- Antes de ONTAP 9.16.1, se recomienda utilizar el control de flujo global (GFC) predeterminado. Si se ha cambiado el ajuste de control de flujo, configure GFC con el `network port modify` comando:

```
network port modify -node <nodename> -port <portname> -flowcontrol-admin
full
```

Obtenga más información sobre `network port modify` en el "Referencia de comandos del ONTAP".

Configuración del sistema cliente

Para obtener información sobre los sistemas operativos cliente compatibles para NFS a través de RDMA, consulte "Matriz de interoperabilidad de NetApp (IMT)" el . Para obtener información sobre las RNIC compatibles con RoCE v2, consulte la documentación del proveedor de RNIC correspondiente.

Aunque el cliente y el servidor pueden conectarse directamente, se recomienda el uso de switches para mejorar el rendimiento de la conmutación por error.

El cliente, el servidor, los switches y todos los puertos de los switches deben configurarse con tramas gigantes. La configuración de control de flujo en los clientes y switches debe coincidir con la configuración de control de flujo de ONTAP. A partir de ONTAP 9.16.1, se recomienda habilitar y configurar el control de flujo de prioridad en ONTAP, los switches y los clientes. Antes de ONTAP 9.16.1, se recomienda utilizar el control de flujo global.

Después de confirmar esta configuración, puede montar la exportación NFS con RDMA.

System Manager

Debe utilizar ONTAP 9.12.1 o una versión posterior para configurar interfaces de red con NFS a través de RDMA mediante System Manager.

Pasos

1. Compruebe si es compatible con RDMA. Vaya a **Red > puertos Ethernet** y seleccione el nodo apropiado en la vista de grupo. Al expandir el nodo, observe el campo **Protocolos RDMA** para un puerto determinado: El valor **RoCE** indica que RDMA es compatible; un guión (**-**) indica que no es compatible.
2. Para agregar una VLAN, seleccione **+ VLAN**. Seleccione el nodo que corresponda. En el menú desplegable **Puerto**, los puertos disponibles muestran el texto **RoCE habilitado** si son compatibles con RDMA. No se muestra texto si no admiten RDMA.
3. Siga el flujo de trabajo en Almacenamiento NAS para servidores Linux mediante NFS para configurar un nuevo servidor NFS.

   Al agregar interfaces de red, tendrá la opción de seleccionar **utilizar puertos roce**. Seleccione esta opción para las interfaces de red que desee utilizar NFS a través de RDMA.

CLI

1. Compruebe si el acceso RDMA está habilitado en el servidor NFS con el comando:

   ```
   vserver nfs show-vserver <SVM_name>
   ```

   De forma predeterminada, `-rdma` debe estar activado. Si no lo está, habilite el acceso RDMA en el servidor NFS:

   ```
   vserver nfs modify -vserver <SVM_name> -rdma enabled
   ```

2. Monte el cliente a través de NFSv4.0 por RDMA:
   a. La entrada del parámetro proto depende de la versión del protocolo IP del servidor. Si es IPv4, utilice `proto=rdma`. Si es IPv6, utilice `proto=rdma6`.
   b. Especifique el puerto de destino NFS como `port=20049` en lugar del puerto estándar 2049:

   ```
   mount -o vers=4,minorversion=0,proto=rdma,port=20049
   <Server_IP_address>:/<volume_path> <mount_point>
   ```

3. **OPCIONAL**: Si necesita desmontar el cliente, ejecute el comando `unmount <mount_path>`

Más información

- Crear servidores NFS de ONTAP
- Almacenamiento NAS para servidores Linux mediante NFS

Configure LIF para NFS a través de RDMA

Para utilizar NFS a través de RDMA, debe configurar las LIF (interfaz de red) para que sean compatibles con RDMA. Tanto el LIF como su pareja de conmutación por error deben ser compatibles con RDMA.

Cree una nueva LIF

System Manager

Debe estar ejecutando ONTAP 9.12.1 o posterior para crear una interfaz de red para NFS a través de RDMA con System Manager.

Pasos

1. Seleccione **Red > Descripción general > interfaces de red**.
2. Seleccione + Add .
3. Cuando selecciona **NFS,SMB/CIFS,S3**, tiene la opción de **usar puertos RoCE**. Seleccione la casilla de verificación **usar puertos roce**.
4. Seleccione la máquina virtual de almacenamiento y el nodo principal. Asigne un **Nombre**, **Dirección IP** y **Máscara de subred**.
5. Una vez introducida la dirección IP y la máscara de subred, System Manager filtra la lista de dominios de retransmisión a los que tienen puertos compatibles con RoCE. Seleccione un dominio de retransmisión. Opcionalmente, puede añadir una puerta de enlace.
6. Seleccione **Guardar**.

CLI

Pasos

1. Cree una LIF:

```
network interface create -vserver SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```

   - La política de servicio debe ser los archivos de datos predeterminados o una política personalizada que incluya el servicio de interfaz de red data-nfs.
   - El `-rdma-protocols` parámetro acepta una lista, que está vacía por defecto. Cuando `roce` se añade como valor, el LIF solo se puede configurar en puertos que admitan la descarga de RoCE, lo que afecta a la migración LIF de bot y al fallo.

Modificar una LIF

System Manager

Debe estar ejecutando ONTAP 9.12.1 o posterior para crear una interfaz de red para NFS a través de RDMA con System Manager.

Pasos

1. Seleccione **Red > Descripción general > interfaces de red**.
2. Seleccione ⋮ **> Editar** junto a la interfaz de red que desea cambiar.
3. Seleccione **usar puertos roce** para activar NFS sobre RDMA o anule la selección de la casilla para desactivarla. Si la interfaz de red se encuentra en un puerto con capacidad para roce, aparecerá una casilla de verificación junto a **usar puertos roce**.
4. Modifique los demás ajustes según sea necesario.
5. Seleccione **Guardar** para confirmar los cambios.

CLI

1. Puede comprobar el estado de sus LIF con `network interface show` el comando. La política de servicio debe incluir el servicio de interfaz de red data-nfs. La `-rdma-protocols` lista debe incluir `roce`. Si alguna de estas condiciones no es verdadera, modifique la LIF.

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

2. Para modificar la LIF, ejecute:

   ```
   network interface modify vserver SVM_name -lif lif_name -service-policy
   service_policy_name -home-node node_name -home-port port_name {-address
   IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
   -policy policy_name -auto-revert {true|false} -rdma-protocols roce
   ```

   Obtenga más información sobre `network interface modify` en el "Referencia de comandos del ONTAP".

> ⓘ Modificar una LIF para requerir un protocolo de descarga determinado cuando la LIF no está asignada actualmente a un puerto que admita ese protocolo producirá un error.

Migre una LIF

ONTAP también le permite migrar interfaces de red (LIF) para utilizar NFS a través de RDMA. Cuando realice esta migración, debe asegurarse de que el puerto de destino sea compatible con roce. A partir de ONTAP 9.12.1, puede completar este procedimiento en System Manager. Al seleccionar un puerto de destino para la interfaz de red, System Manager designará si los puertos son compatibles con roce.

Solo puede migrar un LIF a una configuración de NFS sobre RDMA si:

- Es una interfaz de red RDMA (LIF) NFS alojada en un puerto compatible con roce.
- Es una interfaz de red TCP (LIF) NFS alojada en un puerto compatible con roce.
- Es una interfaz de red TCP (LIF) de NFS alojada en un puerto no compatible con roce.

Para obtener más información sobre la migración de una interfaz de red, consulte Migre una LIF.

Información relacionada

- Cree una LIF
- Cree una LIF
- Modificar una LIF
- Migre una LIF

Modifique la configuración NFS

En la mayoría de los casos, no es necesario modificar la configuración de máquina virtual de almacenamiento con NFS habilitado para NFS sobre RDMA.

Sin embargo, si tiene que enfrentarse a problemas relacionados con chips Mellanox y la migración de LIF, debe aumentar el período de gracia de bloqueo de NFSv4. De forma predeterminada, el período de gracia se establece en 45 segundos. A partir de ONTAP 9.10.1, el período de gracia tiene un valor máximo de 180 (segundos).

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Introduzca el siguiente comando:

   ```
   vserver nfs modify -vserver SVM_name -v4-grace-seconds number_of_seconds
   ```

Para obtener más información sobre esta tarea, consulte Especifique el período de gracia de bloqueo de NFSv4 para las SVM de ONTAP.

Configure SMB con la interfaz de línea de comandos

Obtenga información sobre la configuración del bloque de mensajes del servidor con la CLI de ONTAP

Es posible usar comandos de la CLI de ONTAP 9 para configurar el acceso del cliente SMB a los archivos ubicados en un volumen o un qtree nuevos de una SVM nueva o existente.

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

Use estos procedimientos si desea configurar el acceso de SMB a un volumen o qtree de la siguiente forma:

- Desea utilizar SMB versión 2 o posterior.
- Desea ofrecer servicio únicamente a clientes SMB, no a clientes NFS (no a configuración multiprotocolo).
- Se utilizarán permisos de archivo NTFS para proteger el nuevo volumen.
- Tiene privilegios de administrador de clúster, no de administrador de SVM.

Se necesitan privilegios de administrador de clúster para crear SVM y LIF. Los privilegios de administrador de SVM son suficientes para otras tareas de configuración de SMB.

- Desea utilizar la CLI, no System Manager ni una herramienta de secuencias de comandos automatizadas.

  Para utilizar System Manager para configurar el acceso multiprotocolo NAS, consulte "Aprovisione almacenamiento NAS para Windows y Linux usando NFS y SMB".

- Quiere utilizar las prácticas recomendadas, no explorar todas las opciones disponibles.

  Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

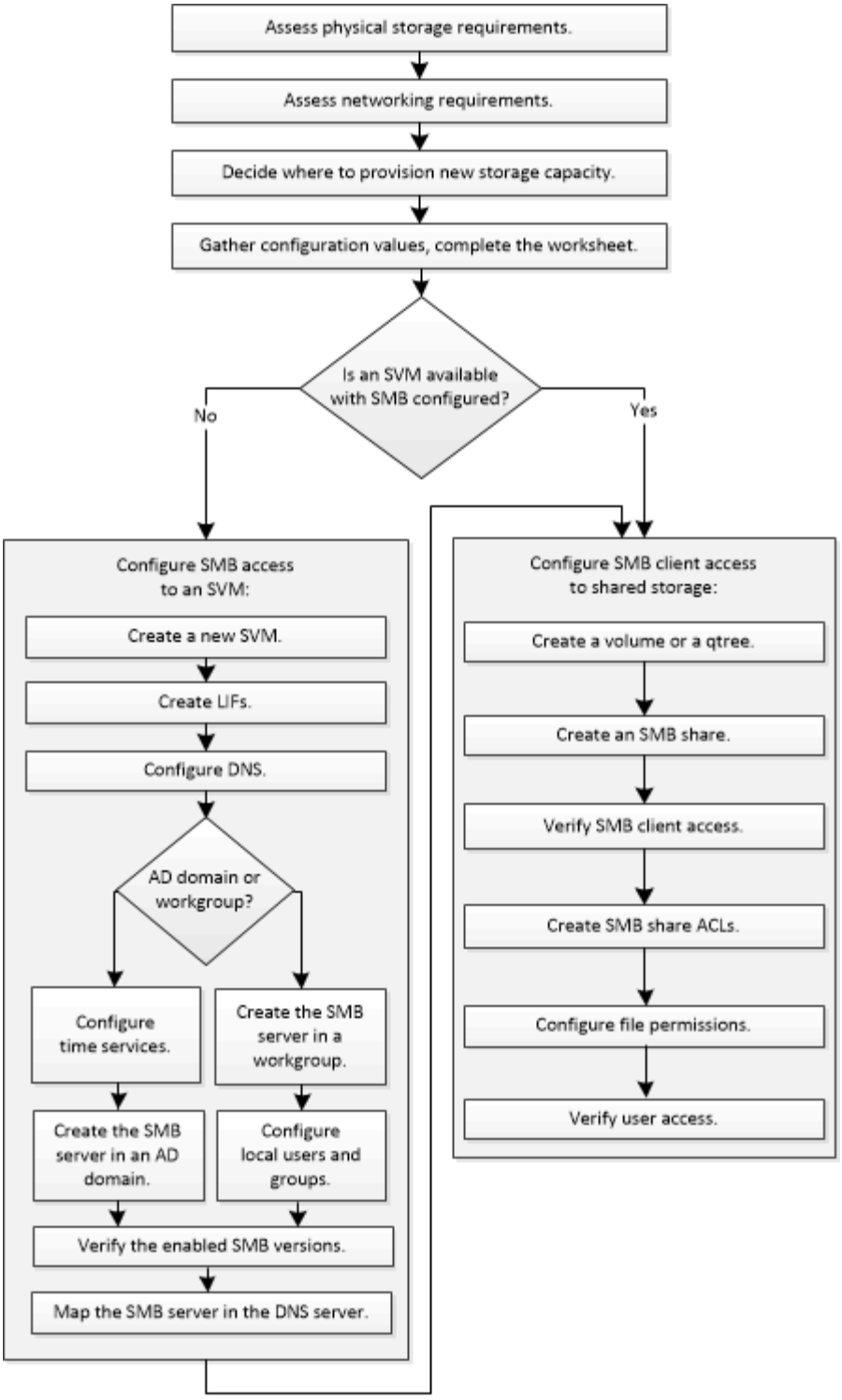
Si desea obtener más información sobre la gama de capacidades del protocolo SMB de ONTAP, consulte la "Información general de referencia de SMB".

Otras maneras de hacerlo en ONTAP

Para ejecutar estas tareas con…	Consulte…
System Manager rediseñado (disponible con ONTAP 9.7 y versiones posteriores)	"Aprovisionar almacenamiento NAS para servidores de Windows mediante SMB"
System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores)	"Información general de la configuración DE SMB"

Flujo de trabajo de configuración de SMB de ONTAP

La configuración de SMB implica evaluar los requisitos de almacenamiento físico y de red y, a continuación, elegir un flujo de trabajo específico del objetivo; configurar el acceso de SMB a una SVM nueva o existente; o añadir un volumen o qtree a una SVM existente que ya esté completamente configurada para el acceso del bloque de mensajes del servidor.



Preparación

Evalúe los requisitos de almacenamiento físico para pymes de ONTAP

Antes de aprovisionar almacenamiento de SMB para clientes, debe asegurarse de que haya espacio suficiente en un agregado existente para el nuevo volumen. Si no lo hay, puede añadir discos a un agregado existente o crear uno nuevo con el tipo deseado.

Pasos

1. Mostrar espacio disponible en los agregados existentes: `storage aggregate show`

   Si hay un agregado con suficiente espacio, registre su nombre en la hoja de cálculo.

```
cluster::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                        normal
aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                        normal
6 entries were displayed.
```

2. Si no hay agregados con espacio suficiente, añada discos a un agregado existente mediante `storage aggregate add-disks` el comando o cree un agregado nuevo mediante el `storage aggregate create` comando.

Información relacionada

- "agregado de almacenamiento, agregar discos"
- "creación de agregados de almacenamiento"

Evalúe los requisitos de red del bloque de mensajes del servidor de ONTAP

Antes de proporcionar almacenamiento SMB a los clientes, debe comprobar que las redes se han configurado correctamente para cumplir los requisitos de aprovisionamiento de SMB.

Antes de empezar

Deben configurarse los siguientes objetos de red de clúster:

- Puertos físicos y lógicos
- Dominios de retransmisión
- Subredes (si es necesario)
- Espacios IP (según se requiera, además del espacio IP predeterminado)
- Grupos de conmutación por error (según sea necesario, además del grupo de conmutación por error predeterminado para cada dominio de retransmisión).
- Firewalls externos

Pasos

1. Muestra los puertos físicos y virtuales disponibles: `network port show`

   - Cuando sea posible, debe utilizar el puerto con la velocidad más alta para la red de datos.
   - Todos los componentes de la red de datos deben tener la misma configuración de MTU para obtener el mejor rendimiento.

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

2. Si tiene pensado utilizar un nombre de subred para asignar la dirección IP y el valor de máscara de red para una LIF, compruebe que la subred exista y que tenga suficientes direcciones disponibles: `network subnet show`

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

   Las subredes contienen un grupo de direcciones IP que pertenecen a la misma subred de capa 3. Las subredes se crean con `network subnet create` el comando.

   Obtenga más información sobre `network subnet create` en el "Referencia de comandos del ONTAP".

3. Mostrar espacios IP disponibles: `network ipspace show`

   Puede usar el espacio IP predeterminado o un espacio IP personalizado.

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

4. Si desea usar direcciones IPv6, compruebe que IPv6 esté habilitado en el clúster: `network options ipv6 show`

   Si es necesario, puede habilitar IPv6 con `network options ipv6 modify` el comando.

   Obtenga más información sobre `network options ipv6 show` y `network options ipv6 modify` en el "Referencia de comandos del ONTAP".

Obtenga más información sobre ONTAP el aprovisionamiento de capacidad de almacenamiento en el bloque de mensajes del servidor

Antes de crear un volumen o qtree de SMB nuevo, debe decidir si colocarlo en una SVM nueva o existente y cuánta configuración requiere la SVM. Esta decisión determina su flujo de trabajo.

Opciones

- Si desea aprovisionar un volumen o qtree en una SVM nueva o en una SVM existente con SMB habilitado pero sin configurar, complete los pasos de «"Configuración del acceso de SMB a una SVM" y «"adición de capacidad de almacenamiento a una SVM habilitada para SMB"».

  Configurar el acceso de SMB a una SVM

  Configurar el acceso de clientes SMB a almacenamiento compartido

  Puede optar por crear una nueva SVM si se cumple alguna de las siguientes condiciones:

- Debe habilitar SMB en un clúster por primera vez.
- Tiene SVM existentes en un clúster en el cual no desea habilitar la compatibilidad con SMB.
- Tiene una o varias SVM habilitadas para SMB en un clúster y desea una de las siguientes conexiones:
  - A un bosque o grupo de trabajo de Active Directory diferente.
  - A un servidor SMB en un espacio de nombres aislado (escenario de multi-tenancy). También debe elegir esta opción para aprovisionar almacenamiento en una SVM existente con SMB habilitado pero sin configurar. Este puede ser el caso si se creó la SVM para el acceso SAN o si no se habilitó ningún protocolo cuando se creó la SVM.

Después de habilitar SMB en la SVM, continúe aprovisionando un volumen o un qtree.

- Si desea aprovisionar un volumen o qtree en una SVM existente que esté completamente configurada para el acceso SMB, complete los pasos del apartado «"adición de capacidad de almacenamiento a una SVM habilitada para SMB».

  Configurar el acceso de clientes SMB a almacenamiento compartido

Hoja de datos de configuración de SMB de ONTAP

La hoja de datos de configuración de SMB permite recopilar la información necesaria para configurar el acceso SMB para clientes.

Debe rellenar una o ambas secciones de la hoja de datos, en función de la decisión que haya tomado sobre dónde aprovisionar almacenamiento:

- Si va a configurar el acceso SMB a una SVM, debe completar ambas secciones.

  Configurar el acceso de SMB a una SVM

  Configurar el acceso de clientes SMB a almacenamiento compartido

- Si va a añadir capacidad de almacenamiento a una SVM habilitada para SMB, solo debe completar la segunda sección.

  Configurar el acceso de clientes SMB a almacenamiento compartido

Obtenga más información sobre los parámetros en el "Referencia de comandos del ONTAP".

Configurar el acceso de SMB a una SVM

Parámetros para crear una SVM

Debe proporcionar estos valores con `vserver create` el comando si va a crear una SVM nueva. Obtenga más información sobre `vserver create` en el "Referencia de comandos del ONTAP".

Campo	Descripción	Su valor
`-vserver`	Un nombre que se proporciona para la SVM nueva que es un nombre de dominio completo (FQDN) o sigue otra convención que aplica nombres de SVM únicos en un clúster.	
`-aggregate`	El nombre de un agregado en el clúster con espacio suficiente para la nueva capacidad de almacenamiento de SMB.	
`-rootvolume`	Un nombre único que se proporciona para el volumen raíz de SVM.	
`-rootvolume-security-style`	Utilice el estilo de seguridad NTFS para la SVM.	`ntfs`
`-language`	Utilice la configuración de idioma predeterminada en este flujo de trabajo.	`C.UTF-8`
`ipspace`	Opcional: Los espacios IP son espacios de direcciones IP distintos en los que residen las SVM.	

Parámetros para crear una LIF

Proporcione estos valores con `network interface create` el comando cuando cree las LIF. Obtenga más información sobre `network interface create` en el "Referencia de comandos del ONTAP".

Campo	Descripción	Su valor
`-lif`	Nombre que se proporciona para la nueva LIF.	
`-role`	Utilice el rol de LIF de datos en este flujo de trabajo.	`data`
`-data-protocol`	Utilice solo el protocolo SMB en este flujo de trabajo.	`cifs`

Campo	Descripción	Su valor
`-home-node`	El nodo al que devuelve la LIF cuando `network interface revert` se ejecuta el comando en la LIF. Obtenga más información sobre `network interface revert` en el "Referencia de comandos del ONTAP".	
`-home-port`	El puerto o grupo de interfaces al que devuelve la LIF cuando `network interface revert` se ejecuta el comando en la LIF.	
`-address`	La dirección IPv4 o IPv6 del clúster que se usará para el acceso a los datos mediante la nueva LIF.	
`-netmask`	La máscara de red y la puerta de enlace para la LIF.	
`-subnet`	Un conjunto de direcciones IP. Se utiliza en lugar de `-address` y `-netmask` para asignar direcciones y máscaras de red automáticamente.	
`-firewall-policy`	Utilice la política de firewall de datos predeterminada en este flujo de trabajo.	`data`
`-auto-revert`	Opcional: Especifica si un LIF de datos se revierte automáticamente a su nodo principal en el inicio o bajo otras circunstancias. El valor predeterminado es `false`.	

Parámetros para la resolución del nombre de host DNS

Proporcione estos valores con `vserver services name-service dns create` el comando cuando configura DNS. Obtenga más información sobre `vserver services name-service dns create` en el "Referencia de comandos del ONTAP".

Campo	Descripción	Su valor
`-domains`	Hasta cinco nombres de dominio DNS.	

Campo	Descripción	Su valor
`-name-servers`	Hasta tres direcciones IP para cada servidor de nombres DNS.	

Configuración de un servidor SMB en un dominio de Active Directory

Parámetros para la configuración del servicio de tiempo

Estos valores se proporcionan con el `cluster time-service ntp server create` comando cuando se configuran los servicios de hora. Obtenga más información sobre `cluster time-service ntp server create` en el "Referencia de comandos del ONTAP".

Campo	Descripción	Su valor
`-server`	El nombre de host o la dirección IP del servidor NTP para el dominio de Active Directory.	

Parámetros para crear un servidor SMB en un dominio de Active Directory

Debe proporcionar estos valores con el `vserver cifs create` comando al crear un nuevo servidor SMB y especificar la información del dominio. Obtenga más información sobre `vserver cifs create` en el "Referencia de comandos del ONTAP".

Campo	Descripción	Su valor
`-vserver`	Nombre de la SVM en la que se creará el servidor SMB.	
`-cifs-server`	El nombre del servidor SMB (hasta 15 caracteres).	
`-domain`	El nombre de dominio completo (FQDN) del dominio de Active Directory para asociarlo con el servidor SMB.	
`-ou`	Opcional: La unidad organizativa del dominio de Active Directory que se asocia con el servidor SMB. De forma predeterminada, este parámetro se establece en CN=Computers.	
`-netbios-aliases`	Opcional: Lista de alias NetBIOS, que son nombres alternativos al nombre del servidor SMB.	

Campo	Descripción	Su valor
`-comment`	Opcional: Comentario de texto para el servidor. Los clientes de Windows pueden ver esta descripción del servidor SMB al explorar servidores en la red.	

Configuración de un servidor SMB en un grupo de trabajo

Parámetros para crear un servidor SMB en un grupo de trabajo

Debe proporcionar estos valores con el `vserver cifs create` comando al crear un nuevo servidor SMB y especificar versiones SMB compatibles. Obtenga más información sobre `vserver cifs create` en el "Referencia de comandos del ONTAP".

Campo	Descripción	Su valor
`-vserver`	Nombre de la SVM en la que se creará el servidor SMB.	
`-cifs-server`	El nombre del servidor SMB (hasta 15 caracteres).	
`-workgroup`	El nombre del grupo de trabajo (hasta 15 caracteres).	
`-comment`	Opcional: Comentario de texto para el servidor. Los clientes de Windows pueden ver esta descripción del servidor SMB al explorar servidores en la red.	

Parámetros para crear usuarios locales

Estos valores se proporcionan cuando se crean usuarios locales con el `vserver cifs users-and-groups local-user create` comando. Son necesarios para los servidores SMB en grupos de trabajo y opcionales en dominios AD. Obtenga más información sobre `vserver cifs users-and-groups local-user create` en el "Referencia de comandos del ONTAP".

Campo	Descripción	Su valor
`-vserver`	El nombre de la SVM en la que se creará el usuario local.	
`-user-name`	El nombre del usuario local (hasta 20 caracteres).	

Campo	Descripción	Su valor
`-full-name`	Optional: Nombre completo del usuario. Si el nombre completo contiene un espacio, escriba el nombre completo entre comillas dobles.	
`-description`	Optional: Una descripción para el usuario local. Si la descripción contiene un espacio, el parámetro debe escribirse entre comillas.	
`-is-account-disabled`	Opcional: Especifica si la cuenta de usuario está habilitada o deshabilitada. Si no se especifica este parámetro, el valor predeterminado es habilitar la cuenta de usuario.	

Parámetros para crear grupos locales

Estos valores se proporcionan al crear grupos locales mediante el `vserver cifs users-and-groups local-group create` comando. Son opcionales para servidores SMB en dominios AD y grupos de trabajo. Obtenga más información sobre `vserver cifs users-and-groups local-group create` en el "Referencia de comandos del ONTAP".

Campo	Descripción	Su valor
`-vserver`	Nombre de la SVM en la que se creará el grupo local.	
`-group-name`	El nombre del grupo local (hasta 256 caracteres).	
`-description`	Opcional: Descripción del grupo local. Si la descripción contiene un espacio, el parámetro debe escribirse entre comillas.	

Se añade capacidad de almacenamiento a una SVM habilitada para SMB

Parámetros para crear un volumen

Debe introducir estos valores con `volume create` el comando si va a crear un volumen en lugar de un qtree. Obtenga más información sobre `volume create` en el "Referencia de comandos del ONTAP".

Campo	Descripción	Su valor
`-vserver`	El nombre de una SVM nueva o existente que alojará el nuevo volumen.	
`-volume`	Se suministra un nombre descriptivo único para el volumen nuevo.	
`-aggregate`	El nombre de un agregado en el clúster de con espacio suficiente para el nuevo volumen de SMB.	
`-size`	Se proporciona un entero para el tamaño del nuevo volumen.	
`-security-style`	Utilice el estilo de seguridad NTFS para este flujo de trabajo.	`ntfs`
`-junction-path`	Ubicación bajo la raíz (/) donde se va a montar el nuevo volumen.	

Parámetros para crear un qtree

Debe proporcionar estos valores con `volume qtree create` el comando si va a crear un qtree en lugar de un volumen. Obtenga más información sobre `volume qtree create` en el "Referencia de comandos del ONTAP".

Campo	Descripción	Su valor
`-vserver`	El nombre de la SVM en la que reside el volumen que contiene el qtree.	
`-volume`	El nombre del volumen que contendrá el nuevo qtree.	
`-qtree`	Nombre descriptivo único que se proporciona para el nuevo qtree, con 64 caracteres o menos.	
`-qtree-path`	El argumento de la ruta de qtree en el formato `/vol/volume_name/qtree_name\>` se puede especificar en lugar de especificar el volumen y el qtree como argumentos independientes.	

Parámetros para crear recursos compartidos SMB

Proporcione estos valores con el `vserver cifs share create` comando. Obtenga más información sobre `vserver cifs share create` en el "Referencia de comandos del ONTAP".

Campo	Descripción	Su valor
`-vserver`	Nombre de la SVM en la que se creará el recurso compartido de SMB.	
`-share-name`	El nombre del recurso compartido de SMB que se desea crear (hasta 256 caracteres).	
`-path`	El nombre de la ruta al recurso compartido de SMB (hasta 256 caracteres). Esta ruta debe existir en un volumen antes de crear el recurso compartido.	
`-share-properties`	Opcional: Una lista de propiedades de recursos compartidos. Los valores predeterminados son `oplocks`, , `browsable changenotify` y `show-previous-versions`.	
`-comment`	Optional: Comentario de texto para el servidor (hasta 256 caracteres). Los clientes de Windows pueden ver esta descripción del recurso compartido de SMB al navegar por la red.	

Parámetros para crear listas de control de acceso de recursos compartidos SMB (ACL)

Proporcione estos valores con el `vserver cifs share access-control create` comando. Obtenga más información sobre `vserver cifs share access-control create` en el "Referencia de comandos del ONTAP".

Campo	Descripción	Su valor
`-vserver`	Nombre de la SVM en la que se creará la ACL de SMB.	
`-share`	Nombre del recurso compartido de SMB en el que se va a crear.	

Campo	Descripción	Su valor
`-user-group-type`	El tipo del usuario o grupo que se añadirá a la ACL del recurso compartido. El tipo predeterminado es `windows`	`windows`
`-user-or-group`	El usuario o grupo que se añadirá a la ACL del recurso compartido. Si especifica el nombre de usuario, debe incluir el dominio del usuario con el formato "dain\username".	
`-permission`	Especifica los permisos para el usuario o grupo.	`[No_access
Read	Change	Full_Control]`

Configure el acceso de SMB a una SVM

Configure el acceso de SMB a las SVM de ONTAP

Si todavía no tiene una SVM configurada para el acceso de cliente de SMB, debe crear y configurar una SVM nueva o configurar una SVM existente. La configuración de SMB implica abrir el acceso a volumen raíz de SVM, crear un servidor SMB, crear una LIF, habilitar la resolución de nombres de host, configurar servicios de nombres y, si lo desea, Habilitar la seguridad Kerberos.

Cree SVM de ONTAP para proporcionar acceso a datos de SMB

Si no tiene al menos una SVM en un clúster para proporcionar acceso a los datos a los clientes de SMB, debe crear una.

Antes de empezar

- A partir de ONTAP 9.13.1, puede establecer una capacidad máxima para una máquina virtual de almacenamiento. También puede configurar alertas cuando la SVM se acerca a un nivel de umbral de capacidad. Para obtener más información, consulte Gestionar la capacidad de SVM.

Pasos

1. Cree una SVM: `vserver create -vserver *svm_name* -rootvolume *root_volume_name* -aggregate *aggregate_name* -rootvolume-security-style ntfs -language C.UTF-8 -ipspace *ipspace_name*`
   - Utilice la configuración NTFS para la `-rootvolume-security-style` opción.
   - Utilice `-language` la opción predeterminada C.UTF-8.
   - `ipspace`El ajuste es opcional.
2. Compruebe la configuración y el estado de la SVM recién creada: `vserver show -vserver *vserver_name*`

El `Allowed Protocols` campo debe incluir CIFS. Puede editar esta lista más tarde.

```
`Vserver Operational State`El campo debe mostrar `running` el estado. Si
muestra `initializing` el estado, significa que se produjo un error en
alguna operación intermedia como la creación del volumen raíz, y debe
eliminar la SVM y volver a crearla.
```

Ejemplos

El siguiente comando crea una SVM para el acceso de los datos en el espacio IP `ipspaceA`:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

El siguiente comando muestra que una SVM se creó con un volumen raíz de 1 GB, y se inició automáticamente y está `running` en estado. El volumen raíz tiene una política de exportación predeterminada que no incluye reglas, por lo que el volumen raíz no se exporta tras la creación.

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                                Vserver Type: data
                             Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: ntfs
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                                Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                         Vserver Admin State: running
                   Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                           Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                        Disallowed Protocols: -
                            QoS Policy Group: -
                                 Config Lock: false
                                IPspace Name: ipspaceA
```

A partir de ONTAP 9.13.1, puede establecer una plantilla de grupo de políticas de calidad de servicio adaptativa, aplicando un límite máximo y mínimo de rendimiento a los volúmenes en la SVM. Solo puede aplicar esta política después de crear la SVM. Para obtener más información sobre este proceso, consulte Defina una plantilla de grupo de políticas adaptativas.

Compruebe que el protocolo SMB esté habilitado en la SVM de ONTAP

Antes de poder configurar y utilizar SMB en las SVM, debe comprobar que el protocolo esté habilitado.

Acerca de esta tarea

Esto suele realizarse durante la configuración de la SVM, pero si no habilitó el protocolo durante la configuración, puede habilitarlo más adelante mediante `vserver add-protocols` el comando.

Una vez creado, no puede agregar ni quitar un protocolo de una LIF.

También puede deshabilitar los protocolos en las SVM con `vserver remove-protocols` el comando.

Pasos

1. Compruebe qué protocolos están habilitados y deshabilitados en la SVM: `vserver show -vserver`

`vserver_name -protocols`

También puede utilizar el `vserver show-protocols` comando para ver los protocolos habilitados actualmente en todas las SVM del clúster.

2. Si es necesario, habilite o deshabilite un protocolo:
   - Para habilitar el protocolo SMB: `vserver add-protocols -vserver vserver_name -protocols cifs`
   - Para desactivar un protocolo: `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`
3. Confirme que los protocolos activados y desactivados se han actualizado correctamente: `vserver show -vserver vserver_name -protocols`

Ejemplo

El siguiente comando muestra qué protocolos están habilitados y deshabilitados actualmente (permitidos y deshabilitados) en la SVM llamada vs1:

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ---------------------     ----------------------
vs1.example.com   cifs                       nfs, fcp, iscsi, ndmp
```

El siguiente comando permite el acceso a través de SMB agregando `cifs` a la lista de protocolos habilitados en la SVM llamada VS1:

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

Abra la política de exportación SMB del volumen raíz de la SVM de ONTAP

La política de exportación predeterminada del volumen raíz de la SVM debe incluir una regla para permitir que todos los clientes tengan acceso abierto a través de SMB. Sin esta regla, se deniega el acceso a la SVM y a sus volúmenes a todos los clientes SMB.

Acerca de esta tarea

Cuando se crea una SVM nueva, se crea automáticamente una política de exportación predeterminada (denominada predeterminada) para el volumen raíz de la SVM. Debe crear una o varias reglas para la política de exportación predeterminada para que los clientes puedan acceder a los datos de la SVM.

Debe verificar que todo el acceso a SMB esté abierto en la política de exportación predeterminada y, más adelante, restringir el acceso a volúmenes individuales mediante la creación de políticas de exportación personalizadas para volúmenes o qtrees individuales.

Pasos

1. Si utiliza una SVM existente, compruebe la política de exportación de volumen raíz predeterminada: `vserver export-policy rule show`

   El resultado del comando debe ser similar a lo siguiente:

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                    Vserver: vs1.example.com
                                Policy Name: default
                                 Rule Index: 1
                            Access Protocol: cifs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                             RO Access Rule: any
                             RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                   Superuser Security Types: any
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

Si existe una regla de este tipo que permite el acceso abierto, esta tarea se completa. De lo contrario, continúe con el siguiente paso.

2. Cree una regla de exportación para el volumen raíz de la SVM: `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. Verifique la creación de reglas con el `vserver export-policy rule show` comando.

Resultados

Ahora, cualquier cliente de SMB puede acceder a cualquier volumen o qtree creado en la SVM.

Cree LIF SMB de ONTAP

Una LIF es una dirección IP asociada con un puerto físico o lógico. Si hay un fallo de un componente, un LIF puede conmutar al respaldo o migrarse a un puerto físico diferente, lo que continúa comunicándose con la red.

Antes de empezar

- El puerto de red físico o lógico subyacente debe haberse configurado en el `up` estado administrativo. Obtenga más información sobre `up` en el "Referencia de comandos del ONTAP".
- Si tiene pensado utilizar un nombre de subred para asignar la dirección IP y el valor de máscara de red para una LIF, la subred ya debe existir.

  Las subredes contienen un grupo de direcciones IP que pertenecen a la misma subred de capa 3. Se crean mediante el `network subnet create` comando.

  Obtenga más información sobre `network subnet create` en el "Referencia de comandos del ONTAP".

- El mecanismo para especificar el tipo de tráfico que maneja una LIF ha cambiado. Para ONTAP 9.5 y versiones anteriores, LIF usaba funciones para especificar el tipo de tráfico que gestionaría. A partir de ONTAP 9.6, los LIF utilizan políticas de servicio para especificar el tipo de tráfico que manejaría.

Acerca de esta tarea

- Puede crear tanto LIF IPv4 como IPv6 en el mismo puerto de red.
- Si tiene un gran número de LIF en su clúster, puede comprobar la capacidad de LIF compatible en el clúster mediante `network interface capacity show` el comando y la capacidad de LIF admitida en cada nodo mediante el comando `network interface capacity details show` (en el nivel de privilegio avanzado).

  Obtenga más información sobre `network interface` en el "Referencia de comandos del ONTAP".

- A partir de ONTAP 9.7, si ya existen otras LIF para la SVM en la misma subred, no es necesario especificar el puerto de inicio de la LIF. ONTAP elige automáticamente un puerto aleatorio en el nodo raíz especificado en el mismo dominio de retransmisión que las otras LIF ya configuradas en la misma subred.

Pasos

1. Cree una LIF:

   `network interface create -vserver vserver_name -lif lif_name -role data -data -protocol cifs -home-node node_name -home-port port_name {-address IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto -revert {true|false}`

ONTAP 9.5 y anteriores
`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol cifs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true
false}`

ONTAP 9.6 y posterior
`network interface create -vserver *vserver_name* -lif *lif_name* -service-policy *service_policy_name* -home -node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true
false}`

   - `-role`No es necesario utilizar el parámetro cuando se crea una LIF mediante una política de servicio (empezando por ONTAP 9.6).
   - `-data-protocol`No es necesario utilizar el parámetro cuando se crea una LIF mediante una política de servicio (empezando por ONTAP 9.6). Cuando se utiliza ONTAP 9 E.5 y versiones anteriores, el `-data-protocol` parámetro se debe especificar al crear la LIF, y no se puede modificar más adelante sin destruir ni volver a crear la LIF de datos.
   - `-home-node` Es el nodo al que devuelve la LIF cuando `network interface revert` se ejecuta el comando en la LIF.

     También puede especificar si el LIF debe volver automáticamente al nodo de inicio y al puerto de inicio con `-auto-revert` la opción.

   - `-home-port` Es el puerto físico o lógico al que devuelve la LIF cuando `network interface`

`revert` el comando se ejecuta en la LIF.

- Puede especificar una dirección IP con las `-address -netmask` opciones y, o bien habilitar la asignación desde una subred con `-subnet_name` la opción.
- Al usar una subred para suministrar la dirección IP y la máscara de red, si la subred se definió con una puerta de enlace, se añadirá automáticamente a la SVM una ruta predeterminada a esa puerta de enlace cuando se cree una LIF con dicha subred.
- Si asigna direcciones IP manualmente (sin una subred), es posible que deba configurar una ruta predeterminada para una puerta de enlace si hay clientes o controladores de dominio en una subred IP diferente. Obtenga más información sobre `network route create` y cómo crear una ruta estática dentro de una SVM en el "Referencia de comandos del ONTAP".
- Para `-firewall-policy` la opción, utilice el mismo valor predeterminado `data` que el rol LIF.

  Si lo desea, puede crear y agregar una política de firewall personalizada más adelante.

  > A partir de ONTAP 9.10.1, las políticas de firewall están obsoletas y sustituidas por completo por políticas de servicios LIF. Para obtener más información, consulte "Configurar políticas de firewall para LIF".

- `-auto-revert` Permite especificar si una LIF de datos se revierte automáticamente a su nodo de inicio en circunstancias como el inicio, los cambios en el estado de la base de datos de gestión o el momento en que se establece la conexión de red. El valor por defecto es `false`, pero puede definirlo en `false` función de las políticas de gestión de red del entorno.

2. Compruebe que la LIF se ha creado correctamente:

   ```
   network interface show
   ```

3. Compruebe que se pueda acceder a la dirección IP configurada:

Para verificar una…	Usar…
Dirección IPv4	`network ping`
Dirección IPv6	`network ping6`

Ejemplos

El siguiente comando crea una LIF y especifica la dirección IP y los valores de la máscara de red mediante `-address -netmask` los parámetros y:

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

El siguiente comando crea una LIF y asigna valores de dirección IP y máscara de red a partir de la subred especificada (denominada cliente1_sub):

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol cifs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

El siguiente comando muestra todas las LIF del clúster-1. Data LIF datalif1 y datalif3 están configurados con direcciones IPv4, y datalif4 está configurado con una dirección IPv6:

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

El siguiente comando muestra cómo crear una LIF de datos NAS que está asignada a la `default-data-files` política de servicio:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

Información relacionada

- "ping de red"
- "reversión de la interfaz de red"

Habilite DNS para la resolución de nombre de host en SMB de ONTAP

Puede usar `vserver services name-service dns` el comando para habilitar DNS en una SVM y configurarlo para que utilice DNS para la resolución de nombre de host. Los nombres de host se resuelven mediante servidores DNS externos. Obtenga más información sobre `vserver services name-service dns` en el "Referencia de comandos del ONTAP".

Antes de empezar

Un servidor DNS para todo el sitio debe estar disponible para las búsquedas de nombre de host.

Debe configurar más de un servidor DNS para evitar un único punto de error. El `vserver services name-service dns create` comando emite una advertencia si se introduce solo un nombre de servidor DNS. Obtenga más información sobre `vserver services name-service dns create` en el "Referencia de comandos del ONTAP".

Acerca de esta tarea

Más información sobre "Configuración de DNS dinámico en la SVM".

Pasos

1. Habilite DNS en la SVM: `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

   El siguiente comando habilita los servidores DNS externos en la SVM vs1:

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   > El `vserver services name-service dns create` comando realiza una validación automática de la configuración y informa un mensaje de error si ONTAP no puede contactar con el servidor de nombres.

2. Muestra la configuración del dominio DNS mediante `vserver services name-service dns show` el comando.

   El siguiente comando muestra las configuraciones de DNS de todas las SVM del clúster:

```
vserver services name-service dns show
                                                 Name
Vserver           State     Domains              Servers
----------------- --------- -------------------- -------------
cluster1          enabled   example.com          192.0.2.201,
                                                 192.0.2.202
vs1.example.com   enabled   example.com          192.0.2.201,
                                                 192.0.2.202
```

El siguiente comando muestra información detallada de la configuración de DNS para SVM vs1:

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
         Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. Valide el estado de los servidores de nombres mediante `vserver services name-service dns check` el comando.

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

Configurar un servidor SMB en un dominio de Active Directory

Configure los servicios de tiempo de ONTAP para servidores SMB

Antes de crear un servidor SMB en una controladora de Active Domain, debe asegurarse de que la hora y la hora del clúster de los controladores de dominio al que pertenecerá el servidor SMB coincidan con en un plazo de cinco minutos.

Acerca de esta tarea

Debe configurar los servicios NTP del clúster para utilizar los mismos servidores NTP para la sincronización que utiliza el dominio de Active Directory.

A partir de ONTAP 9.5, puede configurar el servidor NTP con autenticación simétrica.

Pasos

1. Configure los servicios de hora mediante `cluster time-service ntp server create` el comando.
   - Para configurar los servicios de hora sin autenticación simétrica, introduzca el siguiente comando: `cluster time-service ntp server create -server server_ip_address`
   - Para configurar los servicios de hora con autenticación simétrica, introduzca el siguiente comando: `cluster time-service ntp server create -server server_ip_address -key-id key_id`
     `cluster time-service ntp server create -server 10.10.10.1 cluster time-service ntp server create -server 10.10.10.2`
2. Verifique que los servicios de hora están configurados correctamente mediante `cluster time-service ntp server show` el comando.

   `cluster time-service ntp server show`

```
Server                          Version
------------------------------ -------
10.10.10.1                      auto
10.10.10.2                      auto
```

Información relacionada

- "ntp de servicio horario del clúster"

Comandos de ONTAP para gestionar la autenticación simétrica en servidores NTP

A partir de ONTAP 9.5, se admite la versión 3 del protocolo de tiempo de redes (NTP). NTPv3 incluye autenticación simétrica mediante claves SHA-1 que aumenta la seguridad de la red.

Para hacer esto…	Se usa este comando…
Configure un servidor NTP sin autenticación simétrica	`cluster time-service ntp server create -server server_name`
Configure un servidor NTP con autenticación simétrica	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
Habilitar autenticación simétrica para un servidor NTP existente se puede modificar el servidor NTP existente para habilitar la autenticación agregando el Id. De clave requerido	`cluster time-service ntp server modify -server server_name -key-id key_id`

Para hacer esto…	Se usa este comando…
Configure una clave NTP compartida	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` Las claves compartidas se refieren a un ID. El ID, su tipo y el valor deben ser idénticos tanto en el nodo como en el servidor NTP
Configure un servidor NTP con un ID de clave desconocido	`cluster time-service ntp server create -server server_name -key-id key_id`
Configure un servidor con un ID de clave no configurado en el servidor NTP.	`cluster time-service ntp server create -server server_name -key-id key_id` El ID de clave, el tipo y el valor deben ser idénticos al ID de clave, el tipo y el valor configurados en el servidor NTP.
Deshabilitar la autenticación simétrica	`cluster time-service ntp server modify -server server_name -authentication disabled`

Información relacionada

- "ntp de servicio horario del clúster"

Cree servidores SMB en un dominio de ONTAP Active Directory

Puede usar `vserver cifs create` el comando para crear un servidor SMB en la SVM y especificar el dominio de Active Directory (AD) al que pertenece.

Antes de empezar

Las SVM y los LIF que utiliza para servir datos deben haberse configurado para permitir el protocolo SMB. Las LIF deben poder conectarse a los servidores DNS configurados en la SVM y a un controlador de dominio AD del dominio al que desea unirse al servidor SMB.

Cualquier usuario con autorización para crear cuentas de máquina en el dominio de AD al que se va a unir el servidor SMB puede crear el servidor SMB en la SVM. Esto puede incluir usuarios de otros dominios.

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.

Acerca de esta tarea

Al crear un servidor SMB en un dominio de directorio de actividades:

- Debe usar el nombre de dominio completo (FQDN) al especificar el dominio.

- La configuración predeterminada es agregar la cuenta de máquina del servidor SMB al objeto CN=Computer de Active Directory.
- Puede optar por agregar el servidor SMB a una unidad organizativa (OU) diferente mediante la `-ou` opción.
- Opcionalmente, puede elegir agregar una lista delimitada por comas de uno o más alias NetBIOS (hasta 200) para 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 originales.

Obtenga más información acerca de `vserver cifs` los parámetros opcionales y los requisitos de nomenclatura en el "Referencia de comandos del ONTAP".

A partir de ONTAP 9.8, puede especificar que se cifren las conexiones a los controladores de dominio. ONTAP requiere cifrado para las comunicaciones del controlador de dominio cuando la `-encryption-required -for-dc-connection` opción está establecida en `true`; El valor por defecto 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. .

"Gestión de SMB" Contiene más información sobre las opciones de configuración del servidor SMB.

Pasos

1. Compruebe que SMB tiene licencia en el clúster: `system license show -package cifs`

   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.

   No se requiere una licencia de CIFS si el servidor SMB se usará solo para autenticación.

2. Cree el servidor SMB en un dominio de AD: `vserver cifs create -vserver vserver_name -cifs-server smb_server_name -domain FQDN [-ou organizational_unit][-netbios-aliases NetBIOS_name, ...][-keytab-uri {(ftp|http)://hostname|IP_address}][-comment text]`

   Al unirse a un dominio, este comando puede tardar varios minutos en completarse.

   El siguiente comando crea el servidor SMB «s' mb_server01» en el dominio "'example.com`":

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   smb_server01 -domain example.com
   ```

   El siguiente comando crea el servidor SMB «smemoria_servidor 2» en el dominio «mydomain.com`" y autentica al administrador ONTAP con un archivo keytab:

   ```
   cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
   smb_server02 -domain mydomain.com -keytab-uri
   http://admin.mydomain.com/ontap1.keytab
   ```

3. Verifique la configuración del servidor SMB mediante `vserver cifs show` el comando.

   En este ejemplo, el resultado del comando muestra que se creó en SVM vs1.example.com un servidor SMB denominado "MB_SERVER01", que se unió al dominio "'example.com`".

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

                                          Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    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: -
```

4. Si lo desea, habilite la comunicación cifrada con el controlador de dominio (ONTAP 9, 8 y posterior): `vserver cifs security modify -vserver svm_name -encryption-required-for-dc -connection true`

Ejemplos

El siguiente comando crea un servidor SMB denominado «mb_server02» en la SVM vs2.example.com en el dominio «'example.com`". La cuenta de equipo se crea en el contenedor "'OU=eng,OU=corp,DC=example,DC=com"'. Al servidor SMB se le asigna un alias NetBIOS.

```
cluster1::> vserver cifs create -vserver vs2.example.com –cifs-server
smb_server02 -domain example.com –ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1
                                        Vserver: vs2.example.com
                      CIFS Server NetBIOS Name: SMB_SERVER02
                  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: OLD_CIFS_SERVER01
```

El siguiente comando permite a un usuario de un dominio diferente, en este caso un administrador de un dominio de confianza, crear un servidor SMB denominado «smemoria_servidor03» en la SVM vs3.example.com. `-domain`La opción especifica el nombre del dominio raíz (especificado en la configuración DNS) en el que desea crear el servidor SMB. `username`La opción especifica el administrador del dominio de confianza.

- Dominio principal: example.com
- Dominio de confianza: trust.lab.com
- Nombre de usuario del dominio de confianza: Administrador1

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com

Username: Administrator1@trust.lab.com
Password: . . .
```

Cree archivos keytab para la autenticación SMB de ONTAP

A partir de ONTAP 9.7, ONTAP admite la autenticación de SVM con servidores Active Directory (AD) mediante archivos keytab. Los administradores DE AD generan un archivo keytab y lo ponen a disposición de los administradores de ONTAP como un identificador de recursos uniforme (URI), que se proporciona cuando `vserver cifs` los comandos requieren la autenticación Kerberos con el dominio AD.

Los administradores DE AD pueden crear los archivos keytab utilizando `ktpass` el comando estándar de Windows Server. El comando debe ejecutarse en el dominio principal donde la autenticación es necesaria. El `ktpass` comando se puede utilizar para generar archivos keytab solo para usuarios de dominio primario; las claves generadas con usuarios de dominio de confianza no son compatibles.

Los archivos keytab se generan para usuarios específicos de administrador de ONTAP. Siempre que la contraseña del usuario administrador no cambie, las claves generadas para el tipo de cifrado específico y el dominio no cambiarán. Por lo tanto, se requiere un nuevo archivo keytab cada vez que se cambia la contraseña del usuario admin.

Se admiten los siguientes tipos de cifrado:

- AES256-SHA1
- DES-CBC-MD5

  ⓘ ONTAP no admite el tipo de cifrado DES-CBC-CRC.

- RC4-HMAC

AES256 es el tipo de cifrado más alto y se debe utilizar si está activado en el sistema ONTAP.

Los archivos keytab se pueden generar especificando la contraseña de administrador o mediante una contraseña generada aleatoriamente. Sin embargo, en cualquier momento sólo se puede utilizar una opción de contraseña, ya que en el servidor AD se necesita una clave privada específica para el usuario administrador para descifrar las claves del archivo keytab. Cualquier cambio en la clave privada de un administrador específico anulará el archivo keytab.

Configurar un servidor SMB en un grupo de trabajo

Obtenga información sobre la configuración del servidor SMB en grupos de trabajo de ONTAP

La configuración de un servidor SMB como miembro de un grupo de trabajo consiste en crear el servidor SMB y, a continuación, crear usuarios y grupos locales.

Puede configurar un servidor SMB en un grupo de trabajo cuando la infraestructura de dominio de Microsoft Active Directory no está disponible.

Un servidor SMB en modo de grupo de trabajo sólo admite autenticación NTLM y no admite autenticación Kerberos.

Cree servidores SMB en la SVM de ONTAP con grupos de trabajo especificados

Puede usar `vserver cifs create` el comando para crear un servidor SMB en la SVM y especificar el grupo de trabajo al que pertenece.

Antes de empezar

Las SVM y los LIF que utiliza para servir datos deben haberse configurado para permitir el protocolo SMB. Los LIF deben poder conectarse con los servidores DNS que estén configurados en la SVM.

Acerca de esta tarea

Los servidores SMB en modo de grupo de trabajo no admiten las siguientes funciones de SMB:

- Protocolo de testimonio de SMB3
- Recursos compartidos de CA de SMB3
- SQL sobre SMB
- Redirección de carpetas
- Perfiles de roaming
- Objeto de directiva de grupo (GPO)
- Servicio Snapshot de volumen (VSS)

Obtenga más información acerca de `vserver cifs` los parámetros de configuración opcionales y los requisitos de nomenclatura en el "Referencia de comandos del ONTAP".

Pasos

1. Compruebe que SMB tiene licencia en el clúster: `system license show -package cifs`

   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.

   No se requiere una licencia de CIFS si el servidor SMB se usará solo para autenticación.

2. Cree el servidor SMB en un grupo de trabajo: `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

   El siguiente comando crea el servidor SMB «s' mb_server01» en el grupo de trabajo «'workgroup01'»:

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   SMB_SERVER01 -workgroup workgroup01
   ```

3. Verifique la configuración del servidor SMB mediante `vserver cifs show` el comando.

   En el ejemplo siguiente, el resultado del comando muestra que se creó un servidor SMB denominado «MB_server01» en SVM vs1.example.com en el grupo de trabajo «'workgroup01'»:

```
cluster1::> vserver cifs show -vserver vs0

                                          Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: workgroup01
                      Fully Qualified Domain Name: -
                              Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
                                  Workgroup Name: workgroup01
                             Authentication Style: workgroup
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

Después de terminar

Para un servidor CIFS en un grupo de trabajo, debe crear usuarios locales y, opcionalmente, grupos locales en la SVM.

Información relacionada

"Gestión de SMB"

Cree cuentas de usuario SMB de ONTAP locales

Se puede crear una cuenta de usuario local que se pueda utilizar para autorizar el acceso a los datos contenidos en la SVM a través de una conexión de SMB. También es posible usar cuentas de usuario locales para la autenticación al crear una sesión SMB.

Acerca de esta tarea

La funcionalidad de usuario local se habilita de forma predeterminada cuando se crea la SVM.

Al crear una cuenta de usuario local, debe especificar un nombre de usuario y debe especificar la SVM con la que desea asociar la cuenta.

Obtenga más información acerca de `vserver cifs users-and-groups local-user` los parámetros opcionales y los requisitos de nomenclatura en el "Referencia de comandos del ONTAP".

Pasos

1. Cree el usuario local: `vserver cifs users-and-groups local-user create -vserver` *`vserver_name`* `-user-name` *`user_name optional_parameters`*

   Los siguientes parámetros opcionales pueden ser útiles:

   - `-full-name`

Nombre completo del usuario.

- `-description`

  Una descripción para el usuario local.

- `-is-account-disabled {true|false}`

  Especifica si la cuenta de usuario está habilitada o deshabilitada. Si no se especifica este parámetro, el valor predeterminado es habilitar la cuenta de usuario.

El comando solicita la contraseña del usuario local.

2. Introduzca una contraseña para el usuario local y confirme la contraseña.
3. Compruebe que el usuario se ha creado correctamente: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Ejemplo

En el siguiente ejemplo se crea un usuario local «MMB_SERVER01\sue», con el nombre completo «Sue Chang», asociado a SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                   Full Name  Description
-------- --------------------------- ---------- -------------
vs1      SMB_SERVER01\Administrator             Built-in administrator
account
vs1      SMB_SERVER01\sue            Sue Chang
```

Cree grupos SMB de ONTAP locales

Es posible crear grupos locales que se puedan utilizar para autorizar el acceso a los datos asociados con la SVM a través de una conexión de SMB. También puede asignar privilegios que definen los derechos de usuario o las capacidades que tiene un miembro del grupo.

Acerca de esta tarea

La funcionalidad de grupo local se habilita de forma predeterminada cuando se crea la SVM.

Cuando se crea un grupo local, debe especificar un nombre para el grupo y debe especificar la SVM con la que desea asociar el grupo. Puede especificar un nombre de grupo con o sin el nombre de dominio local y, opcionalmente, puede especificar una descripción para el grupo local. No puede agregar un grupo local a otro grupo local.

Obtenga más información acerca de `vserver cifs users-and-groups local-group` los parámetros opcionales y los requisitos de nomenclatura en el "Referencia de comandos del ONTAP".

Pasos

1. Cree el grupo local: `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

   El siguiente parámetro opcional puede ser útil:

   - `-description`

     Una descripción para el grupo local.

2. Compruebe que el grupo se ha creado correctamente: `vserver cifs users-and-groups local-group show -vserver vserver_name`

Ejemplo

En el siguiente ejemplo se crea un grupo local "MB_SERVER01\engineering" asociado con SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering

cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
Vserver          Group Name                     Description
---------------- ------------------------------ ----------------------------
vs1.example.com  BUILTIN\Administrators         Built-in Administrators
group
vs1.example.com  BUILTIN\Backup Operators       Backup Operators group
vs1.example.com  BUILTIN\Power Users            Restricted administrative
privileges
vs1.example.com  BUILTIN\Users                  All users
vs1.example.com  SMB_SERVER01\engineering
vs1.example.com  SMB_SERVER01\sales
```

Después de terminar

Debe agregar miembros al nuevo grupo.

Gestionar la pertenencia a un grupo SMB de ONTAP local

Puede administrar la pertenencia a grupos locales agregando y eliminando usuarios locales o de dominio, o agregando y eliminando grupos de dominios. Esto resulta útil si desea controlar el acceso a los datos basándose en los controles de acceso colocados en el grupo o si desea que los usuarios tengan privilegios asociados a ese grupo.

Acerca de esta tarea

Si ya no desea que un usuario local, un usuario de dominio o un grupo de dominio tenga derechos de acceso o privilegios basados en la pertenencia a un grupo, puede quitar el miembro del grupo.

Debe tener en cuenta lo siguiente al agregar miembros a un grupo local:

- No puede agregar usuarios al grupo especial *Everyone*.
- No puede agregar un grupo local a otro grupo local.
- Para agregar un usuario o grupo de dominio a un grupo local, ONTAP debe poder resolver el nombre a un SID.

Debe tener en cuenta lo siguiente al quitar miembros de un grupo local:

- No puede eliminar miembros del grupo especial *Everyone*.
- Para quitar un miembro de un grupo local, ONTAP debe poder resolver su nombre a un SID.

Pasos

1. Agregar o quitar un miembro de un grupo.
   - Agregar un miembro: `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     Puede especificar una lista delimitada por comas de usuarios locales, usuarios de dominio o grupos de dominio que desee agregar al grupo local especificado.
   - Eliminar un miembro: `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     Puede especificar una lista delimitada por comas de usuarios locales, usuarios de dominio o grupos de dominio que desee quitar del grupo local especificado.

Ejemplos

En el siguiente ejemplo se agrega un usuario local "MB_SERVER01\sue" al grupo local "MB_SERVER01\engineering" en la SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

En el siguiente ejemplo se eliminan los usuarios locales "MB_SERVER01\sue" y "MB_SERVER01\james" del grupo local "MB_SERVER01\engineering" en la SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Verifique las versiones de bloque de mensajes del servidor de ONTAP habilitadas

En la versión ONTAP 9, se determinan las versiones de SMB que se habilitan de forma predeterminada para las conexiones con clientes y controladoras de dominio. Debe verificar si el servidor SMB admite los clientes y la funcionalidad que requiere su entorno.

Acerca de esta tarea

Para las conexiones con clientes y controladoras de dominio, debe habilitar SMB 2.0 y una versión posterior siempre que sea posible. Por motivos de seguridad, debe evitar el uso de SMB 1.0 y debe deshabilitarlo si ha verificado que no es necesario en su entorno.

A partir de ONTAP 9.3, está deshabilitado de forma predeterminada en las nuevas SVM.

> Si `-smb1-enabled-for-dc-connections` se establece en `false` while `-smb1-enabled` está establecido en `true`, ONTAP deniega las conexiones SMB 1,0 como cliente, pero continúa aceptando las conexiones SMB 1,0 entrantes como servidor.

"Gestión de SMB" Contiene detalles sobre las versiones y la funcionalidad del SMB compatibles.

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Compruebe qué versiones de SMB están habilitadas:

```
vserver cifs options show
```

   Puede desplazarse hacia abajo por la lista para ver las versiones de SMB habilitadas para conexiones de clientes y si está configurando un servidor SMB en un dominio de AD para conexiones de dominio de AD.

3. Habilite o deshabilite el protocolo SMB para las conexiones de cliente según sea necesario:
   - Para habilitar una versión de SMB:

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
true
```

     Valores posibles para `smb_version`:

     - `-smb1-enabled`
     - `-smb2-enabled`
     - `-smb3-enabled`
     - `-smb31-enabled`

     El siguiente comando habilita SMB 3,1 en SVM vs1.example.com:

```
cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31
-enabled true
```

   - Para deshabilitar una versión de SMB:

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
false
```

4. Si el servidor SMB se encuentra en un dominio de Active Directory, habilite o deshabilite el protocolo SMB para las conexiones DC según sea necesario:
   - Para habilitar una versión de SMB:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections true
```

   - Para deshabilitar una versión de SMB:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections false
```

5. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Asigne los servidores SMB de ONTAP en el servidor DNS

El servidor DNS del sitio debe tener una entrada que apunte el nombre del servidor SMB y cualquier alias NetBIOS a la dirección IP de la LIF de datos para que los usuarios de Windows puedan asignar una unidad al nombre del servidor SMB.

Antes de empezar

Debe tener acceso administrativo al servidor DNS del sitio. Si no tiene acceso administrativo, debe solicitar al administrador DNS que realice esta tarea.

Acerca de esta tarea

Si utiliza alias NetBIOS para el nombre del servidor SMB, es una práctica recomendada crear puntos de entrada del servidor DNS para cada alias.

Pasos

1. Inicie sesión en el servidor DNS.
2. Cree entradas de búsqueda hacia delante (a - Registro de dirección) e inversa (PTR - Registro de puntero) para asignar el nombre del servidor SMB a la dirección IP de la LIF de datos.
3. Si utiliza alias NetBIOS, cree una entrada de búsqueda Alias nombre canónico (registro de recursos CNAME) para asignar cada alias a la dirección IP de la LIF de datos del servidor SMB.

Resultados

Una vez que la asignación se propaga a través de la red, los usuarios de Windows pueden asignar una unidad al nombre del servidor SMB o sus alias NetBIOS.

Configure el acceso de clientes SMB al almacenamiento compartido

Configure el acceso de cliente SMB al almacenamiento compartido de ONTAP

Para proporcionar acceso al cliente SMB al almacenamiento compartido en una SVM, debe crear un volumen o qtree para proporcionar un contenedor de almacenamiento y, a continuación, crear o modificar un recurso compartido para ese contenedor. Luego, puede configurar los permisos de recursos compartidos y archivos, y probar el acceso desde sistemas cliente.

Antes de empezar

- El bloque de mensajes del servidor debe estar configurado por completo en la SVM.
- Se debe completar cualquier actualización de la configuración de los servicios de nombres.
- Cualquier adición o modificación a una configuración de dominio o grupo de trabajo de Active Directory debe estar completa.

Cree un volumen o un contenedor de almacenamiento Qtree

Cree volúmenes de bloque de mensajes del servidor de ONTAP

Puede crear un volumen y especificar su punto de unión y otras propiedades mediante `volume create` el comando.

Acerca de esta tarea

Un volumen debe incluir una *ruta de unión* para que sus datos estén disponibles para los clientes. Puede especificar la ruta de unión cuando cree un nuevo volumen. Si crea un volumen sin especificar una ruta de unión, debe *mount* el volumen en el espacio de nombres de la SVM con `volume mount` el comando.

Antes de empezar

- SMB debe estar configurado y en ejecución.
- El estilo de seguridad de la SVM debe ser NTFS.
- A partir de ONTAP 9.13.1, se pueden crear volúmenes con análisis de capacidad y seguimiento de actividades habilitados. Para activar la capacidad o el seguimiento de actividad, ejecute el `volume create` comando con `-analytics-state` o `-activity-tracking-state` establezca en `on`.

  Para obtener más información sobre el análisis de capacidad y el seguimiento de actividades, consulte "Active File System Analytics". Obtenga más información sobre `volume create` en el "Referencia de comandos del ONTAP".

Pasos

1. Cree el volumen con un punto de unión: `volume create -vserver` *`svm_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style ntfs -junction-path` *`junction_path`*`]`

   Las opciones para `-junction-path` son las siguientes:

   - Directamente bajo raíz, por ejemplo, `/new_vol`

     Puede crear un nuevo volumen y especificar que se monte directamente en el volumen raíz de SVM.

- En un directorio existente, por ejemplo, `/existing_dir/new_vol`

  Puede crear un nuevo volumen y especificar que se monte en un volumen existente (en una jerarquía existente), expresado como un directorio.

Si desea crear un volumen en un nuevo directorio (en una jerarquía nueva en un volumen nuevo), por ejemplo, `/new_dir/new_vol`, primero debe crear un volumen primario nuevo que esté unido al volumen raíz de la SVM. A continuación, creará el nuevo volumen secundario en la ruta de unión del nuevo volumen principal (nuevo directorio).

2. Compruebe que el volumen se creó con el punto de unión deseado: `volume show -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction`

Ejemplos

El siguiente comando crea un nuevo volumen denominado user1 en la SVM vs1.example.com y el agregado aggr1. El nuevo volumen está disponible en `/users`. El tamaño del volumen es de 750 GB y su garantía de volumen es del tipo volumen (de forma predeterminada).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver           Volume   Active   Junction Path   Path Source
----------------- ------- -------- --------------- -----------
vs1.example.com   users1   true     /users          RW_volume
```

El siguiente comando crea un nuevo volumen denominado «'home4'» en la SVM»'vs1.example.com`'" y el agregado «'aggr1'». El directorio `/eng/` ya existe en el espacio de nombres para la SVM de VS1, y el nuevo volumen está disponible en `/eng/home`, que se convierte en el directorio inicial del `/eng/` espacio de nombres. El volumen tiene un tamaño de 750 GB y su garantía de volumen es de tipo `volume` (de forma predeterminada).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                          Junction                 Junction
Vserver          Volume   Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4    true     /eng/home       RW_volume
```

Cree qtrees SMB de ONTAP

Puede crear un qtree para que contenga los datos y especificar sus propiedades

mediante `volume qtree create` el comando.

Antes de empezar

- La SVM y el volumen que contendrán el nuevo qtree ya deben existir.
- El estilo de seguridad de la SVM debe ser NTFS y el SMB debe configurarse y ejecutarse.

Pasos

1. Cree el qtree: `volume qtree create -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs`

   Puede especificar el volumen y el qtree como argumentos independientes, o bien especificar el argumento de la ruta de qtree en el formato `/vol/volume_name/_qtree_name`.

2. Compruebe que el qtree se ha creado con la ruta de unión deseada: `volume qtree show -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path }`

Ejemplo

En el ejemplo siguiente se crea un qtree llamado qt01 ubicado en la SVM vs1.example.com que tiene una ruta de unión `/vol/data1`:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style ntfs
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                    Vserver Name: vs1.example.com
                     Volume Name: data1
                      Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                  Security Style: ntfs
                     Oplock Mode: enable
                Unix Permissions: ---rwxr-xr-x
                        Qtree Id: 2
                    Qtree Status: normal
                   Export Policy: default
        Is Export Policy Inherited: true
```

Requisitos y consideraciones al crear recursos compartidos SMB de ONTAP

Antes de crear un recurso compartido SMB, debe comprender los requisitos para las rutas de acceso compartidas y las propiedades compartidas, especialmente para los directorios iniciales.

La creación de un recurso compartido de SMB implica especificar una estructura de ruta de directorio

(mediante `-path` la opción del `vserver cifs share create` comando) a la que accederán los clientes. La ruta de directorio corresponde a la ruta de unión para un volumen o qtree que ha creado en el espacio de nombres de la SVM. Debe haber la ruta de directorio y la ruta de unión correspondiente antes de crear el recurso compartido.

Las rutas de recursos compartidos tienen los siguientes requisitos:

- Un nombre de ruta de acceso de directorio puede tener hasta 255 caracteres.
- Si hay un espacio en el nombre de la ruta de acceso, toda la cadena se debe poner entre comillas (por ejemplo, `"/new volume/mount here"`).
- Si la ruta UNC (`\\servername\sharename\filepath`) del recurso compartido contiene más de 256 caracteres (excluyendo el "\" inicial en la ruta UNC), entonces la pestaña **Seguridad** en el cuadro Propiedades de Windows no estará disponible.

  Se trata de un problema del cliente Windows y no de un problema de ONTAP. Para evitar este problema, no cree recursos compartidos con rutas UNC con más de 256 caracteres.

Se pueden cambiar los valores predeterminados de las propiedades compartidas:

- Las propiedades iniciales por defecto para todos los recursos compartidos son `oplocks`, , `browsable` `changenotify` y `show-previous-versions`.
- Es opcional especificar propiedades de recurso compartido al crear un recurso compartido.

  Sin embargo, si especifica propiedades de recurso compartido al crear el recurso compartido, no se utilizan los valores predeterminados. Si utiliza `-share-properties` el parámetro al crear un recurso compartido, debe especificar todas las propiedades de recurso compartido que desea aplicar al recurso compartido mediante una lista delimitada por comas.

- Para designar un recurso compartido de directorio principal, utilice la `homedirectory` propiedad.

  Esta función permite configurar un recurso compartido que se asigna a directorios diferentes en función del usuario que se conecta a él y un conjunto de variables. En lugar de tener que crear recursos compartidos independientes para cada usuario, puede configurar un solo recurso compartido con varios parámetros del directorio inicial para definir la relación de un usuario entre un punto de entrada (el recurso compartido) y su directorio inicial (un directorio en la SVM).

  No puede agregar ni quitar esta propiedad después de crear el recurso compartido.

Los recursos compartidos del directorio inicial tienen los siguientes requisitos:

- Antes de crear directorios iniciales SMB, debe añadir al menos una ruta de búsqueda del directorio inicial mediante `vserver cifs home-directory search-path add` el comando.
- Los recursos compartidos del directorio inicial especificados por el valor de `homedirectory` en el `-share-properties` parámetro deben incluir `%w` la variable dinámica (nombre de usuario de Windows) en el nombre del recurso compartido.

  El nombre del recurso compartido puede contener además la `%d` variable dinámica (nombre de dominio) (por ejemplo, `%d/%w`) o una parte estática en el nombre del recurso compartido (por ejemplo, `home1_%w`).

- Si los administradores o usuarios utilizan el recurso compartido para conectarse a los directorios principales de otros usuarios (mediante las opciones del `vserver cifs home-directory modify`

comando), el patrón de nombre de recurso compartido dinámico debe ir precedido por una tilde (~).

Obtenga más información sobre `vserver cifs share` en el "Referencia de comandos del ONTAP".

Información relacionada

- "Gestión de SMB"

Crear recursos compartidos de SMB de ONTAP

Debe crear un recurso compartido de SMB para poder compartir datos desde un servidor SMB con clientes SMB. Cuando se crea un recurso compartido, se pueden establecer propiedades de recurso compartido, como designar el recurso compartido como un directorio inicial. También puede personalizar el recurso compartido configurando ajustes opcionales.

Antes de empezar

La ruta de directorio del volumen o qtree debe existir en el espacio de nombres de la SVM antes de crear el recurso compartido.

Acerca de esta tarea

Al crear un recurso compartido, la ACL de uso compartido por defecto (permisos de uso compartido por defecto) es `Everyone / Full Control`. Después de probar el acceso al recurso compartido, debe quitar la ACL de recurso compartido predeterminada y reemplazarla por una alternativa más segura.

Pasos

1. Si es necesario, cree la estructura de ruta de acceso de directorio para el recurso compartido.

   El `vserver cifs share create` comando comprueba la ruta especificada en la `-path` opción durante la creación de recursos compartidos. Si la ruta especificada no existe, el comando falla.

2. Cree un recurso compartido de SMB asociado con la SVM especificada: `vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`
3. Compruebe que se ha creado el recurso compartido:`vserver cifs share show -share-name share_name`

Ejemplos

El siguiente comando crea un recurso compartido de SMB llamado «`share1`» en SVM `vs1.example.com`. Su ruta de acceso al directorio es `/users`, y se crea con propiedades predeterminadas.

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name
SHARE1 -path /users

cluster1::> vserver cifs share show -share-name SHARE1

Vserver          Share    Path     Properties Comment  ACL
---------------  -------- -------- ---------- -------- -----------
vs1.example.com  SHARE1   /users   oplocks    -        Everyone / Full
Control
                                   browsable
                                   changenotify
                                   show-previous-versions
```

Compruebe el acceso del cliente SMB de ONTAP

Debe verificar si ha configurado SMB correctamente accediendo y escribiendo los datos en el recurso compartido. Debe probar el acceso utilizando el nombre del servidor SMB y todos los alias NetBIOS.

Pasos

1. Inicie sesión en un cliente Windows.
2. Probar el acceso mediante el nombre del servidor SMB:

   a. En el Explorador de Windows, asigne una unidad al recurso compartido en el siguiente formato: `\\SMB_Server_Name\Share_Name`

      Si la asignación no se realiza correctamente, es posible que la asignación DNS aún no se haya propagado por toda la red. Debe probar el acceso más adelante con el nombre del servidor SMB.

      Si el servidor SMB se llama vs1.example.com y el recurso compartido se llama share1, debe introducir lo siguiente: `\\vs0.example.com\SHARE1`

   b. En la unidad recién creada, cree un archivo de prueba y, a continuación, elimine el archivo.

   Verificó el acceso de escritura al recurso compartido mediante el nombre del servidor SMB.

3. Repita el paso 2 para cualquier alias NetBIOS.

Cree listas de control de acceso compartido de SMB de ONTAP

La configuración de permisos de uso compartido mediante la creación de listas de control de acceso (ACL) para recursos compartidos de SMB permite controlar el nivel de acceso a un recurso compartido para usuarios y grupos.

Antes de empezar

Debe haber decidido qué usuarios o grupos tendrán acceso al recurso compartido.

Acerca de esta tarea

Puede configurar ACL de nivel compartido utilizando nombres de usuarios o grupos locales o de Windows de

dominio.

Antes de crear una nueva ACL, debe suprimir la ACL de recurso compartido por defecto `Everyone / Full Control` , que representa un riesgo de seguridad.

En modo de grupo de trabajo, el nombre de dominio local es el nombre del servidor SMB.

Pasos

1. Suprima la ACL de recurso compartido predeterminada:`vserver cifs share access-control delete -vserver vserver_name -share share_name -user-or-group everyone`
2. Configure la nueva ACL:

Si desea configurar las ACL utilizando…	Introduzca el comando…
Usuario de Windows	`vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\\user_name -permission access_right`
Grupo Windows	`vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_group_name -permission access_right`

3. Verifique que la ACL aplicada al recurso compartido es correcta mediante `vserver cifs share access-control show` el comando.

Ejemplo

El siguiente comando otorga `Change` permisos al grupo de Windows “Equipo de ventas” para el recurso compartido “ventas” en el “vs1.example.com`"SVM:”

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vserver cifs share access-control show
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
Permission
--------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$         BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales      DOMAIN\"Sales Team"     windows     Change
```

Los siguientes comandos dan `Change` permiso al grupo local de Windows llamado “Equipo Tigre” y `Full_Control` permiso al usuario local de Windows llamado “Sue Chang” para el recurso compartido “atavol5” en el “VS1” SVM:

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    DOMAIN\"Tiger Team"         windows     Change
vs1            datavol5    DOMAIN\"Sue Chang"          windows
Full_Control
```

Configure los permisos de archivos NTFS en recursos compartidos SMB de ONTAP

Para habilitar el acceso a archivos para los usuarios o grupos que tienen acceso a un recurso compartido, debe configurar permisos de archivos NTFS en archivos y directorios de ese recurso compartido desde un cliente de Windows.

Antes de empezar

El administrador que realiza esta tarea debe tener suficientes permisos NTFS para cambiar los permisos en los objetos seleccionados.

Acerca de esta tarea

"Gestión de SMB" Y la documentación de Windows contiene información sobre cómo establecer permisos NTFS estándar y avanzados.

Pasos

1. Inicie sesión en un cliente Windows como administrador.
2. En el menú **Herramientas** del Explorador de Windows, seleccione **asignar unidad de red**.
3. Complete el cuadro **Unidad de red de mapas**:
   a. Seleccione una letra **Unidad**.
   b. En el cuadro **Folder**, escriba el nombre del servidor SMB que contiene el recurso compartido que contiene los datos a los que desea aplicar los permisos y el nombre del recurso compartido.

Si el nombre de su servidor SMB es SMB_SERVER01 y su recurso compartido se denomina «`share1`», debe introducir `\\SMB_SERVER01\SHARE1`.

Puede especificar la dirección IP de la interfaz de datos para el servidor SMB en lugar del nombre del servidor SMB.

c. Haga clic en **Finalizar**.

La unidad seleccionada está montada y lista con la ventana del Explorador de Windows que muestra archivos y carpetas contenidos en el recurso compartido.

4. Seleccione el archivo o directorio para el que desea establecer los permisos de archivo NTFS.
5. Haga clic con el botón secundario del ratón en el archivo o directorio y seleccione **Propiedades**.
6. Seleccione la ficha **Seguridad**.

   La ficha Seguridad muestra la lista de usuarios y grupos para los que se ha establecido el permiso NTFS. El cuadro permisos para <Object> muestra una lista de los permisos permitir y denegar vigentes para el usuario o grupo seleccionado.

7. Haga clic en **Editar**.

   Se abrirá el cuadro permisos para <Object>.

8. Realice las acciones deseadas:

Si quieres	Haga lo siguiente…
Establezca permisos NTFS estándar para un nuevo usuario o grupo	a. Haga clic en **Agregar**. Se abre la ventana Seleccionar usuario, equipos, cuentas de servicio o grupos. b. En el cuadro **Introduzca los nombres de objeto para seleccionar** , escriba el nombre del usuario o grupo en el que desea agregar permiso NTFS. c. Haga clic en **OK**.
Cambiar o quitar permisos NTFS estándar de un usuario o grupo	En el cuadro **nombres de grupo o de usuario** , seleccione el usuario o grupo que desea cambiar o quitar.

9. Realice las acciones deseadas:

Si desea…	Haga lo siguiente
Establezca permisos NTFS estándar para un usuario o grupo nuevo o existente	En el cuadro **permisos para <Object>** , seleccione los cuadros **permitir** o **Denegar** para el tipo de acceso que desea permitir o no permitir para el usuario o grupo seleccionado.

Si desea…	Haga lo siguiente
Quitar un usuario o un grupo	Haga clic en **Quitar**.

Si algunos o todos los cuadros de permiso estándar no se pueden seleccionar, es porque los permisos se heredan del objeto primario. El cuadro **permisos especiales** no se puede seleccionar. Si está seleccionada, significa que se han establecido uno o más derechos avanzados granulares para el usuario o grupo seleccionado.

10. Después de terminar de agregar, quitar o editar permisos NTFS en ese objeto, haga clic en **Aceptar**.

Compruebe el acceso al recurso compartido del usuario SMB de ONTAP

Debe probar que los usuarios configurados pueden acceder al recurso compartido de SMB y a los archivos que contiene.

Pasos

1. En un cliente Windows, inicie sesión como uno de los usuarios que ahora tiene acceso al recurso compartido.
2. En el menú **Herramientas** del Explorador de Windows, seleccione **asignar unidad de red**.
3. Complete el cuadro **Unidad de red de mapas**:
   a. Seleccione una letra **Unidad**.
   b. En el cuadro **carpeta**, escriba el nombre del recurso compartido que proporcionará a los usuarios.

      Si el nombre de su servidor SMB es SMB_SERVER01 y su recurso compartido se denomina «`share1`», debe introducir `\\SMB_SERVER01\share1`.

   c. Haga clic en **Finalizar**.

   La unidad seleccionada está montada y lista con la ventana del Explorador de Windows que muestra archivos y carpetas contenidos en el recurso compartido.
4. Cree un archivo de prueba, compruebe que existe, escriba texto y quite el archivo de prueba.

Gestione SMB con la interfaz de línea de comandos

Obtenga más información sobre SMB de ONTAP

Las funciones de acceso a archivos ONTAP están disponibles para el protocolo SMB. Puede habilitar un servidor CIFS, crear recursos compartidos y habilitar servicios de Microsoft.

SMB (bloque de mensajes del servidor) hace referencia a los dialectos modernos del protocolo del sistema común de archivos de Internet (CIFS). Seguirá viendo *CIFS* en la interfaz de línea de comandos (CLI) de ONTAP y en las herramientas de gestión de OnCommand.

Compatibilidad con servidores SMB

Obtenga más información sobre la compatibilidad con servidores SMB de ONTAP

Puede habilitar y configurar servidores SMB en máquinas virtuales de almacenamiento (SVM) para permitir que los clientes SMB accedan a los archivos del clúster.

- Cada SVM de datos del clúster puede vincularse a exactamente un dominio de Active Directory.
- No es necesario enlazar las SVM de datos con el mismo dominio.
- Pueden vincularse varias SVM al mismo dominio.

Debe configurar las SVM y las LIF que utiliza para proporcionar datos antes de poder crear un servidor SMB. Si la red de datos no es plano, también podría necesitar configurar espacios IP, dominios de retransmisión y subredes.

Información relacionada

"Gestión de redes"

Modificar servidores

"Administración del sistema"

Versiones y funcionalidades de SMB de ONTAP admitidas

Server Message Block (SMB) es un protocolo de uso compartido de archivos remoto que utilizan los servidores y clientes de Microsoft Windows. Todas las versiones de SMB son compatibles. Debe verificar que el servidor SMB de ONTAP admite los clientes y la funcionalidad que se requieren en su entorno.

La información más reciente sobre los clientes SMB y los controladores de dominio compatibles con ONTAP está disponible en *Interoperability Matrix Tool*.

SMB 2,0 y las versiones posteriores se habilitan de forma predeterminada para los servidores SMB de ONTAP, y se pueden habilitar o deshabilitar según sea necesario. SMB 1,0 puede habilitarse o deshabilitarse según sea necesario.

> La configuración predeterminada de las conexiones SMB 1.0 y 2.0 con controladoras de dominio también depende de la versión ONTAP. Obtenga más información sobre `vserver cifs security modify` en el "Referencia de comandos del ONTAP". En el caso de entornos con servidores CIFS existentes que ejecuten SMB 1.0, debe migrar a una versión Lo antes posible. de SMB posterior con el fin de prepararse para las mejoras de seguridad y cumplimiento de normativas. Si quiere más información, póngase en contacto con su representante de NetApp.

La siguiente tabla muestra qué funciones de SMB son compatibles con cada versión de SMB. Algunas funciones de SMB se habilitan de forma predeterminada, por lo que algunas requieren más configuración.

Esta funcionalidad:	Requiere activación:	Es compatible con ONTAP 9 para estas versiones SMB:	
		3,0	3.1.1
Funcionalidad SMB 1.0 heredada		X	X
Asas duraderas		X	X
Operaciones compuestas		X	X
Operaciones asíncronas		X	X
Se han aumentado los tamaños de búfer de lectura y escritura		X	X
Mayor escalabilidad		X	X
Firma SMB	X	X	X
Formato de archivo de flujo de datos alternativo (ADS)	X	X	X
MTU grande (habilitada de forma predeterminada a partir de ONTAP 9.7)	X	X	X
Bloqueos oportunistas del arrendamiento		X	X
Recursos compartidos disponibles en todo momento	X	X	X
Asas persistentes		X	X
Testigo		X	X
CIFRADO SMB: AES-128-CCM	X	X	X

Esta funcionalidad:	Requiere activación:	Es compatible con ONTAP 9 para estas versiones SMB:	
Escalado horizontal (necesario por los recursos compartidos de CA)		X	X
Recuperación transparente tras fallas		X	X
Multicanal de SMB (a partir de ONTAP 9.4)	X	X	X
Integridad de la preautenticación			X
Recuperación tras fallos de cliente de clúster v.2 (CCFv2)			X
CIFRADO SMB: AES-128-GCM	X		X

Información relacionada

Aprenda a utilizar la firma ONTAP para mejorar la seguridad de la red

Establecer el nivel mínimo de seguridad de autenticación del servidor

Configurar el cifrado SMB necesario en servidores SMB para las transferencias de datos a través de SMB

"Interoperabilidad de NetApp"

Funciones de Windows no admitidas en SMB de ONTAP

Antes de utilizar CIFS en la red, debe tener en cuenta determinadas funciones de Windows que ONTAP no admite.

ONTAP no admite las siguientes funciones de Windows:

- Sistema de archivos cifrados (EFS)
- Registro de eventos del sistema de archivos NT (NTFS) en el diario de cambios
- Servicio de replicación de archivos de Microsoft (FRS)
- Servicio de Index Server de Microsoft Windows
- Almacenamiento remoto a través de la gestión de almacenamiento jerárquico (HSM)
- Gestión de cuotas desde clientes Windows
- Semántica de cuotas de Windows
- El archivo LMHOSTS

- Compresión nativa de NTFS

Configure los servicios de nombres NIS o LDAP en las SVM SMB de ONTAP

Con el acceso SMB, se siempre se realiza la asignación de usuario a un usuario UNIX, incluso al acceder a los datos de un volumen de estilo de seguridad NTFS. Si asigna usuarios de Windows a los usuarios UNIX correspondientes cuya información se almacena en almacenes de directorios NIS o LDAP, o si utiliza LDAP para la asignación de nombres, deberá configurar estos servicios de nombres durante la instalación de SMB.

Antes de empezar

Debe haber personalizado la configuración de la base de datos de servicios de nombres para que coincida con su infraestructura de servicios de nombres.

Acerca de esta tarea

Las SVM utilizan las bases de datos ns-switch de servicios de nombres para determinar el orden en el que buscar los orígenes de una base de datos de servicios de nombres determinada. El origen ns-switch puede ser cualquier combinación de `files` , , `nis` o `ldap`. En la base de datos de grupos, ONTAP intenta obtener las pertenencias a grupos de todos los orígenes configurados y, a continuación, utiliza la información consolidada de pertenencia a grupos para las comprobaciones de acceso. Si uno de estos orígenes no está disponible en el momento de obtener información del grupo UNIX, ONTAP no puede obtener las credenciales de UNIX completas y las comprobaciones de acceso posteriores podrían fallar. Por lo tanto, siempre debe comprobar que todas las fuentes del conmutador ns están configuradas para la base de datos de grupo en la configuración del conmutador ns.

El valor predeterminado es que el servidor SMB asigne todos los usuarios de Windows al usuario UNIX predeterminado que se almacena en la `passwd` base de datos local. Si desea utilizar la configuración predeterminada, es opcional configurar los servicios de nombre de usuario y grupo de UNIX NIS o LDAP, o la asignación de usuario LDAP para el acceso a SMB.

Pasos

1. Si la información de usuario, grupo y netgroup de UNIX es administrada por servicios de nombres NIS, configure los servicios de nombres NIS:

   a. Determine el orden actual de los servicios de nombres mediante el `vserver services name-service ns-switch show` comando.

      En este ejemplo, las tres bases de datos (`group`, `passwd` y `netgroup`) que se pueden utilizar `nis` como origen de servicio de nombres sólo se utilizan `files` como origen.

      ```
      vserver services name-service ns-switch show -vserver vs1
      ```

```
                                                          Source
Vserver         Database       Enabled         Order
--------------- ------------   ---------       ---------
vs1             hosts          true            dns,
                                                files
vs1             group          true            files
vs1             passwd         true            files
vs1             netgroup       true            files
vs1             namemap        true            files
```

Debe añadir el `nis` origen a `group` `passwd` las bases de datos y, opcionalmente, a la `netgroup` base de datos.

b. Ajuste el orden de la base de datos ns-switch del servicio de nombres como desee mediante el `vserver services name-service ns-switch modify` comando.

Para obtener el mejor rendimiento, no debe agregar un servicio de nombres a una base de datos del servicio de nombres a menos que planifique configurar ese servicio de nombres en la SVM.

Si modifica la configuración de más de una base de datos de servicio de nombres, debe ejecutar el comando por separado para cada base de datos de servicio de nombres que desee modificar.

En este ejemplo, `nis` y `files` se configuran como orígenes para las `group` `passwd` bases de datos y, en ese orden. El resto de las bases de datos de servicios de nombres no han cambiado.

```
vserver services name-service ns-switch modify -vserver vs1 -database group
-sources nis,files vserver services name-service ns-switch modify -vserver
vs1 -database passwd -sources nis,files
```

c. Compruebe que el orden de los servicios de nombres es correcto mediante el `vserver services name-service ns-switch show` comando.

```
vserver services name-service ns-switch show -vserver vs1
```

```
                                                          Source
Vserver         Database       Enabled         Order
--------------- ------------   ---------       ---------
vs1             hosts          true            dns,
                                                files
vs1             group          true            nis,
                                                files
vs1             passwd         true            nis,
                                                files
vs1             netgroup       true            files
vs1             namemap        true            files
```

d. Cree la configuración del servicio de nombres NIS:

```
vserver services name-service nis-domain create -vserver <vserver_name>
-domain <NIS_domain_name> -servers <NIS_server_IPaddress>,…

vserver services name-service nis-domain create -vserver vs1 -domain
example.com -servers 10.0.0.60
```

de host o una dirección IP para el servidor NIS.

e. Compruebe que el servicio de nombres NIS está configurado correctamente: `vserver services name-service nis-domain show vserver <vserver_name>`

```
vserver services name-service nis-domain show vserver vs1
```

```
Vserver       Domain              Server
------------- ------------------- ---------------
vs1           example.com         10.0.0.60
```

2. Si los servicios de nombres LDAP gestionan la información de usuarios, grupos y grupos de red de UNIX o la asignación de nombres, configure los servicios de nombres LDAP mediante la información ubicada "Gestión de NFS".

Obtenga más información sobre la configuración del switch del servicio de nombres SMB de ONTAP

ONTAP almacena la información de configuración del servicio de nombres en una tabla que es el equivalente al `/etc/nsswitch.conf` archivo en sistemas UNIX. Debe comprender la función de la tabla y cómo la utiliza ONTAP para poder configurarla de forma adecuada para su entorno.

La tabla de conmutador de servicio de nombres ONTAP determina qué orígenes de servicio de nombres consulta ONTAP para recuperar información de un determinado tipo de información del servicio de nombres. ONTAP mantiene una tabla de switch de servicio de nombres independiente para cada SVM.

Tipos de base de datos

La tabla almacena una lista de servicios de nombres independiente para cada uno de los siguientes tipos de base de datos:

Tipo de base de datos	Define orígenes de servicio de nombres para…	Los orígenes válidos son…
hosts	Conversión de nombres de host a direcciones IP	archivos, dns
grupo	Búsqueda de información de grupo de usuarios	archivos, nis, ldap
passwd	Búsqueda de información de usuario	archivos, nis, ldap

Tipo de base de datos	Define orígenes de servicio de nombres para…	Los orígenes válidos son…
grupo de red	Buscando información de netgroup	archivos, nis, ldap
mapa de nombres	Asignando los nombres de usuario	archivos, ldap

Tipos de origen

Los orígenes especifican el nombre de origen de servicio que se utilizará para recuperar la información adecuada.

Especificar tipo de origen…	Para buscar información en…	Administrado por las familias de comandos…

archivos	Archivos de origen local	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	Servidores NIS externos tal como se especifica en la configuración de dominio NIS de la SVM	`vserver services name-service nis-domain`
ldap	Servidores LDAP externos tal como se especifica en la configuración del cliente LDAP de la SVM	`vserver services name-service ldap`
dns	Servidores DNS externos como se especifica en la configuración de DNS de la SVM	`vserver services name-service dns`

Aunque tenga pensado utilizar NIS o LDAP para el acceso a los datos y la autenticación de administración de SVM, deberá incluir `files` y configurar usuarios locales como recuperación en caso de que falle la autenticación NIS o LDAP.

Protocolos utilizados para acceder a fuentes externas

Para acceder a los servidores de fuentes externas, ONTAP utiliza los siguientes protocolos:

Fuente externa del servicio de nombres	Protocolo utilizado para acceder
NIS	UDP

Fuente externa del servicio de nombres	Protocolo utilizado para acceder
DNS	UDP
LDAP	TCP

Ejemplo

En el siguiente ejemplo, se muestra la configuración del switch del servicio de nombres para la SVM `svm_1`:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                Source
Vserver         Database        Order
--------------- ------------    ---------
svm_1           hosts           files,
                                dns
svm_1           group           files
svm_1           passwd          files
svm_1           netgroup        nis,
                                files
```

Para buscar información de usuarios o grupos, ONTAP sólo consulta archivos de fuentes locales. Si la consulta no devuelve ningún resultado, la búsqueda fallará.

Para buscar información de grupos de red, ONTAP consulta primero los servidores NIS externos. Si la consulta no devuelve ningún resultado, el archivo de netgroup local se activa a continuación.

No hay entradas del servicio de nombres para la asignación de nombres en la tabla de la SVM svm svm_1. Por lo tanto, ONTAP sólo consulta archivos de origen local de forma predeterminada.

Gestione servidores SMB

Modificar los servidores SMB de ONTAP

Puede mover un servidor SMB de un grupo de trabajo a un dominio de Active Directory, de un grupo de trabajo a otro grupo de trabajo o de un dominio de Active Directory a un grupo de trabajo mediante el `vserver cifs modify` comando.

Acerca de esta tarea

También puede modificar otros atributos del servidor SMB, como el nombre del servidor SMB y el estado administrativo. Obtenga más información sobre `vserver cifs modify` en el "Referencia de comandos del ONTAP".

Opciones

- Mover el servidor SMB de un grupo de trabajo a un dominio de Active Directory:

  a. Defina el estado administrativo del servidor SMB en `down`.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

b. Mueva el servidor SMB del grupo de trabajo a un dominio de Active Directory: `vsserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`*

```
Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
```

Para crear una cuenta de máquina de Active Directory para el servidor SMB, debe proporcionar el nombre y la contraseña de una cuenta de Windows con suficiente Privileges para agregar equipos al `ou=`*`example`* `ou` contenedor dentro del *`example`* dominio .com.

A partir de ONTAP 9.7, el administrador de AD puede proporcionarle un URI a un archivo keytab como alternativa a proporcionarle un nombre y una contraseña a una cuenta de Windows con privilegios. Cuando reciba el URI, inclúyalo en el `-keytab-uri` parámetro con `vserver cifs` los comandos.

- Mover el servidor SMB de un grupo de trabajo a otro grupo de trabajo:
  a. Defina el estado administrativo del servidor SMB en `down`.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

  b. Modifique el grupo de trabajo para el servidor SMB: `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`new_workgroup_name`*

```
Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
```

- Mover el servidor SMB de un dominio de Active Directory a un grupo de trabajo:
  a. Defina el estado administrativo del servidor SMB en `down`.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

  b. Mueva el servidor SMB del dominio de Active Directory a un grupo de trabajo: `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`workgroup_name`*

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```

Para entrar en el modo de grupo de trabajo, el sistema debe desactivar todas las características basadas en dominios y eliminar su configuración automáticamente, incluidos los recursos compartidos disponibles continuamente, las instantáneas y AES. Sin embargo, las ACL de uso compartido configuradas por el dominio como "EXAMPLE.COM\userName" no funcionarán correctamente, pero ONTAP no las podrá quitar. Quite estas ACL compartidas Lo antes posible. utilizando herramientas externas una vez completado el comando. Si AES está activado, puede que se le solicite que proporcione el nombre y la contraseña de una cuenta de Windows con los privilegios suficientes para deshabilitarla en el dominio "example.com".

- Modifique otros atributos mediante el parámetro adecuado `vserver cifs modify` del comando.

Utilice opciones para personalizar los servidores SMB

Opciones disponibles para el servidor SMB de ONTAP

Resulta útil saber qué opciones hay disponibles cuando se piensa en cómo personalizar el servidor SMB. Aunque algunas opciones se utilizan para uso general en el servidor SMB, se utilizan varias para habilitar y configurar una funcionalidad SMB específica. Las opciones del servidor SMB se controlan con `vserver cifs options modify` la opción.

En la lista siguiente se especifican las opciones del servidor SMB que están disponibles en el nivel de privilegios de administrador:

- **Configuración del valor de tiempo de espera de la sesión SMB**

  La configuración de esta opción permite especificar el número de segundos de tiempo de inactividad antes de desconectar una sesión SMB. Una sesión inactiva es una sesión en la que un usuario no tiene archivos o directorios abiertos en el cliente. El valor predeterminado es 900 segundos.

- **Configuración del usuario UNIX predeterminado**

  La configuración de esta opción le permite especificar el usuario UNIX predeterminado que utiliza el servidor SMB. ONTAP crea automáticamente un usuario predeterminado denominado «'pcuser'» (con un UID de 65534), crea un grupo denominado «'pcuser'» (con un GID de 65534) y agrega el usuario predeterminado al grupo «'pcuser'». Cuando se crea un servidor SMB, ONTAP configura automáticamente «'pcuser'» como el usuario UNIX predeterminado.

- **Configuración del usuario UNIX invitado**

  Al configurar esta opción, puede especificar el nombre de un usuario UNIX al que se asignan los usuarios que inician sesión desde dominios que no son de confianza, lo que permite a un usuario de un dominio que no es de confianza conectarse con el servidor SMB. De forma predeterminada, esta opción no está configurada (no hay ningún valor predeterminado); por lo tanto, el valor predeterminado es no permitir que los usuarios de dominios que no son de confianza se conecten con el servidor SMB.

- **Activación o desactivación de la ejecución de Read GRANT para bits de modo**

  Habilitar o deshabilitar esta opción permite especificar si se permite a los clientes SMB ejecutar archivos ejecutables con bits de modo UNIX a los que tienen acceso de lectura, incluso cuando el bit ejecutable de UNIX no está establecido. Esta opción está deshabilitada de forma predeterminada.

- **Activación o desactivación de la capacidad de eliminar archivos de sólo lectura de clientes NFS**

  Al habilitar o deshabilitar esta opción, se determina si se permite que los clientes NFS eliminen archivos o carpetas con el conjunto de atributos de sólo lectura. La semántica de eliminación NTFS no permite la eliminación de un archivo o carpeta cuando se establece el atributo de sólo lectura. La semántica de eliminación de UNIX ignora el bit de sólo lectura, utilizando los permisos de directorio principal en su lugar para determinar si un archivo o una carpeta se pueden eliminar. La configuración predeterminada es `disabled`, que da como resultado una semántica de supresión NTFS.

- **Configuración de las direcciones del servidor del Servicio de nombres de Internet de Windows**

  La configuración de esta opción le permite especificar una lista de direcciones de servidor del Servicio de nombres Internet de Windows (WINS) como una lista delimitada por comas. Debe especificar direcciones IPv4. Las direcciones IPv6 no son compatibles. No hay un valor predeterminado.

En la lista siguiente se especifican las opciones del servidor SMB que están disponibles en el nivel de privilegio avanzado:

- **Concesión de permisos de grupo UNIX a usuarios de CIFS**

  La configuración de esta opción determina si el usuario CIFS entrante que no sea el propietario del archivo puede recibir el permiso de grupo. Si el usuario CIFS no es el propietario del archivo de estilo de seguridad UNIX y este parámetro se establece en `true`, se concede el permiso de grupo para el archivo. Si el usuario CIFS no es el propietario del archivo de estilo de seguridad UNIX y este parámetro se establece en `false`, se aplican las reglas UNIX normales para otorgar el permiso al archivo. Este parámetro se aplica a los archivos de estilo de seguridad de UNIX que tienen el permiso establecido `mode bits` como y no es aplicable a los archivos con el modo de seguridad NTFS o NFSv4. El valor predeterminado es `false`.

- **Activación o desactivación de SMB 1,0**

  SMB 1.0 está deshabilitado de forma predeterminada en una SVM para la cual se crea un servidor SMB en ONTAP 9.3.

  > A partir de ONTAP 9.3, SMB 1.0 está deshabilitado de forma predeterminada para los nuevos servidores SMB creados en ONTAP 9.3. Debe migrar a una versión Lo antes posible. posterior de SMB para preparar las mejoras de seguridad y cumplimiento de normativas. Si quiere más información, póngase en contacto con su representante de NetApp.

- **Activación o desactivación de SMB 2.x**

  SMB 2.0 es la versión mínima de SMB que admite la conmutación al nodo de respaldo de LIF. Si deshabilita SMB 2.x, ONTAP también deshabilita automáticamente SMB 3.X.

  SMB 2,0 solo es compatible con las SVM. La opción está habilitada de forma predeterminada en las SVM

- **Activación o desactivación de SMB 3,0**

  SMB 3.0 es la versión mínima de SMB que admite recursos compartidos disponibles de forma continua. Windows Server 2012 y Windows 8 son las versiones mínimas de Windows que admiten SMB 3.0.

  SMB 3,0 solo es compatible con las SVM. La opción está habilitada de forma predeterminada en las SVM

- **Activación o desactivación de SMB 3,1**

  Windows 10 es la única versión de Windows que admite SMB 3.1.

  SMB 3,1 solo es compatible con las SVM. La opción está habilitada de forma predeterminada en las SVM

- **Activación o desactivación de la descarga de copias ODX**

  La descarga de copias ODX la utilizan automáticamente clientes de Windows que son compatibles con esta tecnología. Esta opción está habilitada de forma predeterminada.

- **Activación o desactivación del mecanismo de copia directa para la descarga de copias ODX**

  El mecanismo de copia directa aumenta el rendimiento de la operación de descarga de copia cuando los clientes de Windows intentan abrir el archivo de origen de una copia en un modo que impide que se cambie el archivo mientras la copia está en curso. De forma predeterminada, el mecanismo de copia directa está habilitado.

- **Activación o desactivación de referencias automáticas a nodos**

  Con las referencias automáticas a nodos, el servidor SMB hace referencia automáticamente a una LIF de datos local al nodo que aloja los datos a los que se accede a través del recurso compartido solicitado.

- **Activación o desactivación de políticas de exportación para SMB**

  Esta opción está deshabilitada de forma predeterminada.

- **Activación o desactivación mediante puntos de unión como puntos de reanálisis**

  Si esta opción está habilitada, el servidor SMB expone puntos de unión a clientes SMB como puntos de reanálisis. Esta opción solo es válida para conexiones SMB 2.x o SMB 3.0. Esta opción está habilitada de forma predeterminada.

  Esta opción solo es compatible con las SVM. La opción está habilitada de forma predeterminada en las SVM

- **Configuración del número máximo de operaciones simultáneas por conexión TCP**

  El valor predeterminado es 255.

- **Activación o desactivación de la funcionalidad de grupos y usuarios locales de Windows**

  Esta opción está habilitada de forma predeterminada.

- **Activación o desactivación de la autenticación de usuarios locales de Windows**

  Esta opción está habilitada de forma predeterminada.

- **Activación o desactivación de la función de copia de sombra VSS**

  ONTAP utiliza la funcionalidad de copia de respaldo para realizar backups remotos de los datos almacenados mediante la solución Hyper-V mediante SMB.

  Esta opción solo es compatible con las SVM y solo con configuraciones de Hyper-V en SMB. La opción está habilitada de forma predeterminada en las SVM

- **Configuración de la profundidad del directorio de instantáneas**

  La configuración de esta opción permite definir la profundidad máxima de los directorios en los que crear instantáneas cuando se utiliza la función de copia oculta.

  Esta opción solo es compatible con las SVM y solo con configuraciones de Hyper-V en SMB. La opción está habilitada de forma predeterminada en las SVM

- **Activación o desactivación de las capacidades de búsqueda multidominio para la asignación de nombres**

  Si se habilita, cuando un usuario UNIX se asigna a un usuario de dominio de Windows mediante un comodín (*) en la parte de dominio del nombre de usuario de Windows (por ejemplo, *\joe), ONTAP busca el usuario especificado en todos los dominios con confianzas bidireccionales en el dominio principal. El dominio principal es el dominio que contiene la cuenta de equipo del servidor SMB.

  Como alternativa a la búsqueda en todos los dominios de confianza bidireccional, puede configurar una lista de dominios de confianza preferidos. Si esta opción está activada y se ha configurado una lista preferida, la lista preferida se utiliza para realizar búsquedas de asignación de nombres multidominio.

  La opción predeterminada es habilitar las búsquedas de asignación de nombres multidominio.

- **Configuración del tamaño del sector del sistema de archivos**

  Esta opción le permite configurar el tamaño del sector del sistema de archivos en bytes que ONTAP informa a clientes SMB. Hay dos valores válidos para esta opción `4096`: Y `512`. El valor predeterminado es `4096`. Es posible que deba establecer este valor en `512` si la aplicación Windows admite sólo un tamaño de sector de 512 bytes.

- **Activación o desactivación del control de acceso dinámico**

  Al habilitar esta opción, puede proteger objetos en el servidor SMB mediante el control de acceso dinámico (DAC), incluido el uso de auditorías para organizar políticas de acceso centrales y el uso de objetos de políticas de grupo para implementar políticas de acceso centrales. La opción está deshabilitada de forma predeterminada.

  Esta opción solo es compatible con las SVM.

- **Establecer las restricciones de acceso para sesiones no autenticadas (restringir anónimo)**

  Establecer esta opción determina cuáles son las restricciones de acceso para sesiones no autenticadas. Las restricciones se aplican a usuarios anónimos. De forma predeterminada, no hay restricciones de acceso para los usuarios anónimos.

- **Activación o desactivación de la presentación de ACL NTFS en volúmenes con seguridad efectiva UNIX (volúmenes de estilo de seguridad UNIX o volúmenes mixtos de estilo de seguridad con seguridad efectiva UNIX)**

  Al habilitar o deshabilitar esta opción, se determina cómo se presenta la seguridad de archivos y carpetas con seguridad UNIX a los clientes SMB. Si está habilitada, ONTAP presenta archivos y carpetas en volúmenes con seguridad UNIX para clientes de SMB como si tuviera seguridad de archivos NTFS con ACL de NTFS. Si está deshabilitada, ONTAP presenta volúmenes con seguridad UNIX como volúmenes FAT, sin seguridad de archivos. De forma predeterminada, los volúmenes se presentan como con seguridad de archivos NTFS con ACL NTFS.

- **Activación o desactivación de la funcionalidad de apertura falsa SMB**

  Al habilitar esta funcionalidad, se mejora el rendimiento de SMB 2.x y SMB 3.0, ya que se optimiza cómo ONTAP realiza solicitudes de apertura y cierre al consultar información sobre atributos de archivos y directorios. De manera predeterminada, la funcionalidad abierta falsa del SMB está habilitada. Esta opción solo es útil para las conexiones realizadas con SMB 2.x o posterior.

- **Activación o desactivación de las extensiones UNIX**

  Al habilitar esta opción se habilitan las extensiones UNIX en un servidor SMB. Las extensiones UNIX permiten visualizar la seguridad de estilo POSIX/UNIX a través del protocolo SMB. De forma predeterminada, esta opción está deshabilitada.

  Si tiene clientes SMB basados en UNIX, como clientes Mac OSX, en su entorno, debe habilitar extensiones UNIX. La habilitación de las extensiones UNIX permite al servidor SMB transmitir la información de seguridad de POSIX/UNIX a través de SMB al cliente basado en UNIX, lo que a continuación convierte la información de seguridad en la seguridad POSIX/UNIX.

- **Activación o desactivación de la compatibilidad para búsquedas cortas de nombres**

  Al habilitar esta opción, el servidor SMB puede realizar búsquedas en nombres cortos. Una consulta de búsqueda con esta opción habilitada intenta coincidir con 8.3 nombres de archivo junto con nombres de archivo largos. El valor por defecto de este parámetro es `false`.

- **Activación o desactivación del soporte para la publicidad automática de capacidades DFS**

  Habilitar o deshabilitar esta opción determina si los servidores SMB anuncian automáticamente capacidades DFS a clientes SMB 2.x y SMB 3.0 que se conectan a recursos compartidos. ONTAP utiliza referencias DFS en la implementación de enlaces simbólicos para el acceso a SMB. Si está habilitada, el servidor SMB siempre anuncia las capacidades DFS independientemente de si el acceso al enlace simbólico está habilitado. Si está deshabilitado, el servidor SMB anuncia capacidades DFS solo cuando los clientes se conectan a recursos compartidos donde se habilita el acceso al enlace simbólico.

- **Configuración del número máximo de créditos SMB**

  A partir de ONTAP 9.4, configurar la `-max-credits` opción le permite limitar el número de créditos que se otorgarán en una conexión SMB cuando los clientes y el servidor ejecuten SMB versión 2 o posterior. El valor predeterminado es 128.

- **Activación o desactivación de la compatibilidad con SMB multicanal**

  Al habilitar `-is-multichannel-enabled` la opción en ONTAP 9.4 y versiones posteriores, el servidor SMB puede establecer varias conexiones para una única sesión SMB cuando se implementan las NIC adecuadas en el clúster y sus clientes. Al hacerlo, se mejora el rendimiento y la tolerancia a fallos. El valor por defecto de este parámetro es `false`.

  Cuando se habilita SMB MultiChannel, también es posible especificar los siguientes parámetros:

  - El número máximo de conexiones permitidas por sesión multicanal. El valor predeterminado para este parámetro es 32.
  - Número máximo de interfaces de red anunciadas por sesión multicanal. El valor predeterminado para este parámetro es 256.

Configure las opciones del servidor SMB de ONTAP

Puede configurar las opciones del servidor SMB en cualquier momento después de crear un servidor SMB en una máquina virtual de almacenamiento (SVM).

Paso

1. Realice la acción deseada:

Si desea configurar opciones del servidor SMB…	Introduzca el comando…
En el nivel de privilegios de administrador	`vserver cifs options modify -vserver` *`vserver_name options`*
En el nivel de privilegios avanzados	a. `set -privilege advanced` b. `vserver cifs options modify -vserver` *`vserver_name options`* c. `set -privilege admin`

Obtenga más información sobre `vserver cifs options modify` las opciones del servidor SMB y configurarlas en el "Referencia de comandos del ONTAP".

Configure el permiso para otorgar grupos UNIX a los usuarios SMB de ONTAP

Puede configurar esta opción para conceder permisos de grupo para tener acceso a archivos o directorios aunque el usuario SMB entrante no sea el propietario del archivo.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Configure el permiso conceder grupo UNIX según corresponda:

Si desea	Introduzca el comando
Active el acceso a los archivos o directorios para obtener permisos de grupo incluso si el usuario no es el propietario del archivo	`vserver cifs options modify -grant-unix-group-perms-to-others true`
Desactive el acceso a los archivos o directorios para obtener permisos de grupo incluso si el usuario no es el propietario del archivo	`vserver cifs options modify -grant-unix-group-perms-to-others false`

3. Compruebe que la opción está establecida en el valor deseado: `vserver cifs options show -fields grant-unix-group-perms-to-others`
4. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Configura las restricciones de acceso al bloque de mensajes del servidor de ONTAP para usuarios anónimos

De forma predeterminada, un usuario anónimo y sin autenticar (también conocido como *null user*) puede tener acceso a cierta información de la red. Puede usar una opción de servidor SMB para configurar restricciones de acceso para el usuario anónimo.

Acerca de esta tarea

```
`-restrict-anonymous`La opción Servidor SMB corresponde a la
`RestrictAnonymous` entrada del Registro en Windows.
```

Los usuarios anónimos pueden enumerar o enumerar determinados tipos de información del sistema de los hosts de Windows de la red, incluidos los nombres y detalles de usuario, las directivas de cuenta y los nombres de recursos compartidos. Puede controlar el acceso para el usuario anónimo especificando uno de tres ajustes de restricción de acceso:

Valor	Descripción
`no-restriction` (predeterminado)	Especifica que no hay restricciones de acceso para los usuarios anónimos.
`no-enumeration`	Especifica que sólo la enumeración está restringida a los usuarios anónimos.
`no-access`	Especifica que el acceso está restringido para usuarios anónimos.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Configure el valor Restringir anónimo: `vserver cifs options modify -vserver` *`vserver_name`* `-restrict-anonymous {no-restriction|no-enumeration|no-access}`
3. Compruebe que la opción está establecida en el valor deseado: `vserver cifs options show -vserver` *`vserver_name`*
4. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Información relacionada

Opciones de servidor disponibles

Gestione cómo se presenta la seguridad de archivos a los clientes SMB para los datos de estilo de seguridad UNIX

Obtenga más información sobre la presentación de la seguridad de archivos ONTAP a clientes pymes para datos de tipo de seguridad de UNIX

Puede elegir cómo desea presentar la seguridad de archivos a los clientes de SMB para los datos de estilo de seguridad de UNIX habilitando o deshabilitando la presentación de ACL NTFS a clientes SMB. Existen ventajas en cada entorno, que debe entender para elegir el ajuste que mejor se ajuste a los requisitos de su negocio.

De forma predeterminada, ONTAP presenta los permisos de UNIX sobre volúmenes de estilo de seguridad de UNIX a clientes de SMB como ACL de NTFS. Hay escenarios en los que esto es deseable, incluyendo los siguientes:

- Desea ver y editar los permisos de UNIX mediante la ficha **Seguridad** del cuadro Propiedades de Windows.

  No puede modificar los permisos de un cliente Windows si el sistema UNIX no permite la operación. Por ejemplo, no puede cambiar la propiedad de un archivo que no posee, ya que el sistema UNIX no permite esta operación. Esta restricción impide a los clientes SMB omitir los permisos de UNIX establecidos en los archivos y carpetas.

- Los usuarios están editando y guardando archivos en el volumen de estilo de seguridad de UNIX utilizando ciertas aplicaciones de Windows, por ejemplo, Microsoft Office, donde ONTAP debe conservar los permisos de UNIX durante las operaciones de guardado.
- Hay ciertas aplicaciones de Windows en su entorno que esperan leer ACL NTFS en los archivos que utilizan.

En determinadas circunstancias, es posible que desee deshabilitar la presentación de permisos UNIX como ACL NTFS. Si esta funcionalidad está deshabilitada, ONTAP presenta volúmenes de estilo de seguridad UNIX como volúmenes FAT a clientes SMB. Hay motivos específicos por los que puede que desee presentar volúmenes de estilo de seguridad de UNIX como volúmenes FAT a clientes SMB:

- Sólo se pueden cambiar los permisos de UNIX mediante montajes en clientes UNIX.

  La pestaña Seguridad no está disponible cuando se asigna un volumen de estilo de seguridad UNIX en un cliente SMB. La unidad asignada parece formatearse con el sistema de archivos FAT, que no tiene permisos de archivo.

- Está utilizando aplicaciones a través de SMB que establecen ACL NTFS en archivos y carpetas a los que se tiene acceso, lo cual puede fallar si los datos residen en volúmenes de estilo de seguridad de UNIX.

  Si ONTAP informa del volumen como FAT, la aplicación no intenta cambiar una ACL.

Información relacionada

- Configurar estilos de seguridad en volúmenes FlexVol
- Configurar estilos de seguridad en qtrees

Configure la presentación de ACL NTFS a los clientes SMB de ONTAP para datos de estilo de seguridad de UNIX

Puede habilitar o deshabilitar la presentación de ACL NTFS a clientes SMB para datos de estilo de seguridad de UNIX (volúmenes de estilo de seguridad de UNIX y volúmenes mixtos de estilo de seguridad con seguridad efectiva de UNIX).

Acerca de esta tarea

Si habilita esta opción, ONTAP presenta archivos y carpetas en volúmenes con un estilo de seguridad UNIX efectivo para los clientes de SMB como si tuviera ACL NTFS. Si deshabilita esta opción, los volúmenes se presentan como volúmenes FAT a los clientes de SMB. El valor predeterminado es presentar ACL de NTFS a los clientes de SMB.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Configure la opción UNIX NTFS ACL: `vserver cifs options modify -vserver vserver_name -is-unix-nt-acl-enabled {true|false}`
3. Compruebe que la opción está establecida en el valor deseado: `vserver cifs options show -vserver vserver_name`
4. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Obtenga más información sobre la conservación de permisos UNIX para volúmenes de FlexVol SMB de ONTAP

Cuando las aplicaciones Windows editan y guardan archivos de un volumen FlexVol que actualmente tienen permisos UNIX, ONTAP puede preservar los permisos UNIX.

Cuando las aplicaciones de clientes de Windows editan y guardan archivos, leen las propiedades de seguridad del archivo, crean un nuevo archivo temporal, aplican esas propiedades al archivo temporal y, a continuación, asignan al archivo temporal el nombre de archivo original.

Cuando los clientes de Windows realizan una consulta para las propiedades de seguridad, reciben una ACL construida que representa exactamente los permisos de UNIX. El único propósito de esta ACL construida es preservar los permisos UNIX del archivo a medida que las aplicaciones de Windows actualizan los archivos para garantizar que los archivos resultantes tengan los mismos permisos UNIX. ONTAP no establece ninguna ACL de NTFS usando la ACL construida.

Obtenga información sobre la gestión de permisos UNIX mediante la ficha Seguridad de Windows para servidores SMB de ONTAP

Si desea manipular los permisos de UNIX de archivos o carpetas en volúmenes o qtrees de estilo de seguridad mixtos en las SVM, puede utilizar la pestaña Seguridad en clientes de Windows. También puede utilizar aplicaciones que puedan consultar y establecer ACL de Windows.

- Modificación de permisos de UNIX

  Puede usar la pestaña Seguridad de Windows para ver y cambiar los permisos de UNIX para un volumen o un qtree de estilo de seguridad mixto. Si utiliza la ficha Seguridad de Windows principal para cambiar los permisos de UNIX, primero debe quitar la ACE existente que desea editar (esto establece los bits de modo en 0) antes de realizar los cambios. De forma alternativa, puede utilizar el editor avanzado para cambiar los permisos.

  Si se utilizan permisos de modo, puede cambiar directamente los permisos de modo para el UID, GID y otros (todos los demás con una cuenta en el equipo) de la lista. Por ejemplo, si el UID mostrado tiene permisos r-x, puede cambiar los permisos de UID a rwx.

- Cambiar los permisos de UNIX a los permisos NTFS

  Puede usar la pestaña Seguridad de Windows para reemplazar objetos de seguridad UNIX por objetos de seguridad de Windows en un volumen o qtree de estilo de seguridad mixto donde los archivos y carpetas tienen un estilo de seguridad efectivo de UNIX.

  Primero debe quitar todas las entradas de permisos de UNIX enumeradas antes de que pueda reemplazarlas con los objetos de usuario y grupo de Windows deseados. A continuación, puede configurar ACL basados en NTFS en los objetos Usuario y Grupo de Windows. Si quita todos los objetos de

seguridad de UNIX y agrega sólo usuarios y grupos de Windows a un archivo o carpeta de un volumen o qtree de estilo de seguridad mixto, cambie el estilo de seguridad efectivo del archivo o carpeta de UNIX a NTFS.

Al cambiar los permisos de una carpeta, el comportamiento predeterminado de Windows es propagar estos cambios a todas las subcarpetas y archivos. Por lo tanto, debe cambiar la opción de propagación a la configuración deseada si no desea propagar un cambio en el estilo de seguridad a todas las carpetas secundarias, subcarpetas y archivos.

Gestione la configuración de seguridad del servidor SMB

Obtenga más información sobre el manejo de la autenticación del cliente SMB de ONTAP

Antes de que los usuarios puedan crear conexiones SMB para acceder a los datos contenidos en la SVM, el dominio al que pertenece el servidor SMB debe autenticarse. El servidor SMB admite dos métodos de autenticación: Kerberos y NTLM (NTLMv1 o NTLMv2). Kerberos es el método predeterminado utilizado para autenticar usuarios de dominio.

Autenticación Kerberos

ONTAP admite la autenticación Kerberos al crear sesiones SMB autenticadas.

Kerberos es el servicio de autenticación principal para Active Directory. El servidor Kerberos o el servicio de centro de distribución de claves Kerberos (KDC) almacena y recupera información acerca de los principios de seguridad en Active Directory. A diferencia del modelo NTLM, los clientes de Active Directory que deseen establecer una sesión con otro equipo, como el servidor SMB, póngase en contacto directamente con un KDC para obtener sus credenciales de sesión.

Autenticación NTLM

La autenticación de clientes NTLM se realiza mediante un protocolo de respuesta a desafío basado en el conocimiento compartido de un secreto específico del usuario basado en una contraseña.

Si un usuario crea una conexión SMB con una cuenta de usuario local de Windows, el servidor SMB realiza la autenticación localmente con NTLMv2.

Obtenga más información sobre la configuración de seguridad del servidor SMB para la configuración de la recuperación ante desastres SVM de ONTAP

Antes de crear una SVM que está configurada como destino de recuperación de desastres en el que la identidad no se conserva (`-identity-preserve`la opción se establece en en `false` en la configuración de SnapMirror), debe conocer cómo se gestionan las configuraciones de seguridad del servidor SMB en la SVM de destino.

- La configuración de seguridad del servidor SMB no predeterminada no se replica en el destino.

  Cuando se crea un servidor SMB en la SVM de destino, todas las opciones de seguridad del servidor SMB se establecen en valores predeterminados. Cuando el destino de recuperación ante desastres de SVM se inicializa, se actualiza o se vuelve a sincronizar, la configuración de seguridad del servidor SMB en el origen no se replica en el destino.

- Debe configurar manualmente las opciones de seguridad del servidor SMB no predeterminadas.

  Si tiene configuradas las opciones de seguridad del servidor SMB no predeterminadas en la SVM de origen, debe configurar manualmente estas mismas opciones en la SVM de destino después de que el destino pase a ser de lectura y escritura (después de que se rompa la relación de SnapMirror).

Mostrar información sobre la configuración de seguridad del servidor SMB de ONTAP

Puede ver información acerca de la configuración de seguridad del servidor SMB en las máquinas virtuales de almacenamiento (SVM). Puede utilizar esta información para comprobar que la configuración de seguridad es correcta.

Acerca de esta tarea

Una configuración de seguridad mostrada puede ser el valor predeterminado para ese objeto o un valor no predeterminado que se configura mediante la CLI de ONTAP o mediante objetos de directiva de grupo de Active Directory (GPO).

No utilice `vserver cifs security show` el comando para servidores SMB en modo de grupo de trabajo, ya que algunas de las opciones no son válidas.

Paso

1. Ejecute una de las siguientes acciones:

Si desea mostrar información acerca de…	Introduzca el comando…
Toda la configuración de seguridad en una SVM especificada	`vserver cifs security show -vserver` *`vserver_name`*
Una configuración o configuración de seguridad específica en la SVM	`vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]` Puede introducir `-fields ?` para determinar qué campos puede utilizar.

Ejemplo

En el siguiente ejemplo, se muestran todas las opciones de seguridad de la SVM vs1:

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                          Kerberos Clock Skew:        5 minutes
                          Kerberos Ticket Age:        10 hours
                         Kerberos Renewal Age:        7 days
                         Kerberos KDC Timeout:        3 seconds
                          Is Signing Required:        false
               Is Password Complexity Required:        true
          Use start_tls For AD LDAP connection:        false
                     Is AES Encryption Enabled:        false
                        LM Compatibility Level:        lm-ntlm-ntlmv2-krb
                    Is SMB Encryption Required:        false
                       Client Session Security:        none
              SMB1 Enabled for DC Connections:        false
              SMB2 Enabled for DC Connections:        system-default
LDAP Referral Enabled For AD LDAP connections:        false
             Use LDAPS for AD LDAP connection:        false
    Encryption is required for DC Connections:        false
 AES session key enabled for NetLogon channel:        false
  Try Channel Binding For AD LDAP Connections:        false
```

Tenga en cuenta que la configuración mostrada depende de la versión de ONTAP en ejecución.

En el siguiente ejemplo, se muestra el desfase de reloj de Kerberos para SVM vs1:

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

            vserver kerberos-clock-skew
            ------- -------------------
            vs1     5
```

Información relacionada

Mostrar información acerca de las configuraciones de GPO

Configure la complejidad de la contraseña de ONTAP para usuarios locales de SMB

La complejidad de contraseña necesaria proporciona una seguridad mejorada para los usuarios de SMB locales en sus máquinas virtuales de almacenamiento (SVM). La función de complejidad de contraseña necesaria está activada de forma predeterminada. Puede deshabilitarla y volver a habilitarla en cualquier momento.

Antes de empezar

Los usuarios locales, los grupos locales y la autenticación de usuarios locales deben estar habilitados en el servidor CIFS.

Acerca de esta tarea

No utilice `vserver cifs security modify` el comando para un servidor CIFS en modo grupo de trabajo porque algunas de las opciones no son válidas.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea que la complejidad de contraseña requerida para los usuarios locales de la SMB sea…	Introduzca el comando…
Activado	`vserver cifs security modify -vserver vserver_name -is-password-complexity -required true`
Deshabilitado	`vserver cifs security modify -vserver vserver_name -is-password-complexity -required false`

2. Compruebe la configuración de seguridad para la complejidad necesaria de la contraseña: `vserver cifs security show -vserver vserver_name`

Ejemplo

El siguiente ejemplo muestra que la complejidad de contraseña necesaria está habilitada para los usuarios locales de SMB para SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
------- -------------------------------
vs1     true
```

Información relacionada

- Mostrar información sobre la configuración de seguridad del servidor
- Obtenga información sobre los usuarios y grupos locales
- Requisitos para las contraseñas de usuario local
- Cambiar las contraseñas de la cuenta de usuario local

Puede modificar ciertos ajustes de seguridad Kerberos del servidor CIFS, incluyendo la hora de desfase de reloj de Kerberos máxima permitida, la duración de la incidencia de Kerberos y el número máximo de días de renovación de incidencias.

Acerca de esta tarea

La modificación de la configuración de Kerberos del servidor CIFS mediante `vserver cifs security modify` el comando modifica los ajustes solo en la única máquina virtual de almacenamiento (SVM) que especifique con el `-vserver` parámetro. Puede administrar de forma centralizada la configuración de seguridad Kerberos para todas las SVM del clúster que pertenecen al mismo dominio de Active Directory mediante objetos de directiva de grupo (GPO) de Active Directory.

Pasos

1. Ejecute una o varias de las siguientes acciones:

Si desea…	Introduzca…
Especifique el tiempo máximo permitido de inclinación del reloj Kerberos en minutos (9.13.1 y posteriores) o segundos (9.12.1 o anteriores).	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-clock-skew` *`integer_in_minutes`* El valor predeterminado es 5 minutos.
Especifique la duración del billete Kerberos en horas.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours` El valor predeterminado es 10 horas.
Especifique el número máximo de días de renovación de la tarjeta.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-renew-age` *`integer_in_days`* El valor predeterminado es 7 días.
Especifique el tiempo de espera para los sockets de los KDC después de lo cual todos los KDC están marcados como inaccesibles.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-kdc-timeout` *`integer_in_seconds`* El valor predeterminado es 3 segundos.

2. Compruebe la configuración de seguridad de Kerberos:

   `vserver cifs security show -vserver` *`vserver_name`*

Ejemplo

En el ejemplo siguiente se realizan los cambios siguientes en la seguridad de Kerberos: «'Kerberos Clock Skew» se establece en 3 minutos y «'Kerberos Ticket Age'» se establece en 8 horas para SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                    Kerberos Clock Skew:                    3 minutes
                    Kerberos Ticket Age:                    8 hours
                  Kerberos Renewal Age:                     7 days
                  Kerberos KDC Timeout:                     3 seconds
                    Is Signing Required:                false
         Is Password Complexity Required:                 true
   Use start_tls For AD LDAP connection:                 false
              Is AES Encryption Enabled:                 false
                 LM Compatibility Level:  lm-ntlm-ntlmv2-krb
             Is SMB Encryption Required:                 false
```

Información relacionada

"Mostrar información sobre la configuración de seguridad del servidor"

"Objetos de normativa de grupo compatibles"

"Aplicar objetos de directiva de grupo a servidores CIFS"

Establezca el nivel de seguridad de autenticación mínimo del servidor SMB de ONTAP

Puede establecer el nivel de seguridad mínimo del servidor SMB, también conocido como *LMCompatibilityLevel*, en el servidor SMB para satisfacer los requisitos de seguridad del negocio para el acceso de cliente SMB. El nivel de seguridad mínimo es el nivel mínimo de los tokens de seguridad que acepta el servidor SMB de los clientes SMB.

Acerca de esta tarea

- Los servidores SMB en modo de grupo de trabajo sólo admiten la autenticación NTLM. La autenticación Kerberos no es compatible.
- LmCompatibilityLevel se aplica sólo a la autenticación de cliente SMB, no a la autenticación de administrador.

Es posible configurar el nivel de seguridad de autenticación mínimo en uno de los cuatro niveles de seguridad compatibles.

Valor	Descripción
`lm-ntlm-ntlmv2-krb` (predeterminado)	La máquina virtual de almacenamiento (SVM) acepta seguridad de autenticación LM, NTLMv2 y Kerberos.

Valor	Descripción
`ntlm-ntlmv2-krb`	La SVM acepta la seguridad de autenticación NTLM, NTLMv2 y Kerberos. La SVM rechaza la autenticación LM.
`ntlmv2-krb`	La SVM acepta la seguridad de autenticación NTLMv2 y Kerberos. La SVM rechaza la autenticación LM y NTLM.
`krb`	La SVM solo acepta la seguridad de autenticación de Kerberos. La SVM deniega la autenticación LM, NTLM y NTLMv2.

Pasos

1. Establezca el nivel de seguridad de autenticación mínimo: `vserver cifs security modify -vserver` *`vserver_name`* `-lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. Verifique que el nivel de seguridad de autenticación esté definido en el nivel deseado: `vserver cifs security show -vserver` *`vserver_name`*

Información relacionada

Configurar el cifrado AES para la comunicación basada en Kerberos

Configure la seguridad SMB de ONTAP sólida para la comunicación basada en Kerberos mediante el cifrado AES

Para obtener la mayor seguridad con la comunicación basada en Kerberos, puede habilitar el cifrado AES-256 y AES-128 en el servidor SMB. De manera predeterminada, cuando crea un servidor SMB en la SVM, el cifrado Advanced Encryption Standard (AES) está deshabilitado. Debe habilitarla para aprovechar la seguridad robusta proporcionada por el cifrado AES.

La comunicación relacionada con Kerberos para SMB se utiliza durante la creación del servidor SMB en la SVM, así como durante la fase de configuración de la sesión SMB. El servidor SMB es compatible con los siguientes tipos de cifrado para la comunicación de Kerberos:

- AES 256
- AES 128
- DES
- RC4-HMAC

Si desea utilizar el tipo de cifrado de seguridad más alto para la comunicación de Kerberos, debe habilitar el cifrado AES para la comunicación de Kerberos en la SVM.

Cuando se crea el servidor SMB, el controlador de dominio crea una cuenta de equipo en Active Directory. En este momento, el KDC se da cuenta de las capacidades de cifrado de la cuenta de equipo en particular. Posteriormente, se selecciona un tipo de cifrado concreto para cifrar el ticket de servicio que el cliente presenta al servidor durante la autenticación.

A partir de ONTAP 9.12.1, puede especificar los tipos de cifrado que desea anunciar en el KDC de Active Directory (AD). Puede utilizar `-advertised-enc-types` la opción para habilitar los tipos de cifrado recomendados, y puede utilizarla para deshabilitar los tipos de cifrado más débiles. Aprenda a "Configurar el cifrado AES para la comunicación basada en Kerberos".

> Las nuevas instrucciones de AES (Intel AES ni) están disponibles en SMB 3.0, mejorando el algoritmo AES y acelerando el cifrado de datos con las familias de procesadores compatibles.a partir de SMB 3.1.1, AES-128-GCM reemplaza a AES-128-CCM como el algoritmo hash utilizado por el cifrado SMB.

Información relacionada

Modificar la configuración de seguridad del servidor

Configure el cifrado AES para la comunicación basada en Kerberos SMB de ONTAP

Para aprovechar la seguridad más fuerte con la comunicación basada en Kerberos, debe utilizar el cifrado AES-256 y AES-128 en el servidor SMB. A partir de ONTAP 9.13.1, el cifrado AES está habilitado de forma predeterminada. Si no desea que el servidor SMB seleccione los tipos de cifrado AES para la comunicación basada en Kerberos con el KDC de Active Directory (AD), puede deshabilitar el cifrado AES.

Si el cifrado AES está habilitado de forma predeterminada y si tiene la opción de especificar tipos de cifrado depende de su versión de ONTAP.

Versión de ONTAP	El cifrado AES está activado…	¿Puede especificar tipos de cifrado?
9.13.1 y posterior	De forma predeterminada	Sí
9.12.1	Manualmente	Sí
9.11.1 y anteriores	Manualmente	No

A partir de ONTAP 9.12,1, el cifrado AES se habilita y se deshabilita mediante la `-advertised-enc-types` opción, que le permite especificar los tipos de cifrado anunciados al KDC de AD. La configuración predeterminada es `rc4` AND `des`, pero cuando se especifica un tipo AES, se activa el cifrado AES. También puede utilizar la opción para desactivar explícitamente los tipos de cifrado RC4 y DES más débiles. En ONTAP 9.11,1 y versiones anteriores, debe usar `-is-aes-encryption-enabled` la opción para habilitar y deshabilitar el cifrado AES, y no se pueden especificar los tipos de cifrado.

Para mejorar la seguridad, la máquina virtual de almacenamiento (SVM) cambia su contraseña de cuenta de máquina en AD cada vez que se modifica la opción de seguridad AES. El cambio de la contraseña podría requerir credenciales AD administrativas para la unidad organizativa (OU) que contiene la cuenta del equipo.

Si una SVM se configura como un destino de recuperación ante desastres en el que la identidad no se conserva (`-identity-preserve`la opción se establece en en `false` en la configuración de SnapMirror), los ajustes de seguridad del servidor SMB no predeterminados no se replican en el destino. Si habilitó el cifrado AES en la SVM de origen, debe habilitarla manualmente.

Ejemplo 1. Pasos

ONTAP 9.12.1 y versiones posteriores

1. Ejecute una de las siguientes acciones:

Si desea que los tipos de cifrado AES para la comunicación Kerberos sean…	Introduzca el comando…
Activado	`vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256`
Deshabilitado	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

   Nota: La `-is-aes-encryption-enabled` opción está en desuso en ONTAP 9.12,1 y podría ser eliminada en una versión posterior.

2. Compruebe que el cifrado AES está activado o desactivado como desee: `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

Ejemplos

En el siguiente ejemplo, se habilitan los tipos de cifrado AES para el servidor SMB en la SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs1      aes-128,aes-256
```

En el ejemplo siguiente se habilitan los tipos de cifrado AES para el servidor SMB en la SVM vs2. Se solicita al administrador que introduzca las credenciales AD administrativas para la unidad organizativa que contiene el servidor SMB.

```
cluster1::> vserver cifs security modify -vserver vs2 -advertised-enc
-types aes-128,aes-256

Info: In order to enable SMB AES encryption, the password for the SMB
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs2      aes-128,aes-256
```

ONTAP 9.11.1 y anteriores

1. Ejecute una de las siguientes acciones:

Si desea que los tipos de cifrado AES para la comunicación Kerberos sean…	Introduzca el comando…
Activado	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled true`
Deshabilitado	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false`

2. Compruebe que el cifrado AES está activado o desactivado como desee: `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

   `is-aes-encryption-enabled`El campo muestra `true` si el cifrado AES está activado y `false` si está desactivado.

Ejemplos

En el siguiente ejemplo, se habilitan los tipos de cifrado AES para el servidor SMB en la SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs1      true
```

En el ejemplo siguiente se habilitan los tipos de cifrado AES para el servidor SMB en la SVM vs2. Se solicita al administrador que introduzca las credenciales AD administrativas para la unidad organizativa que contiene el servidor SMB.

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs2      true
```

Información relacionada

"El usuario de dominio no puede iniciar sesión en el clúster con el túnel de dominio"

Utilice la firma SMB para mejorar la seguridad de la red

Obtenga más información sobre el uso de la firma SMB de ONTAP para mejorar la seguridad de la red

La firma SMB ayuda a garantizar que el tráfico de red entre el servidor SMB y el cliente no se vea comprometido; esto evita los ataques de repetición. De forma predeterminada, ONTAP admite la firma SMB cuando lo solicita el cliente. De manera opcional, el administrador de almacenamiento puede configurar el servidor SMB para que requiera la

firma SMB.

Conozca cómo las políticas de firma afectan a la comunicación con servidores SMB de ONTAP

Además de la configuración de seguridad de firma SMB del servidor CIFS, dos políticas de firma SMB en clientes de Windows controlan la firma digital de las comunicaciones entre clientes y el servidor CIFS. Puede configurar el ajuste que cumpla con sus requisitos empresariales.

Las directivas SMB de cliente se controlan a través de la configuración de la directiva de seguridad local de Windows, que se configuran mediante Microsoft Management Console (MMC) o los GPO de Active Directory. Para obtener más información acerca de los problemas de firma SMB de cliente y de seguridad, consulte la documentación de Microsoft Windows.

A continuación, se muestran descripciones de las dos políticas de firma SMB en los clientes de Microsoft:

- `Microsoft network client: Digitally sign communications (if server agrees)`

  Esta configuración controla si la capacidad de firma SMB del cliente está habilitada. Está activado de forma predeterminada. Cuando se deshabilita esta configuración en el cliente, las comunicaciones del cliente con el servidor CIFS dependen de la configuración de firma SMB en el servidor CIFS.

- `Microsoft network client: Digitally sign communications (always)`

  Esta configuración controla si el cliente requiere la firma SMB para comunicarse con un servidor. Está desactivado de forma predeterminada. Cuando esta configuración está deshabilitada en el cliente, el comportamiento de la firma SMB se basa en la configuración de la política `Microsoft network client: Digitally sign communications (if server agrees)` y del servidor CIFS.

> Si el entorno incluye clientes de Windows configurados para requerir la firma SMB, debe habilitar la firma SMB en el servidor CIFS. Si no lo hace, el servidor CIFS no puede proporcionar datos a estos sistemas.

Los resultados efectivos de la configuración de firma SMB del cliente y del servidor CIFS dependen de si las sesiones SMB utilizan SMB 1.0 o SMB 2.x y versiones posteriores.

En la tabla siguiente se resume el comportamiento efectivo de la firma SMB si la sesión utiliza SMB 1.0:

Cliente	No se requiere firma con ONTAP	Se requiere firma ONTAP
Firma desactivada y no requerida	No firmado	Firmado
Firma habilitada y no requerida	No firmado	Firmado
Firma desactivada y obligatoria	Firmado	Firmado
Firma habilitada y requerida	Firmado	Firmado

Es posible que los clientes Windows SMB 1 anteriores y algunos clientes SMB 1 distintos de Windows no puedan conectarse si la firma está deshabilitada en el cliente, pero es necesaria en el servidor CIFS.

En la tabla siguiente se resume el comportamiento efectivo de la firma SMB si la sesión utiliza SMB 2.x o SMB 3.0:

Para los clientes SMB 2.x y SMB 3.0, la firma SMB siempre está habilitada. No se puede deshabilitar.

Cliente	No se requiere firma con ONTAP	Se requiere firma ONTAP
No se requiere firma	No firmado	Firmado
Se requiere firma	Firmado	Firmado

En la tabla siguiente se resume el comportamiento de firma SMB de servidor y cliente de Microsoft predeterminado:

Protocolo	Algoritmo hash	Puede activar/desactivar	Se puede requerir o no se puede requerir	Valor predeterminado del cliente	Valor predeterminado del servidor	DC predeterminado
SMB 1,0	MD5	Sí	Sí	Habilitado (no es necesario)	Deshabilitado (no obligatorio)	Obligatorio
SMB 2.x	HMAC SHA-256	No	Sí	No es obligatorio	No es obligatorio	Obligatorio
SMB 3,0	AES-CMAC.	No	Sí	No es obligatorio	No es obligatorio	Obligatorio

Microsoft ya no recomienda utilizar `Digitally sign communications (if client agrees)` `Digitally sign communications (if server agrees)` la configuración de directiva de grupo o. Microsoft ya no recomienda utilizar `EnableSecuritySignature` la configuración del Registro. Estas opciones solo afectan al comportamiento de SMB 1 y se pueden reemplazar por la `Digitally sign communications (always)` configuración de directiva de grupo o la `RequireSecuritySignature` configuración del registro. También puede obtener más información en el blog de Microsoft.Conceptos básicos de The para la firma de SMB (cubriendo tanto SMB1 como SMB2)

Conozca el impacto en el rendimiento de la firma SMB de ONTAP

Cuando las sesiones SMB utilizan la firma SMB, todas las comunicaciones SMB a y desde clientes de Windows experimentan un impacto en el rendimiento, lo cual afecta tanto a los clientes como al servidor (es decir, los nodos del clúster que ejecuta la SVM que contiene el servidor SMB).

El impacto en el rendimiento muestra que el uso de CPU ha aumentado tanto en los clientes como en el servidor, aunque la cantidad de tráfico de red no cambia.

La magnitud del impacto en el rendimiento depende de la versión de ONTAP 9 que esté ejecutando. A partir de ONTAP 9.7, un nuevo algoritmo de descarga del cifrado puede permitir un mejor rendimiento en el tráfico de SMB firmado. La descarga de firma SMB se habilita de forma predeterminada cuando se habilita la firma SMB.

El rendimiento mejorado de la firma SMB requiere la funcionalidad de descarga de AES-ni. Consulte el Hardware Universe (HWU) para verificar que la descarga AES-ni es compatible con su plataforma.

Otras mejoras de rendimiento también son posibles si usted es capaz de utilizar SMB versión 3,11 que admite el algoritmo GCM mucho más rápido.

Según la red, la versión de ONTAP 9, la versión de SMB y la implementación de SVM, el impacto en el rendimiento de la firma SMB puede variar enormemente; puede verificarlo únicamente mediante pruebas en el entorno de red.

La mayoría de los clientes de Windows negocian la firma SMB de forma predeterminada si está habilitada en el servidor. Si necesita protección SMB para algunos de sus clientes Windows y la firma SMB está provocando problemas de rendimiento, puede deshabilitar la firma SMB en cualquiera de sus clientes Windows que no necesiten protección contra ataques de repetición. Para obtener información sobre cómo deshabilitar la firma SMB en clientes Windows, consulte la documentación de Microsoft Windows.

Recomendaciones de configuración de firma SMB de ONTAP

Puede configurar un comportamiento de firma SMB entre clientes SMB y el servidor CIFS para satisfacer sus requisitos de seguridad. La configuración que elija al configurar la firma SMB en el servidor CIFS depende de cuáles sean sus requisitos de seguridad.

Es posible configurar la firma SMB en el cliente o en el servidor CIFS. Tenga en cuenta las siguientes recomendaciones al configurar la firma SMB:

Si…	Recomendación…
Desea aumentar la seguridad de la comunicación entre el cliente y el servidor	Haga que se requiera la firma SMB en el cliente habilitando `Require Option (Sign always)` la configuración de seguridad en el cliente.
Es conveniente que todo el tráfico de SMB esté firmado a una determinada máquina virtual de almacenamiento (SVM)	Para requerir la firma SMB en el servidor CIFS, configure la configuración de seguridad para requerir la firma SMB.

Consulte la documentación de Microsoft para obtener más información acerca de la configuración de la seguridad del cliente de Windows.

Obtenga información sobre la configuración de firma SMB de ONTAP para varias LIFS de datos

Si habilita o deshabilita la firma SMB requerida en el servidor SMB, debe tener en cuenta las directrices para varias configuraciones de LIF de datos para una SVM.

Cuando configura un servidor SMB, puede haber varios LIF de datos configurados. Si es así, el servidor DNS

contiene varias `A` entradas de registro para el servidor CIFS, todos utilizando el mismo nombre de host del servidor SMB, pero cada uno con una dirección IP exclusiva. Por ejemplo, un servidor SMB que tiene dos LIF de datos configuradas puede tener las siguientes `A` entradas de registro DNS:

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

El comportamiento normal es que, al cambiar la configuración de firma SMB necesaria, solo las nuevas conexiones de clientes se ven afectadas por el cambio en la configuración de firma SMB. Sin embargo, hay una excepción a este comportamiento. Existe un caso en el que un cliente tiene una conexión existente con un recurso compartido y éste crea una nueva conexión con el mismo recurso compartido después de cambiar la configuración, manteniendo la conexión original. En este caso, tanto la conexión SMB nueva como la existente adoptan los nuevos requisitos de firma SMB.

Observe el siguiente ejemplo:

1. CLIENT1 se conecta a un recurso compartido sin necesidad de firma SMB mediante la ruta de acceso `O:\`.
2. El administrador de almacenamiento modifica la configuración del servidor SMB para requerir la firma SMB.
3. CLIENT1 se conecta al mismo recurso compartido con la firma SMB necesaria mediante la ruta de acceso `S:\` (manteniendo la conexión mediante la ruta `O:\`).
4. El resultado es que se utiliza la firma SMB cuando se accede a los datos `O:\` en `S:\` las unidades y.

Configure la firma ONTAP para el tráfico SMB entrante

Puede aplicar el requisito de que los clientes firmen mensajes SMB habilitando la firma SMB requerida. Si está habilitada, ONTAP solo acepta mensajes SMB si tienen firmas válidas. Si desea permitir la firma SMB, pero no la requiere, puede deshabilitar la firma SMB requerida.

Acerca de esta tarea

De manera predeterminada, la firma SMB requerida está deshabilitada. Es posible habilitar o deshabilitar la firma SMB requerida en cualquier momento.

> La firma SMB no está deshabilitada de forma predeterminada en las siguientes circunstancias:
>
> 1. La firma SMB necesaria está habilitada y el clúster se revierte a una versión de ONTAP que no admite la firma SMB.
> 2. Posteriormente, el clúster se actualiza a una versión de ONTAP que admite la firma SMB.
>
> En estas circunstancias, la configuración de firma SMB configurada originalmente en una versión compatible de ONTAP se conserva mediante la reversión y la posterior actualización.

Cuando se configura una relación de recuperación ante desastres de una máquina virtual de almacenamiento (SVM), el valor que se selecciona para `-identity-preserve` la opción del `snapmirror create` comando determina los detalles de configuración que se replican en la SVM de destino.

Si establece `-identity-preserve` la opción en `true` (ID-preserve), la configuración de seguridad de firma SMB se replica en el destino.

Si establece `-identity-preserve` la opción en `false` (non-ID-preserve), la configuración de seguridad de firma SMB no se replica en el destino. En este caso, la configuración de seguridad del servidor CIFS en el destino se establece en los valores predeterminados. Si habilitó la firma SMB requerida en la SVM de origen, debe habilitar manualmente la firma SMB requerida en la SVM de destino.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea que la firma SMB sea…	Introduzca el comando…
Activado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required true`
Deshabilitado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required false`

2. Compruebe que la firma SMB necesaria esté habilitada o deshabilitada; para ello, determine si el valor del `Is Signing Required` campo de la salida del siguiente comando está establecido en el valor deseado: `vserver cifs security show -vserver` *`vserver_name`* `-fields is-signing-required`

Ejemplo

En el siguiente ejemplo, se habilita la firma SMB requerida para SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver  is-signing-required
-------- --------------------
vs1      true
```

Los cambios en la configuración de cifrado surten efecto para las nuevas conexiones. Las conexiones existentes no se ven afectadas.

Información relacionada

- "snapmirror create"

Determinar si las sesiones SMB de ONTAP están firmadas

Puede ver información sobre las sesiones SMB conectadas en el servidor CIFS. Puede usar esta información para determinar si las sesiones SMB están firmadas. Esto puede resultar útil para determinar si las sesiones de cliente SMB se conectan con la

configuración de seguridad deseada.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea mostrar información acerca de…	Introduzca el comando…
Todas las sesiones firmados en una máquina virtual de almacenamiento (SVM) específica	`vserver cifs session show -vserver` *`vserver_name`* `-is-session-signed true`
Detalles de una sesión firmada con un ID de sesión específico en la SVM	`vserver cifs session show -vserver` *`vserver_name`* `-session-id integer -instance`

Ejemplos

El siguiente comando muestra información de sesión sobre las sesiones firmadas en la SVM vs1. El resultado de resumen predeterminado no muestra el campo de salida "'is Session Signed"':

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279 1       10.1.1.1         DOMAIN\joe          2          23s
```

El siguiente comando muestra información detallada de sesión, incluido si la sesión está firmada, en una sesión SMB con un ID de sesión de 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

Información relacionada

Supervisar estadísticas de sesión firmada por SMB

Supervisar las estadísticas de sesión firmadas por SMB de ONTAP

Es posible supervisar las estadísticas de sesiones SMB y determinar qué sesiones establecidas se han firmado y cuáles no.

Acerca de esta tarea

`statistics`El comando en el nivel de privilegio avanzado proporciona `signed_sessions` el contador que se puede utilizar para supervisar el número de sesiones SMB firmadas. El `signed_sessions` contador está disponible con los siguientes objetos de estadísticas:

- `cifs` Permite supervisar la firma SMB para todas las sesiones de SMB.
- `smb1` Permite supervisar la firma SMB para sesiones SMB 1,0.
- `smb2` Permite supervisar la firma SMB para sesiones SMB 2.x y SMB 3,0.

  Las estadísticas de SMB 3,0 se incluyen en la salida del `smb2` objeto.

Si desea comparar el Núm. De sesiones firmadas con el Núm. Total de sesiones, puede comparar la salida del `signed_sessions` contador con la salida del `established_sessions` contador.

Debe iniciar una colección de ejemplos de estadísticas para poder ver los datos resultantes. Puede ver los datos de la muestra si no detiene la recopilación de datos. Al detener la recopilación de datos, se proporciona una muestra fija. No detener la recopilación de datos le ofrece la posibilidad de obtener datos actualizados que puede utilizar para compararlos con consultas anteriores. La comparación puede ayudarle a identificar tendencias.

Pasos

1. Establezca el nivel de privilegio en AVANZADO:
   `set -privilege advanced`
2. Iniciar una recopilación de datos:
   `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Si no se especifica `-sample-id` el parámetro, el comando genera un identificador de muestra para usted y define esta muestra como la muestra predeterminada de la sesión CLI. El valor para `-sample-id` es una cadena de texto. Si ejecuta este comando durante la misma sesión de la CLI y no se especifica `-sample-id` el parámetro, el comando sobrescribe la muestra predeterminada anterior.

   Opcionalmente, puede especificar el nodo en el que se desea recoger estadísticas. Si no especifica el nodo, la muestra recopila estadísticas para todos los nodos del clúster.

   Obtenga más información sobre `statistics start` en el "Referencia de comandos del ONTAP".
3. Utilice `statistics stop` el comando para detener la recogida de datos para la muestra.

   Obtenga más información sobre `statistics stop` en el "Referencia de comandos del ONTAP" .
4. Ver estadísticas de firma SMB:

Si desea ver información acerca de…	Introduzca…
Sesiones firmadas	`show -sample-id sample_ID -counter signed_sessions
node_name [-node *node_name*]`	Sesiones firmadas y sesiones establecidas
`show -sample-id *sample_ID* -counter signed_sessions	established_sessions

   Si desea mostrar información de un solo nodo, especifique el `-node` parámetro opcional.

   Obtenga más información sobre `statistics show` en el "Referencia de comandos del ONTAP".
5. Vuelva al nivel de privilegio de administrador:
   `set -privilege admin`

Ejemplos

El siguiente ejemplo muestra cómo se pueden supervisar las estadísticas de firma de SMB 2.x y SMB 3.0 en vs1 de la máquina virtual de almacenamiento (SVM).

El siguiente comando cambia al nivel de privilegio avanzado:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

El siguiente comando inicia la recogida de datos de una nueva muestra:

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

El siguiente comando detiene la recogida de datos de la muestra:

```
cluster1::*> statistics stop -sample-id smbsigning_sample
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

El siguiente comando muestra sesiones SMB firmadas y sesiones SMB establecidas por nodo a partir de la muestra:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|established_sessions|node_name

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    established_sessions                                         0
    node_name                                                node1
    signed_sessions                                              0
    established_sessions                                         1
    node_name                                                node2
    signed_sessions                                              1
    established_sessions                                         0
    node_name                                                node3
    signed_sessions                                              0
    established_sessions                                         0
    node_name                                                node4
    signed_sessions                                              0
```

En el siguiente comando, se muestran las sesiones SMB firmadas para el nodo 2 en la muestra:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|node_name -node node2

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    node_name                                                node2
    signed_sessions                                              1
```

El siguiente comando vuelve a pasar al nivel de privilegios de administrador:

```
cluster1::*> set -privilege admin
```

Información relacionada

- Determinar si se han firmado las sesiones SMB
- "Información general sobre la gestión y el control del rendimiento"

Configurar el cifrado SMB necesario en servidores SMB para las transferencias de datos a través de SMB

Obtenga más información sobre el cifrado SMB de ONTAP

El cifrado SMB para las transferencias de datos a través de SMB es una mejora de seguridad que se puede habilitar o deshabilitar en servidores SMB. También puede configurar el valor de cifrado SMB deseado de forma compartida mediante una configuración de propiedad de recurso compartido.

De forma predeterminada, cuando crea un servidor SMB en la máquina virtual de almacenamiento (SVM), el cifrado SMB se deshabilita. Debe habilitarla para aprovechar la seguridad mejorada proporcionada por el cifrado SMB.

Para crear una sesión SMB cifrada, el cliente SMB debe admitir el cifrado SMB. Los clientes de Windows que empiezan con Windows Server 2012 y Windows 8 admiten el cifrado SMB.

El cifrado SMB en la SVM se controla mediante dos opciones de configuración:

- Una opción de seguridad del servidor SMB que habilita la funcionalidad en la SVM
- Una propiedad de recurso compartido SMB que configura la configuración de cifrado SMB de recurso compartido

Puede decidir si se requiere el cifrado para acceder a todos los datos en la SVM o si se requiere el cifrado SMB para acceder solo a los datos en recursos compartidos seleccionados. La configuración a nivel de SVM tiene preferencia en la configuración a nivel de recurso compartido.

La configuración efectiva del cifrado SMB depende de la combinación de las dos opciones y se describe en la siguiente tabla:

Cifrado SMB Server habilitado	Configuración de cifrado compartido de datos activada	Comportamiento de cifrado del servidor
Verdadero	Falso	El cifrado a nivel de servidor está habilitado para todos los recursos compartidos de la SVM. Con esta configuración, se produce el cifrado en toda la sesión SMB.
Verdadero	Verdadero	El cifrado a nivel de servidor se habilita para todos los recursos compartidos de la SVM, independientemente del cifrado a nivel de recurso compartido. Con esta configuración, se produce el cifrado en toda la sesión SMB.

Cifrado SMB Server habilitado	Configuración de cifrado compartido de datos activada	Comportamiento de cifrado del servidor
Falso	Verdadero	El cifrado a nivel de recurso compartido está habilitado para los recursos compartidos específicos. Con esta configuración, el cifrado se produce desde la conexión de árbol.
Falso	Falso	No hay ningún cifrado activado.

Los clientes SMB que no admiten cifrado no pueden conectarse a un servidor SMB o recurso compartido que requiera cifrado.

Los cambios en la configuración de cifrado surten efecto para las nuevas conexiones. Las conexiones existentes no se ven afectadas.

Obtenga información sobre el impacto en el rendimiento del cifrado de bloques de mensajes del servidor de ONTAP

Cuando las sesiones SMB utilizan el cifrado SMB, todas las comunicaciones SMB a y desde clientes de Windows experimentan un impacto en el rendimiento, lo cual afecta tanto a los clientes como al servidor (es decir, los nodos del clúster que ejecuta la SVM que contiene el servidor SMB).

El impacto en el rendimiento muestra que el uso de CPU ha aumentado tanto en los clientes como en el servidor, aunque la cantidad de tráfico de red no cambia.

La magnitud del impacto en el rendimiento depende de la versión de ONTAP 9 que esté ejecutando. A partir de ONTAP 9.7, un nuevo algoritmo de descarga del cifrado puede permitir un mejor rendimiento en el tráfico SMB cifrado. La descarga de cifrado SMB se habilita de forma predeterminada cuando se habilita el cifrado SMB.

El rendimiento del cifrado SMB mejorado requiere la capacidad de descarga de AES-ni. Consulte el Hardware Universe (HWU) para verificar que la descarga AES-ni es compatible con su plataforma.

Otras mejoras de rendimiento también son posibles si usted es capaz de utilizar SMB versión 3,11 que admite el algoritmo GCM mucho más rápido.

Según la red, la versión de ONTAP 9, la versión de SMB y la implementación de SVM, el impacto en el rendimiento del cifrado SMB puede variar enormemente; puede verificarlo únicamente mediante pruebas en su entorno de red.

El cifrado SMB está deshabilitado de forma predeterminada en el servidor SMB. Debe habilitar el cifrado SMB solo en aquellos recursos compartidos SMB o servidores SMB que requieran cifrado. Con el cifrado SMB, ONTAP realiza un procesamiento adicional de descifrar las solicitudes y cifrar las respuestas para cada solicitud. Por tanto, el cifrado SMB solo debe habilitarse cuando sea necesario.

Habilite o deshabilite el cifrado SMB de ONTAP para el tráfico entrante

Si desea requerir el cifrado SMB para el tráfico SMB entrante puede habilitarla en el

servidor CIFS o en el nivel de recurso compartido. De manera predeterminada, no es necesario el cifrado SMB.

Acerca de esta tarea

Puede habilitar el cifrado SMB en el servidor CIFS, que se aplica a todos los recursos compartidos del servidor CIFS. Si no desea usar el cifrado SMB necesario para todos los recursos compartidos en el servidor CIFS o si desea habilitar el cifrado SMB necesario para el tráfico SMB entrante de acuerdo con recurso compartido por recurso, puede deshabilitar el cifrado SMB requerido en el servidor CIFS.

Cuando se configura una relación de recuperación ante desastres de una máquina virtual de almacenamiento (SVM), el valor que selecciona para `-identity-preserve` la opción del `snapmirror create` comando determina los detalles de configuración que se replican en la SVM de destino.

Si establece `-identity-preserve` la opción en `true` (ID-preserve), la configuración de seguridad de cifrado SMB se replica en el destino.

Si establece `-identity-preserve` la opción en `false` (non-ID-preserve), la configuración de seguridad de cifrado SMB no se replica en el destino. En este caso, la configuración de seguridad del servidor CIFS en el destino se establece en los valores predeterminados. Si ha habilitado el cifrado SMB en la SVM de origen, debe habilitar manualmente el cifrado SMB del servidor CIFS en el destino.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea que el cifrado SMB para el tráfico SMB entrante en el servidor CIFS sea…	Introduzca el comando…
Activado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required true`
Deshabilitado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required false`

2. Compruebe que el cifrado SMB necesario en el servidor CIFS está habilitado o deshabilitado como desee: `vserver cifs security show -vserver` *`vserver_name`* `-fields is-smb-encryption-required`

```
`is-smb-encryption-required`El campo muestra `true` si el cifrado SMB
necesario está habilitado en el servidor CIFS y `false` si está
deshabilitado.
```

Ejemplo

En el ejemplo siguiente se habilita el cifrado SMB requerido para el tráfico SMB entrante para el servidor CIFS en la SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

Información relacionada

- "snapmirror create"

Determine si los clientes están conectados mediante sesiones SMB de ONTAP cifradas

Puede mostrar información sobre las sesiones SMB conectadas para determinar si los clientes están utilizando conexiones SMB cifradas. Esto puede resultar útil para determinar si las sesiones de cliente SMB se conectan con la configuración de seguridad deseada.

Acerca de esta tarea

Las sesiones de clientes de SMB pueden tener uno de tres niveles de cifrado:

- `unencrypted`

  La sesión SMB no está cifrada. No se configura ni el cifrado a nivel de equipo virtual de almacenamiento (SVM) ni el nivel de recurso compartido.

- `partially-encrypted`

  El cifrado se inicia cuando se produce la conexión de árbol. Se configuró el cifrado a nivel de recurso compartido. El cifrado a nivel de SVM no está habilitado.

- `encrypted`

  La sesión SMB está totalmente cifrada. El cifrado de la SVM está habilitado. Es posible que el cifrado de nivel de recurso compartido esté habilitado o no. La configuración de cifrado a nivel de SVM sustituye la configuración de cifrado a nivel de recurso compartido.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea mostrar información acerca de…	Introduzca el comando…
Sesiones con una configuración de cifrado especificada para sesiones en una SVM especificada	`vserver cifs session show -vserver *vserver_name* {unencrypted
partially-encrypted	encrypted} -instance`

Si desea mostrar información acerca de…	Introduzca el comando…
La configuración de cifrado para un ID de sesión específico en una SVM especificada	`vserver cifs session show -vserver` *`vserver_name`* `-session-id` *`integer`* `-instance`

Ejemplos

El siguiente comando muestra información detallada de la sesión, incluida la configuración de cifrado, en una sesión SMB con un ID de sesión de 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                Open Shares: 1
                 Open Files: 1
                 Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

Supervise las estadísticas de cifrado del bloque de mensajes del servidor de ONTAP

Es posible supervisar las estadísticas de cifrado SMB y determinar qué sesiones establecidas y conexiones de uso compartido están cifradas y cuáles no lo están.

Acerca de esta tarea

`statistics`El comando en el nivel de privilegios avanzados proporciona los siguientes contadores, que puede utilizar para supervisar el número de sesiones SMB cifradas y conexiones compartidas:

Nombre del contador	Descripciones
`encrypted_sessions`	Proporciona el número de sesiones cifradas SMB 3.0
`encrypted_share_connections`	Proporciona el número de recursos compartidos cifrados en los que se ha producido una conexión de árbol
`rejected_unencrypted_sessions`	Da el número de configuraciones de sesión rechazadas debido a la falta de capacidad de cifrado del cliente
`rejected_unencrypted_shares`	Proporciona el número de asignaciones de recursos compartidos rechazadas debido a la falta de capacidad de cifrado del cliente

Estos contadores están disponibles con los siguientes objetos de estadísticas:

- `cifs` Permite supervisar el cifrado SMB para todas las sesiones de SMB 3,0.

  Las estadísticas de SMB 3,0 se incluyen en la salida del `cifs` objeto. Si desea comparar el Núm. De sesiones cifradas con el Núm. Total de sesiones, puede comparar la salida del `encrypted_sessions` contador con la salida del `established_sessions` contador.

  Si desea comparar el número de conexiones compartidas cifradas con el número total de conexiones compartidas, puede comparar la salida del `encrypted_share_connections` contador con la salida del contador `connected_shares`.

- `rejected_unencrypted_sessions` Proporciona la cantidad de veces que se ha intentado establecer una sesión SMB que requiere cifrado de un cliente que no admite cifrado SMB.
- `rejected_unencrypted_shares` Proporciona la cantidad de veces que se ha intentado conectarse a un recurso compartido SMB que requiere cifrado de un cliente que no admite cifrado SMB.

Debe iniciar una colección de ejemplos de estadísticas para poder ver los datos resultantes. Puede ver los datos de la muestra si no detiene la recopilación de datos. Al detener la recopilación de datos, se proporciona una muestra fija. No detener la recopilación de datos le ofrece la posibilidad de obtener datos actualizados que puede utilizar para compararlos con consultas anteriores. La comparación puede ayudarle a identificar tendencias.

Pasos

1. Establezca el nivel de privilegio en AVANZADO:
   `set -privilege advanced`
2. Iniciar una recopilación de datos:
   `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Si no se especifica `-sample-id` el parámetro, el comando genera un identificador de muestra para usted y define esta muestra como la muestra predeterminada de la sesión CLI. El valor para `-sample-id` es una cadena de texto. Si ejecuta este comando durante la misma sesión de la CLI y no se especifica `-sample-id` el parámetro, el comando sobrescribe la muestra predeterminada anterior.

Opcionalmente, puede especificar el nodo en el que se desea recoger estadísticas. Si no especifica el nodo, la muestra recopila estadísticas para todos los nodos del clúster.

Obtenga más información sobre `statistics start` en el "Referencia de comandos del ONTAP".

3. Utilice `statistics stop` el comando para detener la recogida de datos para la muestra.

   Obtenga más información sobre `statistics stop` en el "Referencia de comandos del ONTAP" .

4. Ver estadísticas de cifrado SMB:

Si desea ver información acerca de…	**Introduzca…**
Sesiones cifradas	`show -sample-id *sample_ID* -counter encrypted_sessions
node_name [-node *node_name*]`	Sesiones cifradas y sesiones establecidas
`show -sample-id *sample_ID* -counter encrypted_sessions	established_sessions
node_name [-node *node_name*]`	Conexiones de recursos compartidos cifradas
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`
Conexiones de recursos compartidos cifradas y recursos compartidos conectados	`show -sample-id *sample_ID* -counter encrypted_share_connections
connected_shares	*node_name* [-node *node_name*]`
Sesiones no cifradas rechazadas	`show -sample-id *sample_ID* -counter rejected_unencrypted_sessions
node_name [-node *node_name*]`	Se han rechazado conexiones compartidas sin cifrar
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

   Si desea mostrar información solo de un solo nodo, especifique el `-node` parámetro opcional.

   Obtenga más información sobre `statistics show` en el "Referencia de comandos del ONTAP".

5. Vuelva al nivel de privilegio de administrador:
   `set -privilege admin`

Ejemplos

El ejemplo siguiente muestra cómo se pueden supervisar las estadísticas de cifrado de SMB 3.0 en vs1 de la máquina virtual de almacenamiento (SVM).

El siguiente comando cambia al nivel de privilegio avanzado:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

El siguiente comando inicia la recogida de datos de una nueva muestra:

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

El siguiente comando detiene la recogida de datos de esa muestra:

```
cluster1::*> statistics stop -sample-id smbencryption_sample
Statistics collection is being stopped for Sample-id:
smbencryption_sample
```

El siguiente comando muestra sesiones SMB cifradas y sesiones SMB establecidas por el nodo a partir de la muestra:

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2

    Counter                                 Value
    ----------------------------  ----------------------
    established_sessions                       1
    encrypted_sessions                         1

2 entries were displayed
```

El siguiente comando muestra el número de sesiones SMB no cifradas rechazadas por el nodo a partir de la muestra:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2

    Counter                                     Value
    ----------------------------    ----------------------
    rejected_unencrypted_sessions                 1

1 entry was displayed.
```

El siguiente comando muestra el número de recursos compartidos de SMB conectados y recursos compartidos de SMB cifrados mediante el nodo de la muestra:

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

    Counter                                     Value
    --------------------------    ----------------------
    connected_shares                              2
    encrypted_share_connections                   1

2 entries were displayed.
```

El siguiente comando muestra el número de conexiones de recursos compartidos SMB no cifradas rechazadas por el nodo a partir de la muestra:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

    Counter                                     Value
    -------------------------------    ----------------------
    rejected_unencrypted_shares                   1

1 entry was displayed.
```

Información relacionada

- Determinar qué estadísticas, objetos y contadores están disponibles en los servidores
- "Información general sobre la gestión y el control del rendimiento"

Comunicación segura de sesiones LDAP

Obtenga más información sobre la firma y el sellado LDAP en el bloque de mensajes del servidor ONTAP

A partir de ONTAP 9, puede configurar la firma y el sellado para habilitar la seguridad de

la sesión LDAP en consultas a un servidor de Active Directory (AD). Debe configurar los ajustes de seguridad del servidor CIFS en la máquina virtual de almacenamiento (SVM) para corresponder a los del servidor LDAP.

La firma comprueba la integridad de la carga de datos LDAP mediante una tecnología de clave secreta. El sellado cifra la carga de datos LDAP para impedir la transmisión de información confidencial en texto sin cifrar. Una opción *LDAP Security Level* indica si es necesario firmar, firmar y sellar el tráfico LDAP o no. El valor predeterminado es `none`.

La firma y el sellado LDAP en el tráfico CIFS están habilitados en la SVM con `-session-security-for-ad-ldap` la opción para `vserver cifs security modify` el comando.

Habilite la firma y el sellado LDAP en los servidores SMB de ONTAP

Antes de que el servidor CIFS pueda utilizar la firma y el sellado para establecer una comunicación segura con un servidor LDAP de Active Directory, debe modificar la configuración de seguridad del servidor CIFS para habilitar la firma y el sellado LDAP.

Antes de empezar

Debe consultar al administrador del servidor AD para determinar los valores de configuración de seguridad adecuados.

Pasos

1. Configure las opciones de seguridad del servidor CIFS que permitan el tráfico firmado y sellado con servidores LDAP de Active Directory: `vserver cifs security modify -vserver` *`vserver_name`* `-session-security-for-ad-ldap {none|sign|seal}`

   Puede activar la firma (`sign`, integridad de datos), la firma y el sellado (`seal`, la integridad y el cifrado de los datos), o ninguno `none`, sin firma ni sellado). El valor predeterminado es `none`.

2. Compruebe que la configuración de seguridad de firma y sellado LDAP se ha definido correctamente: `vserver cifs security show -vserver` *`vserver_name`*

> Si la SVM utiliza el mismo servidor LDAP para consultar la asignación de nombres u otra información de UNIX, como usuarios, grupos y netgroups, debe habilitar la configuración correspondiente con `-session-security` la opción `vserver services name-service ldap client modify` del comando.

Configure LDAP sobre TLS

Exporte certificados de CA raíz autofirmados para las SVM SMB de ONTAP

Para utilizar LDAP sobre SSL/TLS para proteger la comunicación de Active Directory, primero debe exportar una copia del certificado raíz autofirmado del Servicio de certificados de Active Directory a un archivo de certificado y convertirlo en un archivo de texto ASCII. ONTAP utiliza este archivo de texto para instalar el certificado en la máquina virtual de almacenamiento (SVM).

Antes de empezar

El servicio de certificados de Active Directory ya debe estar instalado y configurado para el dominio al que

pertenece el servidor CIFS. Puede encontrar información acerca de la instalación y configuración de Active Director Certificate Services consultando la biblioteca de Microsoft TechNet.

"Biblioteca de Microsoft TechNet: technet.microsoft.com"

Paso

1. Obtenga un certificado de CA raíz del controlador de dominio en `.pem` formato de texto.

   "Biblioteca de Microsoft TechNet: technet.microsoft.com"

Después de terminar

Instale el certificado en la SVM.

Información relacionada

"Biblioteca de Microsoft TechNet"

Instale los certificados de CA raíz autofirmados en la SVM SMB de ONTAP

Si se requiere la autenticación LDAP con TLS al enlazar con servidores LDAP, primero debe instalar el certificado de CA raíz autofirmado en la SVM.

Acerca de esta tarea

Todas las aplicaciones de ONTAP que utilizan comunicaciones TLS pueden comprobar el estado del certificado digital mediante el protocolo de estado de certificado en línea (OCSP). Si OCSP está habilitado para LDAP over TLS, se rechazan los certificados revocados y la conexión falla.

Pasos

1. Instale el certificado de CA raíz autofirmado:
   a. Comience la instalación del certificado: `security certificate install -vserver vserver_name -type server-ca`

      La salida de la consola muestra el siguiente mensaje: `Please enter Certificate: Press <Enter> when done`

   b. Abra el `.pem` archivo de certificado con un editor de texto, copie el certificado, incluidas las líneas que empiezan por `-----BEGIN CERTIFICATE-----` y terminan por y `-----END CERTIFICATE-----`, a continuación, pegue el certificado después del símbolo del sistema.
   c. Compruebe que el certificado se muestra correctamente.
   d. Para completar la instalación, pulse Intro.
2. Compruebe que el certificado está instalado: `security certificate show -vserver vserver_name`

Información relacionada

- "instalación del certificado de seguridad"
- "Mostrar certificado de seguridad"

Habilite LDAP over TLS en el servidor SMB de ONTAP

Antes de que el servidor SMB pueda utilizar TLS para obtener comunicación segura con

un servidor LDAP de Active Directory, debe modificar la configuración de seguridad del servidor SMB para habilitar LDAP over TLS.

A partir de ONTAP 9.10.1, el enlace de canal LDAP se admite de forma predeterminada tanto para las conexiones LDAP de Active Directory (AD) como de los servicios de nombres. ONTAP intentará establecer la vinculación de canal con las conexiones LDAP solo si Start-TLS o LDAPS está habilitado junto con la seguridad de la sesión establecida en Sign o Seal. Para deshabilitar o volver a habilitar el enlace de canal LDAP con los servidores AD, utilice `-try-channel-binding-for-ad-ldap` el parámetro con `vserver cifs security modify` el comando.

Para obtener más información, consulte:

- "Obtenga más información sobre LDAP para SVM NFS de ONTAP"
- "2020 requisitos de enlace de canal LDAP y firma LDAP para Windows".

Pasos

1. Configure los ajustes de seguridad del servidor SMB que permitan una comunicación LDAP segura con los servidores LDAP de Active Directory: `vserver cifs security modify -vserver` *`vserver_name`* `-use-start-tls-for-ad-ldap true`
2. Compruebe que la configuración de seguridad LDAP over TLS está establecida en `true`: `vserver cifs security show -vserver` *`vserver_name`*

> Si la SVM utiliza el mismo servidor LDAP para consultar la asignación de nombres u otra información de UNIX (como usuarios, grupos y netgroups), también debe modificar la `-use -start-tls` opción mediante `vserver services name-service ldap client modify` el comando.

Configurar ONTAP SMB Multicanal para el rendimiento y la redundancia

A partir de ONTAP 9.4, puede configurar SMB MultiChannel para proporcionar varias conexiones entre ONTAP y clientes en una sola sesión SMB. Al hacerlo, se mejora el rendimiento y la tolerancia a fallos.

Antes de empezar

Solo se puede utilizar la funcionalidad multicanal de SMB cuando los clientes negocian en SMB 3.0 o versiones posteriores. De forma predeterminada, SMB 3.0 y las versiones posteriores se encuentran habilitadas en el servidor SMB de ONTAP.

Acerca de esta tarea

Los clientes de SMB detectan y utilizan automáticamente varias conexiones de red si se identifica una configuración adecuada en el clúster de ONTAP.

El número de conexiones simultáneas en una sesión SMB depende de las NIC que haya implementado:

- **1G NIC en el cluster ONTAP y cliente**

  El cliente establece una conexión por NIC y enlaza la sesión a todas las conexiones.

- **NIC 10G y mayor capacidad en cluster ONTAP** y cliente

  El cliente establece hasta cuatro conexiones por NIC y enlaza la sesión a todas las conexiones. El cliente

puede establecer conexiones en varias NIC de 10 G y de mayor capacidad.

También puede modificar los siguientes parámetros (privilegios avanzados):

- `-max-connections-per-session`

  El número máximo de conexiones permitidas por sesión multicanal. El valor predeterminado es 32 conexiones.

  Si desea habilitar más conexiones que las predeterminadas, debe realizar ajustes comparables a la configuración del cliente, que también tiene un valor predeterminado de 32 conexiones.

- `-max-lifs-per-session`

  Número máximo de interfaces de red anunciadas por sesión multicanal. El valor predeterminado es 256 interfaces de red.

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Habilite multicanal de SMB en el servidor SMB:

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. Compruebe que ONTAP informa de sesiones multicanal de SMB:

```
vserver cifs session show
```

4. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Ejemplo

En el siguiente ejemplo, se muestra información sobre todas las sesiones SMB, donde se muestran varias conexiones para una sola sesión:

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User         Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

En el siguiente ejemplo, se muestra información detallada sobre una sesión SMB con el ID de sesión 1:

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                          Node: node1
                    Session ID: 1
                Connection IDs: 138683,138684,138685
              Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
       Workstation IP Address: 10.1.1.1
      Authentication Mechanism: NTLMv1
         User Authenticated as: domain-user
                  Windows User: DOMAIN\administrator
                     UNIX User: root
                   Open Shares: 2
                    Open Files: 5
                    Open Other: 0
                Connected Time: 5s
                     Idle Time: 5s
              Protocol Version: SMB3
        Continuously Available: No
             Is Session Signed: false
                  NetBIOS Name: -
```

Configurar los mapas de usuario UNIX predeterminados de usuario de Windows en el servidor SMB

Configure el usuario UNIX SMB de ONTAP predeterminado

Puede configurar el usuario UNIX predeterminado para que lo utilice si fallan todos los demás intentos de asignación para un usuario o si no desea asignar usuarios individuales entre UNIX y Windows. De manera alternativa, si desea que la autenticación de usuarios no asignados falle, no debe configurar el usuario UNIX predeterminado.

Acerca de esta tarea

De forma predeterminada, el nombre del usuario UNIX predeterminado es "'pcuser'", lo que significa que, de forma predeterminada, se activa la asignación de usuarios al usuario UNIX predeterminado. Puede especificar otro nombre que se utilizará como usuario UNIX predeterminado. El nombre que especifique debe existir en las bases de datos del servicio de nombres configuradas para la máquina virtual de almacenamiento (SVM). Si esta opción está establecida en una cadena nula, nadie puede acceder al servidor CIFS como usuario predeterminado de UNIX. Es decir, cada usuario debe tener una cuenta en la base de datos de contraseñas para poder acceder al servidor CIFS.

Para que un usuario pueda conectarse al servidor CIFS con la cuenta de usuario UNIX predeterminada, el usuario debe cumplir los siguientes requisitos previos:

- El usuario se autentica.
- El usuario se encuentra en la base de datos de usuarios Windows local del servidor CIFS, en el dominio principal del servidor CIFS o en un dominio de confianza (si las búsquedas de asignación de nombres multidominio están activadas en el servidor CIFS).
- El nombre de usuario no se asigna explícitamente a una cadena nula.

Pasos

1. Configure el usuario UNIX predeterminado:

Si desea …	Introduzca …
Utilizar el usuario UNIX predeterminado "'pcuser'"	`vserver cifs options modify -default -unix-user pcuser`
Utilice otra cuenta de usuario UNIX como usuario predeterminado	`vserver cifs options modify -default -unix-user` *`user_name`*
Desactive el usuario UNIX predeterminado	`vserver cifs options modify -default -unix-user ""`

```
vserver cifs options modify -default-unix-user pcuser
```

2. Compruebe que el usuario UNIX predeterminado está configurado correctamente: `vserver cifs options show -vserver` *`vserver_name`*

   En el siguiente ejemplo, tanto el usuario UNIX predeterminado como el usuario UNIX invitado en SVM vs1 están configurados para utilizar el usuario UNIX "'pcuser'":

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : pcuser
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

Configure el usuario UNIX SMB de ONTAP invitado

Configurar la opción de usuario UNIX invitado significa que los usuarios que inician sesión desde dominios que no son de confianza se asignan al usuario UNIX invitado y pueden conectarse al servidor CIFS. Como alternativa, si desea que la autenticación de usuarios de dominios que no son de confianza falle, no debe configurar el usuario UNIX invitado. El valor predeterminado es no permitir que los usuarios de dominios que no son de confianza se conecten al servidor CIFS (la cuenta UNIX invitada no está configurada).

Acerca de esta tarea

Debe tener en cuenta lo siguiente al configurar la cuenta de UNIX de invitado:

- Si el servidor CIFS no puede autenticar al usuario en un controlador de dominio para el dominio principal, un dominio de confianza o la base de datos local y esta opción está habilitada, el servidor CIFS considera al usuario como un usuario invitado y lo asigna al usuario UNIX especificado.
- Si esta opción se establece en una cadena nula, el usuario UNIX invitado estará deshabilitado.
- Debe crear un usuario UNIX para usarlo como usuario UNIX invitado en una de las bases de datos del servicio de nombres de máquina virtual de almacenamiento (SVM).
- Un usuario que inició sesión como usuario invitado es automáticamente miembro del grupo BUILTIN\guest en el servidor CIFS.
- La opción 'homedrs-public' se aplica sólo a los usuarios autenticados. Un usuario que ha iniciado sesión como usuario invitado no tiene un directorio principal y no puede acceder a los directorios principales de otros usuarios.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca…
Configure el usuario UNIX invitado	`vserver cifs options modify -guest -unix-user` *`unix_name`*
Deshabilite el usuario UNIX invitado	`vserver cifs options modify -guest -unix-user ""`

```
vserver cifs options modify -guest-unix-user pcuser
```

2. Compruebe que el usuario UNIX invitado está configurado correctamente: `vserver cifs options show -vserver vserver_name`

   En el siguiente ejemplo, tanto el usuario UNIX predeterminado como el usuario UNIX invitado en SVM vs1 están configurados para utilizar el usuario UNIX "'pcuser'":

   ```
   vserver cifs options show -vserver vs1
   ```

   ```
   Vserver: vs1

     Client Session Timeout : 900
     Default Unix Group     : -
     Default Unix User      : pcuser
     Guest Unix User        : pcuser
     Read Grants Exec       : disabled
     Read Only Delete       : disabled
     WINS Servers           : -
   ```

Asigne los grupos de administrador a la raíz de SMB de ONTAP

Si solo tiene clientes CIFS en su entorno y su máquina virtual de almacenamiento (SVM) está configurada como un sistema de almacenamiento multiprotocolo, debe tener al menos una cuenta de Windows con privilegios raíz para acceder a los archivos en la SVM; De lo contrario, no puede gestionar la SVM porque no tiene suficientes derechos de usuario.

Acerca de esta tarea

Si el sistema de almacenamiento se configuró como solo NTFS, `/etc` el directorio tiene una ACL en el nivel de archivos que permite que el grupo de administradores acceda a los archivos de configuración de ONTAP.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Configure la opción del servidor CIFS que asigna el grupo de administradores a la raíz, según corresponda:

Si desea…	Realice lo siguiente…
Asigne los miembros del grupo de administradores a la raíz	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled true` Todas las cuentas del grupo de administradores se consideran raíz, incluso si no tiene una `/etc/usermap.cfg` entrada que asigne las cuentas a raíz. Si crea un archivo utilizando una cuenta que pertenece al grupo de administradores, el archivo es propiedad de root cuando ve el archivo desde un cliente UNIX.
Desactive la asignación de los miembros del grupo de administradores a la raíz	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled false` Las cuentas del grupo de administradores ya no se asignan a raíz. Sólo se puede asignar explícitamente un solo usuario a la raíz.

3. Compruebe que la opción está establecida en el valor deseado: `vserver cifs options show -vserver` *`vserver_name`*
4. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Mostrar información sobre los tipos de usuarios que están conectados en sesiones SMB de ONTAP

Puede ver información acerca del tipo de usuarios que están conectados en sesiones SMB. Esto puede ayudarle a asegurarse de que solo el tipo adecuado de usuario se conecte a través de sesiones SMB en la máquina virtual de almacenamiento (SVM).

Acerca de esta tarea

Los siguientes tipos de usuarios pueden conectarse a través de sesiones SMB:

- `local-user`

  Se autentica como usuario CIFS local

- `domain-user`

  Autenticado como usuario de dominio (ya sea desde el dominio principal del servidor CIFS o desde un dominio de confianza)

- `guest-user`

  Autenticado como usuario invitado

- `anonymous-user`

  Autenticado como usuario anónimo o nulo

Pasos

1. Determine qué tipo de usuario está conectado en una sesión SMB: `vserver cifs session show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type`

Si desea mostrar información sobre tipos de usuario para las sesiones establecidas…	Introduzca el siguiente comando…
Para todas las sesiones con un tipo de usuario especificado	`vserver cifs session show -vserver *vserver_name* -user-type {local-user
domain-user	guest-user
anonymous-user}`	Para un usuario específico

Ejemplos

El siguiente comando muestra información de sesión sobre el tipo de usuario para las sesiones en SVM vs1 establecidas por el usuario "' iepubs\user1"':

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node      vserver session-id connection-id lif-address  address
windows-user         user-type
--------- ------- ---------- ------------- ------------ -------------
-------------------- -----------
pub1node1 pub1    1          3439441860    10.0.0.1     10.1.1.1
IEPUBS\user1         domain-user
```

Opciones de comando de ONTAP para limitar el consumo excesivo de recursos de cliente de Windows

Las opciones que incluyen `vserver cifs options modify` el comando le permiten controlar el consumo de recursos de los clientes de Windows. Esto puede ser útil si algún cliente está fuera de los límites normales del consumo de recursos, por ejemplo, si hay un número inusualmente alto de archivos abiertos, sesiones abiertas o peticiones de notificación de cambio.

```
`vserver cifs options modify`Se han agregado las siguientes opciones al
comando para controlar el consumo de recursos del cliente de Windows. Si
se supera el valor máximo de cualquiera de estas opciones, se deniega la
solicitud y se envía un mensaje EMS. También se envía un mensaje de
advertencia EMS cuando se alcanza el 80 % del límite configurado para
estas opciones.
```

- `-max-opens-same-file-per-tree`

  Número máximo de apertura en el mismo archivo por árbol CIFS

- `-max-same-user-sessions-per-connection`

  Número máximo de sesiones abiertas por el mismo usuario por conexión

- `-max-same-tree-connect-per-session`

  Número máximo de conexiones de árbol en el mismo recurso compartido por sesión

- `-max-watches-set-per-tree`

  Número máximo de relojes (también conocido como *change notifics*) establecido por árbol

Obtenga más información sobre `vserver cifs options modify` en el "Referencia de comandos del ONTAP".

A partir de ONTAP 9.4, los servidores que ejecutan SMB versión 2 o posterior pueden limitar el número de solicitudes pendientes (*créditos SMB*) que el cliente puede enviar al servidor en una conexión SMB. La gestión de créditos SMB es iniciada por el cliente y controlada por el servidor.

La `-max-credits` opción controla el número máximo de solicitudes pendientes que se pueden otorgar en una conexión SMB. El valor predeterminado de esta opción es 128.

Mejore el rendimiento del cliente con los bloqueos oportunistas tradicionales y de arrendamiento

Obtenga información sobre cómo mejorar el rendimiento del cliente de bloque de mensajes del servidor de ONTAP con los bloqueos oportunistas de arrendamiento tradicionales

Los bloqueos oportunistas tradicionales (bloqueos oportunistas oportunistas oportunistas) y los bloqueos oportunistas de arrendamiento habilitan un cliente SMB en determinados escenarios de uso compartido de archivos para realizar el almacenamiento en caché en el lado del cliente de información de lectura anticipada, escritura subyacente y bloqueo. A continuación, un cliente puede leer o escribir en un archivo sin recordar periódicamente al servidor que necesita acceso al archivo en cuestión. Esto mejora el rendimiento al reducir el tráfico de red.

Los bloqueos oportunistas del arrendamiento son una forma mejorada de bloqueos oportunistas disponibles con el protocolo SMB 2.1 y versiones posteriores. Los bloqueos oportunistas de arrendamiento permiten a un cliente obtener y conservar el estado de almacenamiento en caché del cliente en múltiples abiertos de SMB originados por sí mismo.

Los bloqueos oportunistas pueden controlarse de dos formas:

- Mediante una propiedad de recurso compartido, utilizando el `vserver cifs share create` comando cuando se crea el recurso compartido, o el `vserver share properties` comando después de la creación.
- Mediante una propiedad de qtree, el uso `volume qtree create` del comando cuando se crea el qtree, o `volume qtree oplock` los comandos después de su creación.

Obtenga más información sobre la escritura de consideraciones sobre pérdida de datos en la caché del bloque de mensajes del servidor de ONTAP cuando se utilizan bloqueos oportunistas

En determinadas circunstancias, si un proceso tiene un oplock exclusivo en un archivo y

un segundo proceso intenta abrir el archivo, el primer proceso debe invalidar los datos almacenados en caché y vaciar las escrituras y los bloqueos. A continuación, el cliente debe renunciar al oplock y acceder al archivo. Si hay un fallo de red durante este vaciado, se pueden perder los datos de escritura en caché.

- Posibilidades de pérdida de datos

  Cualquier aplicación que tenga datos en la caché de la escritura puede perder esos datos en el siguiente conjunto de circunstancias:

  - La conexión se realiza mediante SMB 1.0.
  - Tiene un oplock exclusivo en el archivo.
  - Se le indica que rompa ese oplock o cierre el archivo.
  - Durante el proceso de vaciado de la caché de escritura, la red o el sistema de destino genera un error.
- Gestión de errores y finalización de escritura

  La caché en sí no tiene ninguna gestión de errores. Las aplicaciones sí. Cuando la aplicación escribe en la caché, la escritura siempre se completa. Si la caché, a su vez, realiza una escritura en el sistema de destino a través de una red, debe asumir que la escritura se completa porque, si no lo hace, los datos se pierden.

Habilite o deshabilite los bloqueos oportunistas al crear recursos compartidos de SMB de ONTAP

Los bloqueos oportunistas permiten a los clientes bloquear archivos y contenido de la caché localmente, lo que puede aumentar el rendimiento de las operaciones de archivos. Los bloqueos oportunistas están habilitados en los recursos compartidos de SMB que residen en máquinas virtuales de almacenamiento (SVM). En algunas circunstancias, es posible que desee deshabilitar los bloqueos oportunistas. Puede habilitar o deshabilitar los bloqueos oportunistas de acuerdo con el recurso compartido por recurso compartido.

Acerca de esta tarea

Si los bloqueos oportunistas están habilitados en el volumen que contiene un recurso compartido pero la propiedad de recurso compartido de oplock para ese recurso compartido está deshabilitada, los bloqueos oportunistas se deshabilitan para ese recurso compartido. La deshabilitación de los bloqueos oportunistas en un recurso compartido tiene prioridad sobre la configuración de oplock de volumen. Al deshabilitar los bloqueos oportunistas del recurso compartido, se deshabilitan los bloqueos oportunistas oportunistas de arrendamiento y oportunistas.

Puede especificar otras propiedades de recursos compartidos además de especificar la propiedad de recursos compartidos de oplock mediante una lista delimitada por comas. También puede especificar otros parámetros de recursos compartidos.

Pasos

1. Realice la acción correspondiente:

Si desea…	Realice lo siguiente…
Habilite los bloqueos oportunistas del recurso compartido durante la creación de recursos compartidos	Introduzca el siguiente comando: `vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]` Si desea que el recurso compartido tenga sólo las propiedades de recurso compartido por defecto, que son `oplocks` `browsable` , y `changenotify` están activadas, no es necesario especificar el `-share-properties` parámetro al crear un recurso compartido SMB. Si desea una combinación de propiedades de recurso compartido que no sea la predeterminada, debe especificar el `-share-properties` parámetro con la lista de propiedades de recurso compartido que se utilizará para ese recurso compartido.
Deshabilite los bloqueos oportunistas del recurso compartido durante la creación de recursos compartidos	Introduzca el siguiente comando: `vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]` Al desactivar los bloqueos oportunistas, debe especificar una lista de propiedades de recurso compartido al crear el recurso compartido, pero no debe especificar la `oplocks` propiedad.

Información relacionada

Habilite o deshabilite los bloqueos oportunistas en los recursos compartidos de SMB existentes

Controlar el estado del plock

Comandos de ONTAP para habilitar o deshabilitar los bloqueos oportunistas en volúmenes y qtrees de SMB

Los bloqueos oportunistas permiten a los clientes bloquear archivos y contenido de la caché localmente, lo que puede aumentar el rendimiento de las operaciones de archivos. Debe conocer los comandos para habilitar o deshabilitar los bloqueos oportunistas en volúmenes o qtrees. También debe saber cuándo puede habilitar o deshabilitar los bloqueos oportunistas de los volúmenes y qtrees.

- Los bloqueos oportunistas están habilitados en los volúmenes de forma predeterminada.
- No se pueden deshabilitar los bloqueos oportunistas cuando crea un volumen.
- Puede habilitar o deshabilitar los bloqueos oportunistas de los volúmenes existentes de las SVM en cualquier momento.
- Puede habilitar los bloqueos oportunistas en qtrees para SVM.

  La configuración del modo oplock es una propiedad del ID de qtree 0, el qtree predeterminado que tienen todos los volúmenes. Si no se especifica una configuración de oplock al crear un qtree, el qtree hereda la configuración oplock del volumen principal, que se habilita de forma predeterminada. Sin embargo, si se especifica una configuración de oplock en el nuevo qtree, tendrá prioridad sobre la configuración de oplock en el volumen.

Si desea…	Se usa este comando…
Habilite los bloqueos oportunistas en volúmenes o qtrees	`volume qtree oplocks` con el `-oplock-mode` parámetro establecido en `enable`
Deshabilite los bloqueos oportunistas en volúmenes o qtrees	`volume qtree oplocks` con el `-oplock-mode` parámetro establecido en `disable`

Información relacionada

Controlar el estado del plock

Habilite o deshabilite los bloqueos oportunistas en recursos compartidos de SMB de ONTAP existentes

Los bloqueos oportunistas están habilitados en recursos compartidos de SMB en máquinas virtuales de almacenamiento (SVM) de forma predeterminada. En algunas circunstancias, puede que desee deshabilitar los bloqueos oportunistas; de forma alternativa, si ha deshabilitado los bloqueos oportunistas en un recurso compartido anteriormente, puede que desee volver a habilitar los bloqueos oportunistas.

Acerca de esta tarea

Si los bloqueos oportunistas están habilitados en el volumen que contiene un recurso compartido, pero la propiedad de recurso compartido oplock de ese recurso compartido está deshabilitada, los bloqueos oportunistas se deshabilitan para ese recurso compartido. La deshabilitación de los bloqueos oportunistas en un recurso compartido tiene prioridad sobre el hecho de habilitar los bloqueos oportunistas en el volumen. Al deshabilitar los bloqueos oportunistas del recurso compartido, se deshabilitan los bloqueos oportunistas oportunistas de arrendamiento y oportunistas. Puede habilitar o deshabilitar los bloqueos oportunistas de los recursos compartidos existentes en cualquier momento.

Paso

1. Realice la acción correspondiente:

Si desea…	Realice lo siguiente…
Habilite los bloqueos oportunistas del recurso compartido modificando un recurso compartido existente	Introduzca el siguiente comando: `vserver cifs share properties add -vserver` *`vserver_name`* `-share-name share_name -share-properties oplocks` Puede especificar propiedades de recursos compartidos adicionales que desea agregar mediante una lista delimitada por comas. Las propiedades recién agregadas se agregan a la lista existente de propiedades de recursos compartidos. Todas las propiedades de recurso compartido que haya especificado anteriormente permanecen vigentes.
Deshabilite los bloqueos oportunistas de un recurso compartido modificando un recurso compartido existente	Introduzca el siguiente comando: `vserver cifs share properties remove -vserver` *`vserver_name`* `-share-name` *`share_name`* `-share-properties oplocks` Puede especificar propiedades de recursos compartidos adicionales que desea quitar mediante una lista delimitada por comas. Las propiedades de recursos compartidos que se quitan se eliminan de la lista existente de propiedades de recursos compartidos; sin embargo, las propiedades de recursos compartidos configuradas previamente que no se quitan permanecen vigentes.

Ejemplos

El siguiente comando habilita los bloqueos oportunistas del recurso compartido denominado «'Engineering» en la máquina virtual de almacenamiento (SVM, antes conocida como Vserver) vs1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      oplocks
                                  browsable
                                  changenotify
                                  showsnapshot
```

El siguiente comando deshabilita los bloqueos oportunistas del recurso compartido denominado "'Engineering'" en SVM vs1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      browsable
                                  changenotify
                                  showsnapshot
```

Información relacionada

- Habilite o deshabilite los bloqueos oportunistas al crear recursos compartidos de SMB
- Controlar el estado del plock
- Agregar o eliminar propiedades de recursos compartidos en recursos compartidos existentes

Supervise el estado de bloqueo oportunista del bloque de mensajes del servidor de ONTAP

Puede supervisar y mostrar información sobre el estado de los plock. Puede usar esta información para determinar qué archivos tienen bloqueos oportunistas, cuál son el nivel de plocock y el nivel de estado de plocock y si se utiliza el leasing de plocock. También puede determinar la información acerca de los bloqueos que podría necesitar interrumpir manualmente.

Acerca de esta tarea

Puede mostrar información acerca de todos los bloqueos oportunistas en un formulario de resumen o en un formulario de lista detallado. También puede utilizar parámetros opcionales para mostrar información sobre un subconjunto más pequeño de bloqueos existentes. Por ejemplo, puede especificar que la salida devuelva solo los bloqueos con la dirección IP del cliente especificada o con la ruta especificada.

Puede mostrar la siguiente información acerca de los bloqueos oportunistas tradicionales y de arrendamiento:

- SVM, nodo, volumen y LIF en los que se establece el oplock
- Bloquear UUID
- Dirección IP del cliente con el oplock
- Ruta en la que se establece el oplock
- Protocolo de bloqueo (SMB) y tipo (oplock)
- Estado de bloqueo
- Nivel de plock
- Estado de la conexión y tiempo de caducidad del bloque de mensajes del servidor
- Abra el código de grupo si se concede un seguro de arrendamiento

Obtenga más información sobre `vserver oplocks show` en el "Referencia de comandos del ONTAP".

Pasos

1. Muestra el estado de bloqueo oportunista mediante `vserver locks show` el comando.

Ejemplos

El siguiente comando muestra información predeterminada sobre todos los bloqueos. El bloqueo oportunista del archivo mostrado se concede con un `read-batch` nivel de bloqueo oportunista:

```
cluster1::> vserver locks show

Vserver: vs0
Volume   Object Path        LIF         Protocol  Lock Type   Client
-------- ------------------ ----------- --------- ----------- ----------
vol1     /vol1/notes.txt    node1_data1
                                        cifs      share-level 192.168.1.5
         Sharelock Mode: read_write-deny_delete
                                                  op-lock     192.168.1.5
         Oplock Level: read-batch
```

El siguiente ejemplo muestra información más detallada sobre el bloqueo en un archivo con la ruta `/data2/data2_2/intro.pptx`. Se otorga un bloqueo oportunista de concesión en el archivo con un `batch` nivel de bloqueo oportunista a un cliente con una dirección IP `10.3.1.3` de :

> Al mostrar información detallada, el comando proporciona una salida independiente para la información de plock y sharelock. En este ejemplo sólo se muestra la salida de la sección de plock.

```
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Información relacionada

Habilite o deshabilite los bloqueos oportunistas al crear recursos compartidos de SMB

Habilite o deshabilite los bloqueos oportunistas en los recursos compartidos de SMB existentes

Comandos para habilitar o deshabilitar bloqueos operacionales en volúmenes SMB y qtrees

Aplicar objetos de directiva de grupo a servidores SMB

Obtenga información sobre la aplicación de objetos de directiva de grupo a servidores SMB de ONTAP

El servidor SMB admite objetos de directiva de grupo (GPO), un conjunto de reglas conocidas como atributos de directiva de grupo_ que se aplican a equipos de un entorno de Active Directory. Puede utilizar los GPO para gestionar de forma centralizada la configuración de todas las máquinas virtuales de almacenamiento (SVM) del clúster que pertenece al mismo dominio de Active Directory.

Cuando se habilitan los GPO en el servidor SMB, ONTAP envía consultas LDAP al servidor de Active Directory que solicita información de GPO. Si hay definiciones de GPO aplicables al servidor SMB, el servidor

Active Directory devuelve la siguiente información de GPO:

- Nombre de GPO
- Versión de GPO actual
- Ubicación de la definición de GPO
- Listas de UUID (identificadores universales únicos) para conjuntos de directivas de GPO

Información relacionada

- Obtenga más información sobre la seguridad del acceso a archivos para servidores
- "Seguimiento de seguridad y auditoría de SMB y NFS"

Obtenga más información sobre los GPO para SMB de ONTAP compatibles

Aunque no todos los objetos de políticas de grupo (GPO) se aplican a las máquinas virtuales de almacenamiento (SVM) habilitadas para CIFS, las SVM pueden reconocer y procesar el conjunto de objetos de normativa de grupo correspondiente.

Actualmente, los siguientes GPO son compatibles con las SVM:

- Ajustes de configuración de directivas de auditoría avanzadas:

  Acceso a objetos: Escalonamiento de la directiva de acceso central

  Especifica el tipo de eventos que se auditarán para la configuración provisional de la directiva de acceso central (CAP), incluida la siguiente configuración:

  - No auditar
  - Auditar solo los eventos de éxito
  - Auditar solo los eventos de fallo
  - Auditar eventos de éxito y fallo

  > Si se establece cualquiera de las tres opciones de auditoría (sólo eventos de éxito de auditoría, auditar sólo eventos de fallo, auditar eventos de éxito y de fallo), ONTAP audita tanto eventos de éxito como de fallo.

  Se establece mediante la `Audit Central Access Policy Staging` configuración de `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO.

  > Para utilizar las opciones de GPO de configuración de directivas de auditoría avanzadas, la auditoría debe configurarse en la SVM habilitada para CIFS a la que desee aplicar estas opciones. Si la auditoría no está configurada en la SVM, la configuración de GPO no se aplicará y se descarta.

- Configuración del registro:

  - Intervalo de actualización de la directiva de grupo para la SVM habilitada para CIFS

    Se establece mediante el `Registry` GPO.

  - Actualización aleatoria de directivas de grupo

Se establece mediante el `Registry` GPO.

- Publicación de hash para BranchCache

  El GPO Hash Publication para BranchCache corresponde al modo operativo de BranchCache. Se admiten los tres modos de funcionamiento compatibles siguientes:

  - Por recurso compartido
  - Todos los recursos compartidos
  - Se desactiva mediante `Registry` GPO.

- Compatibilidad de la versión de hash para BranchCache

  Se admiten las tres configuraciones de la siguiente versión de hash:

  - BranchCache versión 1
  - BranchCache versión 2
  - Las versiones 1 y 2 de BranchCache se establecen mediante `Registry` GPO.

> Para usar la configuración de GPO de BranchCache, BranchCache debe configurarse en la SVM habilitada para CIFS a la que desea aplicar esta configuración. Si no se configura BranchCache en la SVM, no se aplicará la configuración de GPO y se descarta.

- Configuración de seguridad
  - Política de auditoría y registro de eventos
    - Auditar eventos de inicio de sesión

      Especifica el tipo de eventos de inicio de sesión que se van a auditar, incluida la siguiente configuración:

      - No auditar
      - Auditar solo los eventos de éxito
      - Auditoría de eventos de fallo
      - Audite los eventos de éxito y fallo definidos mediante la `Audit logon events` configuración del `Local Policies/Audit Policy` GPO.

> Si se establece cualquiera de las tres opciones de auditoría (sólo eventos de éxito de auditoría, auditar sólo eventos de fallo, auditar eventos de éxito y de fallo), ONTAP audita tanto eventos de éxito como de fallo.

    - Auditar el acceso a objetos

      Especifica el tipo de acceso al objeto que se va a auditar, incluida la siguiente configuración:

      - No auditar
      - Auditar solo los eventos de éxito
      - Auditoría de eventos de fallo
      - Audite los eventos de éxito y fallo definidos mediante la `Audit object access`

configuración del `Local Policies/Audit Policy` GPO.

> Si se establece cualquiera de las tres opciones de auditoría (sólo eventos de éxito de auditoría, auditar sólo eventos de fallo, auditar eventos de éxito y de fallo), ONTAP audita tanto eventos de éxito como de fallo.

- Método de retención de registros

  Especifica el método de retención del registro de auditoría, incluida la siguiente configuración:

  - Sobrescribir el registro de eventos cuando el tamaño del archivo de registro supere el tamaño máximo del registro
  - No sobrescriba el registro de eventos (borrar registro manualmente) establecido mediante la `Retention method for security log` configuración del `Event Log` GPO.

- Tamaño máximo del registro

  Especifica el tamaño máximo del registro de auditoría.

  Se establece mediante la `Maximum security log size` configuración de `Event Log` GPO.

> Para utilizar la configuración de directiva de auditoría y GPO de registro de eventos, la auditoría debe configurarse en la SVM habilitada para CIFS a la que desea aplicar esta configuración. Si la auditoría no está configurada en la SVM, la configuración de GPO no se aplicará y se descarta.

◦ Seguridad del sistema de archivos

Especifica una lista de archivos o directorios en los que se aplica la seguridad de archivos a través de un GPO.

Se establece mediante el `File System` GPO.

> Debe existir la ruta de acceso del volumen donde se configura el GPO de seguridad del sistema de archivos en la SVM.

◦ Política de Kerberos

- Desviación máxima del reloj

  Especifica la tolerancia máxima en minutos para la sincronización del reloj del equipo.

  Se establece mediante la `Maximum tolerance for computer clock synchronization` configuración de `Account Policies/Kerberos Policy` GPO.

- Antigüedad máxima del billete

  Especifica la duración máxima en horas para el ticket de usuario.

  Se establece mediante la `Maximum lifetime for user ticket` configuración de `Account Policies/Kerberos Policy` GPO.

- Antigüedad máxima de renovación del boleto

Especifica la duración máxima en días para la renovación de la tarjeta de usuario.

Se establece mediante la `Maximum lifetime for user ticket renewal` configuración de `Account Policies/Kerberos Policy` GPO.

- Asignación de derechos de usuario (derechos de privilegio)
  - Asuma la propiedad

    Especifica la lista de usuarios y grupos que tienen derecho a asumir la propiedad de cualquier objeto asegurable.

    Se establece mediante la `Take ownership of files or other objects` configuración de `Local Policies/User Rights Assignment` GPO.

  - Privilegio de seguridad

    Especifica la lista de usuarios y grupos que pueden especificar opciones de auditoría para el acceso a objetos de recursos individuales, como archivos, carpetas y objetos de Active Directory.

    Se establece mediante la `Manage auditing and security log` configuración de `Local Policies/User Rights Assignment` GPO.

  - Cambiar privilegio de notificación (comprobación de recorrido de derivación)

    Especifica la lista de usuarios y grupos que pueden recorrer los árboles de directorios aunque los usuarios y los grupos puedan no tener permisos en el directorio de recorrido.

  El mismo privilegio es necesario para que los usuarios reciban notificaciones de cambios en archivos y directorios. Se establece mediante la `Bypass traverse checking` configuración de `Local Policies/User Rights Assignment` GPO.

- Valores del Registro
  - Firma Configuración requerida

    Especifica si la firma SMB necesaria está habilitada o deshabilitada.

  Se establece mediante la `Microsoft network server: Digitally sign communications (always)` configuración de `Security Options` GPO.

- Restringir anónimo

  Especifica cuáles son las restricciones para los usuarios anónimos e incluye las tres configuraciones de GPO siguientes:

  - No hay enumeración de cuentas del Administrador de cuentas de seguridad (SAM):

    Esta configuración de seguridad determina qué permisos adicionales se conceden para las conexiones anónimas al equipo. Esta opción se muestra como `no-enumeration` en ONTAP si está habilitada.

    Se establece mediante la `Network access: Do not allow anonymous enumeration of SAM accounts` configuración de `Local Policies/Security Options` GPO.

- No hay enumeración de cuentas y recursos compartidos de SAM

  Esta configuración de seguridad determina si se permite la enumeración anónima de cuentas SAM y recursos compartidos. Esta opción se muestra como `no-enumeration` en ONTAP si está habilitada.

  Se establece mediante la `Network access: Do not allow anonymous enumeration of SAM accounts and shares` configuración de `Local Policies/Security Options` GPO.

- Restringir el acceso anónimo a recursos compartidos y canalizaciones con nombre

  Esta configuración de seguridad restringe el acceso anónimo a recursos compartidos y tuberías. Esta opción se muestra como `no-access` en ONTAP si está habilitada.

  Se establece mediante la `Network access: Restrict anonymous access to Named Pipes and Shares` configuración de `Local Policies/Security Options` GPO.

  Cuando se muestra información sobre las políticas de grupo definidas y aplicadas, el `Resultant restriction for anonymous user` campo de salida proporciona información sobre la restricción resultante de los tres valores de GPO anónimos de restricción. Las posibles restricciones resultantes son las siguientes:

° `no-access`

Al usuario anónimo se le deniega el acceso a los recursos compartidos especificados y a las canalizaciones con nombre, y no se puede utilizar la enumeración de cuentas y recursos compartidos SAM. Esta restricción resultante se ve si el `Network access: Restrict anonymous access to Named Pipes and Shares` GPO está habilitado.

° `no-enumeration`

El usuario anónimo tiene acceso a los recursos compartidos y canalizaciones con nombre especificados, pero no puede utilizar la enumeración de cuentas y recursos compartidos SAM. Esta restricción resultante se observa si se cumplen las dos condiciones siguientes:

- El `Network access: Restrict anonymous access to Named Pipes and Shares` GPO está desactivado.
- `Network access: Do not allow anonymous enumeration of SAM accounts`O los `Network access: Do not allow anonymous enumeration of SAM accounts and shares` objetos de normativa de grupo están activados.

° `no-restriction`

El usuario anónimo tiene acceso completo y puede utilizar la enumeración. Esta restricción resultante se observa si se cumplen las dos condiciones siguientes:

- El `Network access: Restrict anonymous access to Named Pipes and Shares` GPO está desactivado.
- Los `Network access: Do not allow anonymous enumeration of SAM accounts` `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPO y están desactivados.
  - Grupos restringidos

Puede configurar grupos restringidos para administrar de forma centralizada la pertenencia a grupos integrados o definidos por el usuario. Cuando aplica un grupo restringido a través de una directiva de grupo, la pertenencia a un grupo local de servidor CIFS se establece automáticamente para que coincida con la configuración de la lista de miembros definida en la directiva de grupo aplicada.

Se establece mediante el `Restricted Groups` GPO.

- Configuración de la directiva de acceso central

  Especifica una lista de directivas de acceso central. Las políticas de acceso central y las reglas de política de acceso central asociadas determinan los permisos de acceso para varios archivos en la SVM.

Información relacionada

- Habilitar o deshabilitar la compatibilidad con GPO en los servidores
- Obtenga más información sobre la seguridad del acceso a archivos para servidores
- "Seguimiento de seguridad y auditoría de SMB y NFS"
- Modificar la configuración de seguridad del servidor
- Obtenga información sobre cómo usar BranchCache para almacenar en caché contenido compartido en una sucursal
- Aprenda a utilizar la firma ONTAP para mejorar la seguridad de la red
- Obtenga información sobre cómo configurar la comprobación de recorrido de derivación
- Configurar restricciones de acceso para usuarios anónimos

Requisitos del servidor SMB de ONTAP para GPO

Para utilizar objetos de directiva de grupo (GPO) con el servidor SMB, el sistema debe cumplir varios requisitos.

- Las licencias de SMB deben estar en el clúster. La licencia SMB se incluye con "ONTAP One". Si no tiene ONTAP One y la licencia no está instalada, póngase en contacto con su representante de ventas.
- Debe haber un servidor SMB configurado y Unido a un dominio de Windows Active Directory.
- El estado del administrador del servidor SMB debe ser on.
- Los GPO deben configurarse y aplicarse a la unidad organizativa (OU) de Active Directory de Windows que contiene el objeto de equipo servidor SMB.
- La compatibilidad con GPO debe estar habilitada en el servidor SMB.

Habilitar o deshabilitar la compatibilidad de GPO en los servidores SMB de ONTAP

Puede habilitar o deshabilitar la compatibilidad con objetos de directiva de grupo (GPO) en un servidor CIFS. Si habilita la compatibilidad de GPO en un servidor CIFS, los GPO aplicables definidos en la directiva de grupo (la directiva que se aplica a la unidad organizativa (OU) que contiene el objeto de equipo del servidor CIFS) se aplican al servidor CIFS.

Acerca de esta tarea

Los GPO no pueden habilitarse en servidores CIFS en modo de grupo de trabajo.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el comando…
Habilite los GPO	`vserver cifs group-policy modify -vserver vserver_name -status enabled`
Deshabilitar GPO	`vserver cifs group-policy modify -vserver vserver_name -status disabled`

2. Compruebe que el soporte de GPO está en el estado deseado: `vserver cifs group-policy show -vserver +vserver_name_`

   El estado de la directiva de grupo de los servidores CIFS en el modo de grupo se muestra como "desactivado".

Ejemplo

En el siguiente ejemplo, se habilita la compatibilidad de GPO en máquinas virtuales de almacenamiento (SVM) vs1:

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

            Vserver: vs1
Group Policy Status: enabled
```

Información relacionada

Obtenga más información sobre los GPO compatibles

Requisitos del servidor para GPO

Obtenga información sobre cómo actualizar GPO en servidores SMB

Actualizar manualmente la configuración de GPO en servidores SMB

Mostrar información acerca de las configuraciones de GPO

Cómo se actualizan los GPO en el servidor SMB

Obtenga información sobre la actualización de GPO en servidores SMB de ONTAP

De forma predeterminada, ONTAP recupera y aplica los cambios de objeto de directiva de grupo (GPO) cada 90 minutos. La configuración de seguridad se actualiza cada 16 horas. Si desea actualizar GPO para aplicar nuevas configuraciones de directivas de GPO antes de que ONTAP las actualice automáticamente, puede activar una actualización manual en un servidor CIFS con un comando ONTAP.

- De forma predeterminada, todos los GPO se verifican y actualizan según sea necesario cada 90 minutos.

  Este intervalo se puede configurar y se puede ajustar mediante `Refresh interval` `Random offset` los ajustes de y GPO.

  ONTAP consulta a Active Directory los cambios realizados en los GPO. Si los números de versión de GPO registrados en Active Directory son superiores a los del servidor CIFS, ONTAP recupera y aplica los nuevos GPO. Si los números de versión son los mismos, los GPO en el servidor CIFS no se actualizan.

- Configuración de seguridad los GPO se actualizan cada 16 horas.

  ONTAP recupera y aplica los GPO de configuración de seguridad cada 16 horas, independientemente de que estos GPO hayan cambiado o no.

  > El valor predeterminado de 16 horas no se puede cambiar en la versión actual de ONTAP. Es una configuración predeterminada del cliente Windows.

- Todos los GPO se pueden actualizar manualmente con un comando ONTAP.

  Este comando simula el `gpupdate.exe` comando Windows/force`.

Información relacionada

Actualizar manualmente la configuración de GPO en servidores SMB

Actualice manualmente la configuración de GPO en los servidores SMB de ONTAP

Si desea actualizar inmediatamente la configuración del objeto de directiva de grupo (GPO) en el servidor CIFS, puede actualizar manualmente la configuración. Sólo puede actualizar los ajustes modificados o puede forzar una actualización para todos los ajustes, incluidos los que se aplicaron anteriormente pero no se han modificado.

Paso

1. Ejecute la acción adecuada:

Si desea actualizar…	Introduzca el comando…
Ha cambiado la configuración de GPO	`vserver cifs group-policy update -vserver` *`vserver_name`*
Todas las configuraciones de GPO	`vserver cifs group-policy update -vserver` *`vserver_name`* `-force-reapply -all-settings true`

Información relacionada

Obtenga información sobre cómo actualizar GPO en servidores SMB

Mostrar información sobre las configuraciones de GPO SMB de ONTAP

Puede mostrar información acerca de las configuraciones de objeto de directiva de grupo (GPO) definidas en Active Directory y acerca de las configuraciones de GPO aplicadas al

servidor CIFS.

Acerca de esta tarea

Puede mostrar información acerca de todas las configuraciones de GPO definidas en Active Directory del dominio al que pertenece el servidor CIFS o solo puede mostrar información acerca de las configuraciones de GPO aplicadas a un servidor CIFS.

Pasos

1. Mostrar información acerca de las configuraciones de GPO realizando una de las siguientes acciones:

Si desea mostrar información acerca de todas las configuraciones de directiva de grupo…	Introduzca el comando…
Definido en Active Directory	`vserver cifs group-policy show-defined -vserver vserver_name`
Aplicado a una máquina virtual de almacenamiento (SVM) habilitada para CIFS	`vserver cifs group-policy show-applied -vserver vserver_name`

Ejemplo

En el siguiente ejemplo, se muestran las configuraciones de GPO definidas en Active Directory al que pertenece la SVM habilitada para CIFS con el nombre vs1:

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache : version1
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
```

```
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
    Status: enabled
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication for Mode BranchCache: per-share
    Hash Version Support for BranchCache: version1
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
```

```
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

En el siguiente ejemplo, se muestran las configuraciones de GPO aplicadas a la SVM vs1 habilitada para CIFS:

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
-----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
```

```
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
```

```
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

Información relacionada

Habilitar o deshabilitar la compatibilidad con GPO en los servidores

Mostrar información sobre los GPO de grupo restringido SMB de ONTAP

Puede mostrar información detallada sobre los grupos restringidos que se definen como objetos de directiva de grupo (GPO) en Active Directory y que se aplican al servidor CIFS.

Acerca de esta tarea

De forma predeterminada, se muestra la siguiente información:

- Nombre de la política de grupo
- Versión de la directiva de grupo
- Enlace

  Especifica el nivel en el que se configura la directiva de grupo. Los valores de salida posibles incluyen los siguientes:

  - `Local` Cuando la política de grupo está configurada en ONTAP
  - `Site` cuando la política de grupo se configura en el nivel de sitio en el controlador de dominio
  - `Domain` cuando la política de grupo se configura en el nivel de dominio en el controlador de dominio
  - `OrganizationalUnit` Cuando la directiva de grupo se configura en el nivel de unidad organizativa (OU) en el controlador de dominio
  - `RSOP` para el conjunto resultante de políticas derivadas de todas las políticas de grupo definidas en varios niveles
- Nombre de grupo restringido
- Los usuarios y grupos que pertenecen al grupo restringido y que no pertenecen al mismo
- Lista de grupos a los que se agrega el grupo restringido

  Un grupo puede ser miembro de grupos distintos de los que se enumeran aquí.

Paso

1. Muestre información acerca de todos los GPO de grupo restringidos realizando una de las siguientes acciones:

Si desea mostrar información sobre todos los GPO de grupo restringidos…	Introduzca el comando…
Definido en Active Directory	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
Aplicado a un servidor CIFS	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

Ejemplo

En el siguiente ejemplo, se muestra información sobre los objetos de normativa de grupo restringidos definidos en el dominio de Active Directory al que pertenece la SVM habilitada para CIFS, llamada vs1:

```
cluster1::> vserver cifs group-policy restricted-group show-defined
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9
```

En el siguiente ejemplo, se muestra información sobre los objetos de normativa de grupo restringidos aplicados a la SVM vs1 habilitada para CIFS:

```
cluster1::> vserver cifs group-policy restricted-group show-applied
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9
```

Información relacionada

Mostrar información acerca de las configuraciones de GPO

Muestra información sobre las políticas de acceso central de SMB de ONTAP

Puede mostrar información detallada acerca de las directivas de acceso central definidas en Active Directory. También puede mostrar información sobre las políticas de acceso central que se aplican al servidor CIFS a través de objetos de política de grupo (GPO).

Acerca de esta tarea

De forma predeterminada, se muestra la siguiente información:

- Nombre de SVM
- Nombre de la política de acceso central
- SID
- Descripción
- Hora de creación
- Tiempo de modificación
- Normas de los miembros

> Los servidores CIFS en el modo de grupo de trabajo no se muestran porque no admiten los GPO.

Paso

1. Muestre información acerca de las directivas de acceso central realizando una de las siguientes acciones:

Si desea mostrar información sobre todas las directivas de acceso central…	Introduzca el comando…
Definido en Active Directory	`vserver cifs group-policy central-access-policy show-defined -vserver` *vserver_name*
Aplicado a un servidor CIFS	`vserver cifs group-policy central-access-policy show-applied -vserver` *vserver_name*

Ejemplo

El siguiente ejemplo muestra información de todas las directivas de acceso central definidas en Active Directory:

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name                 SID
-------- --------------------
----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

El siguiente ejemplo muestra información de todas las políticas de acceso central que se aplican a las máquinas virtuales de almacenamiento (SVM) del clúster:

```
cluster1::> vserver cifs group-policy central-access-policy show-applied

Vserver    Name                 SID
-------- --------------------
----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

Información relacionada

- Obtenga más información sobre la seguridad del acceso a archivos para servidores
- Mostrar información acerca de las configuraciones de GPO
- Muestra información acerca de las reglas de la política de acceso central

Mostrar información sobre las reglas de política de acceso central de SMB de ONTAP

Puede mostrar información detallada acerca de las reglas de directiva de acceso central asociadas a las directivas de acceso central definidas en Active Directory. También puede mostrar información sobre las reglas de políticas de acceso central que se aplican al servidor CIFS a través de los GPO de la política de acceso central (objetos de política de grupo).

Acerca de esta tarea

Puede mostrar información detallada acerca de las reglas de directiva de acceso central definidas y aplicadas. De forma predeterminada, se muestra la siguiente información:

- Nombre del Vserver
- Nombre de la regla de acceso central
- Descripción
- Hora de creación
- Tiempo de modificación
- Permisos actuales
- Permisos propuestos

- Recursos objetivo

Si desea mostrar información acerca de todas las reglas de directiva de acceso central asociadas con las directivas de acceso central…	Introduzca el comando…
Definido en Active Directory	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
Aplicado a un servidor CIFS	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

Ejemplo

En el siguiente ejemplo se muestra información de todas las reglas de directiva de acceso central asociadas a las directivas de acceso central definidas en Active Directory:

```
cluster1::> vserver cifs group-policy central-access-rule show-defined

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

El siguiente ejemplo muestra información de todas las reglas de políticas de acceso central asociadas con las políticas de acceso centrales aplicadas a las máquinas virtuales de almacenamiento (SVM) en el clúster:

```
cluster1::> vserver cifs group-policy central-access-rule show-applied

Vserver     Name
----------- --------------------
vs1         r1
            Description: rule #1
          Creation Time: Tue Oct 22 09:33:48 2013
      Modification Time: Tue Oct 22 09:33:48 2013
    Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
   Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1         r2
            Description: rule #2
          Creation Time: Tue Oct 22 10:27:57 2013
      Modification Time: Tue Oct 22 10:27:57 2013
    Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
   Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

Información relacionada

- Obtenga más información sobre la seguridad del acceso a archivos para servidores
- Mostrar información acerca de las configuraciones de GPO
- Muestra información sobre las políticas de acceso central

Comandos de ONTAP para gestionar contraseñas de cuentas de equipo de servidor SMB

Debe conocer los comandos para cambiar, restablecer y deshabilitar contraseñas, así como para configurar las programaciones de actualización automática. También puede configurar una programación en el servidor SMB para que la actualice automáticamente.

Si desea…	Se usa este comando…
Cambie la contraseña de la cuenta de dominio cuando ONTAP esté sincronizado con los servicios de AD	`vserver cifs domain password change`
Restablezca la contraseña de la cuenta de dominio cuando ONTAP no esté sincronizado con los servicios de AD	`vserver cifs domain password reset`
Configurar servidores SMB para cambios automáticos de contraseña de cuenta de equipo	`vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true`

Si desea…	Se usa este comando…
Deshabilite los cambios automáticos de contraseña de cuenta de equipo en servidores SMB	`vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false`

Obtenga más información sobre `vserver cifs domain password` en el "Referencia de comandos del ONTAP".

Gestione las conexiones del controlador de dominio

Mostrar información sobre los servidores detectados por el bloque de mensajes del servidor de ONTAP

Puede mostrar información relacionada con los servidores LDAP y las controladoras de dominio detectados en el servidor CIFS.

Paso

1. Para mostrar la información relacionada con los servidores detectados, introduzca el siguiente comando: `vserver cifs domain discovered-servers show`

Ejemplo

En el siguiente ejemplo, se muestran los servidores detectados para la SVM vs1:

```
cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address     Status
--------------- -------- ---------- ----------- -------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4        OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5        OK
example.com     MS-DC    adequate   DC-1        1.1.3.4        OK
example.com     MS-DC    adequate   DC-2        1.1.3.5        OK
```

Información relacionada

- Restablecer y volver a detectar servidores
- Detener o iniciar servidores

Restablecer y volver a detectar los servidores SMB de ONTAP

La restauración y la nueva detección de servidores en el servidor CIFS permite que el servidor CIFS deseche la información almacenada sobre los servidores LDAP y las controladoras de dominio. Tras descartar información del servidor, el servidor CIFS vuelve a adquirir la información actual de estos servidores externos. Esto puede ser útil cuando los servidores conectados no responden adecuadamente.

Pasos

1. Introduzca el siguiente comando: `vserver cifs domain discovered-servers reset-servers -vserver vserver_name`
2. Mostrar información sobre los servidores recién redetectados: `vserver cifs domain discovered-servers show -vserver vserver_name`

Ejemplo

En el siguiente ejemplo, se restablecen y vuelven a detectar los servidores para la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1:

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver
vs1

cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

Información relacionada

- Muestra información sobre los servidores detectados
- Detener o iniciar servidores

Gestione la detección de controlador de dominio SMB de ONTAP

A partir de ONTAP 9.3, puede modificar el proceso predeterminado por el que se detectan los controladores de dominio (DC). Esto le permite limitar la detección a sus instalaciones o a un conjunto de centros de datos preferidos, lo que puede mejorar el rendimiento en función del entorno.

Acerca de esta tarea

De forma predeterminada, el proceso de detección dinámica detecta todos los centros de datos disponibles, incluidos los centros de datos preferidos, todos los centros de datos del sitio local y todos los centros de datos remotos. Esta configuración puede provocar latencia en autenticación y acceder a recursos compartidos en determinados entornos. Si ya ha determinado el grupo de DC que desea utilizar o si los DC remotos son inadecuados o inaccesibles, puede cambiar el método de descubrimiento.

En las versiones ONTAP 9.3 y posteriores, el `discovery-mode` parámetro del `cifs domain discovered-servers` comando permite seleccionar una de las siguientes opciones de detección:

- Se descubren todos los DC del dominio.

- Sólo se descubren los centros de datos del sitio local.

  `default-site`El parámetro del servidor SMB se puede definir para utilizar este modo con LIF que no están asignadas a un sitio en sites-and-services.

- No se realiza la detección del servidor, la configuración del servidor SMB depende únicamente de los centros de datos preferidos.

  Para utilizar este modo, primero debe definir los DC preferidos para el servidor SMB.

Antes de empezar

Debe estar en el nivel de privilegio avanzado.

Paso

1. Especifique la opción de detección deseada: `vserver cifs domain discovered-servers discovery-mode modify -vserver` *`vserver_name`* `-mode {all|site|none}`

   Opciones para el `mode` parámetro:

   - `all`

     Descubrir todos los DC disponibles (predeterminado).

   - `site`

     Limite el descubrimiento de DC a su sitio.

   - `none`

     Utilice sólo los centros de datos preferidos y no realice la detección.

Añada controladoras de dominio SMB de ONTAP preferidas

ONTAP detecta automáticamente controladoras de dominio a través de DNS. Opcionalmente, puede añadir uno o varios controladores de dominio a la lista de controladores de dominio preferidos para un dominio específico.

Acerca de esta tarea

Si ya existe una lista de controladores de dominio preferido para el dominio especificado, la nueva lista se combina con la lista existente.

Paso

1. Para agregar a la lista de controladores de dominio preferidos, introduzca el siguiente comando: `vserver cifs domain preferred-dc add -vserver` *`vserver_name`* `-domain` *`domain_name`* `-preferred-dc IP_address, …+`

   `-vserver` *`vserver_name`* Especifica el nombre de la máquina virtual de almacenamiento (SVM).

`-domain` *`domain_name`* Especifica el nombre completo de Active Directory del dominio al que pertenecen los controladores de dominio especificados.

`-preferred-dc` *`IP_address`*,... especifica una o más direcciones IP de los controladores de dominio preferidos, como una lista delimitada por comas, en orden de preferencia.

Ejemplo

El siguiente comando añade los controladores de dominio 172.17.102.25 y 172.17.102.24 a la lista de controladores de dominio preferidos que el servidor SMB en SVM vs1 utiliza para gestionar el acceso externo al dominio cifs.lab.example.com.

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

Información relacionada

Comandos para gestionar controladoras de dominio preferidas

Comandos de ONTAP para gestionar las controladoras de dominio SMB preferidas

Debe conocer los comandos para añadir, mostrar y eliminar controladoras de dominio preferidas.

Si desea…	Se usa este comando…
Agregar un controlador de dominio preferido	`vserver cifs domain preferred-dc add`
Mostrar los controladores de dominio preferidos	`vserver cifs domain preferred-dc show`
Quite una controladora de dominio preferida	`vserver cifs domain preferred-dc remove`

Obtenga más información sobre `vserver cifs domain preferred-dc` en el "Referencia de comandos del ONTAP".

Información relacionada

Añada controladores de dominio preferidos

Habilite las conexiones cifradas a los controladores de dominio SMB de ONTAP

A partir de ONTAP 9.8, puede especificar que se cifren las conexiones a los controladores de dominio.

Acerca de esta tarea

ONTAP requiere cifrado para las comunicaciones del controlador de dominio (DC) cuando la `-encryption-required-for-dc-connection` opción está establecida en `true`; el valor predeterminado es `false`. Cuando se establece la opción, solo se utilizará el protocolo SMB3 para las conexiones ONTAP-DC, ya que el cifrado solo es compatible con SMB3.

Cuando se requieren comunicaciones CC cifradas, la `-smb2-enabled-for-dc-connections` opción se

ignora, ya que ONTAP solo negocia conexiones SMB3. Si un controlador de dominio no admite SMB3 y cifrado, ONTAP no se conectará a él.

Paso

1. Habilitar la comunicación cifrada con el DC: `vserver cifs security modify -vserver` *`svm_name`* `-encryption-required-for-dc-connection true`

Utilice sesiones nulas para acceder al almacenamiento en entornos que no sean de Kerberos

Utilice sesiones nulas de SMB de ONTAP para acceder al almacenamiento en entornos que no sean Kerberos

El acceso de sesión nulo proporciona permisos para recursos de red, como datos del sistema de almacenamiento, y para servicios basados en cliente que se ejecutan en el sistema local. Una sesión nula se produce cuando un proceso de cliente utiliza la cuenta "system" para acceder a un recurso de red. La configuración de sesión nula es específica para la autenticación que no es de Kerberos.

Descubra cómo los sistemas de almacenamiento para pymes de ONTAP proporcionan un acceso nulo a la sesión

Debido a que los recursos compartidos de sesión nulos no requieren autenticación, los clientes que requieren acceso de sesión nulo deben tener sus direcciones IP asignadas en el sistema de almacenamiento.

De forma predeterminada, los clientes de sesión nula sin asignar pueden acceder a determinados servicios del sistema ONTAP, como la enumeración de recursos compartidos, pero se limitan a acceder a cualquier dato del sistema de almacenamiento.

> ONTAP admite los valores de configuración del Registro anónimo con la `-restrict-anonymous` opción. Esto permite controlar hasta qué punto los usuarios nulos no asignados pueden ver o acceder a los recursos del sistema. Por ejemplo, puede deshabilitar la enumeración de recursos compartidos y el acceso al recurso compartido IPC$ (recurso compartido de canalizaciones con nombre oculto). Obtenga más información acerca de `vserver cifs options modify` y `vserver cifs options show` y la `-restrict-anonymous` opción en el "Referencia de comandos del ONTAP".

A menos que se configure lo contrario, un cliente que ejecute un proceso local que solicite acceso al sistema de almacenamiento a través de una sesión nula sólo es miembro de grupos no restrictivos, como «'todos'». Para limitar el acceso de sesión nulo a los recursos del sistema de almacenamiento seleccionados, es posible que desee crear un grupo al que pertenecen todos los clientes de sesión nulos; al crear este grupo se le permite restringir el acceso al sistema de almacenamiento y establecer permisos de recursos del sistema de almacenamiento que se aplican específicamente a clientes de sesión nulos.

ONTAP proporciona una sintaxis de asignación en el `vserver name-mapping` conjunto de comandos para especificar la dirección IP de los clientes que permite el acceso a los recursos del sistema de almacenamiento mediante una sesión de usuario nula. Después de crear un grupo para usuarios nulos, puede especificar restricciones de acceso para los recursos del sistema de almacenamiento y permisos de recursos que se apliquen solo a sesiones nulas. El usuario nulo se identifica como inicio de sesión anónimo. Los usuarios nulos no tienen acceso a ningún directorio principal.

Todos los usuarios nulos que acceden al sistema de almacenamiento desde una dirección IP asignada se conceden permisos de usuario asignado. Considere las precauciones adecuadas para evitar el acceso no autorizado a sistemas de almacenamiento asignados con usuarios nulos. Para obtener la máxima protección,

coloque el sistema de almacenamiento y todos los clientes que necesiten un acceso nulo al sistema de almacenamiento de usuarios en una red independiente, con el fin de eliminar la posibilidad de que se produzca una dirección IP «posing».

Información relacionada

Configurar restricciones de acceso para usuarios anónimos

Otorgue acceso de usuarios nulos a recursos compartidos del sistema de archivos SMB de ONTAP

Puede permitir el acceso a los recursos del sistema de almacenamiento por parte de clientes de sesión nulos asignando un grupo para que lo utilicen clientes de sesión nulos y registrando las direcciones IP de clientes de sesión nulos para añadirlas a la lista de clientes a los que el sistema de almacenamiento puede acceder a los datos mediante sesiones nulas.

Pasos

1. Utilice el `vserver name-mapping create` comando para asignar el usuario nulo a cualquier usuario válido de Windows, con un cualificador de IP.

   El siguiente comando asigna el usuario nulo al usuario1 con un nombre de host válido google.com:

   ```
   vserver name-mapping create -direction win-unix  -position 1 -pattern
   "ANONYMOUS LOGON" -replacement user1 - hostname google.com
   ```

   El siguiente comando asigna el usuario nulo a user1 con una dirección IP válida 10.238.2.54/32:

   ```
   vserver name-mapping create -direction win-unix  -position 2 -pattern
   "ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
   ```

2. Utilice `vserver name-mapping show` el comando para confirmar la asignación de nombres.

   ```
   vserver name-mapping show

   Vserver:   vs1
   Direction: win-unix
   Position Hostname         IP Address/Mask
   -------- --------         ----------------
   1        -                10.72.40.83/32      Pattern: anonymous logon
                                              Replacement: user1
   ```

3. Utilice `vserver cifs options modify –win-name-for-null-user` el comando para asignar la pertenencia de Windows al usuario nulo.

   Esta opción sólo se aplica cuando hay una asignación de nombres válida para el usuario nulo.

```
vserver cifs options modify -win-name-for-null-user user1
```

4. Utilice el `vserver cifs options show` comando para confirmar la asignación del usuario nulo al usuario o grupo de Windows.

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```

Administrar alias NetBIOS para servidores SMB

Obtenga información sobre la administración de alias de NetBIOS para servidores SMB de ONTAP

Los alias NetBIOS son nombres alternativos para el servidor SMB que los clientes SMB pueden utilizar al conectarse con el servidor SMB. La configuración de alias NetBIOS para un servidor SMB puede ser útil cuando está consolidando datos de otros servidores de archivos en el servidor SMB y desea que el servidor SMB responda a los nombres de los servidores de archivos originales.

Puede especificar una lista de alias NetBIOS cuando cree el servidor SMB o en cualquier momento después de crear el servidor SMB. Puede agregar o quitar alias NetBIOS de la lista en cualquier momento. Puede conectarse al servidor SMB utilizando cualquiera de los nombres de la lista de alias NetBIOS.

Información relacionada

Muestra información acerca de NetBIOS sobre conexiones TCP

Agregue listas de alias de NetBIOS a los servidores SMB de ONTAP

Si desea que los clientes SMB se conecten al servidor SMB mediante un alias, puede crear una lista de alias NetBIOS o agregar alias NetBIOS a una lista existente de alias NetBIOS.

Acerca de esta tarea

- El nombre del alias NetBIOS puede tener una longitud máxima de 15 caracteres.
- Puede configurar hasta 200 alias NetBIOS en el servidor SMB.
- No se permiten los siguientes caracteres:

  @ # * ( ) = + [ ] | ; : " , < > \ / ?

Pasos

1. Agregue los alias de NetBIOS:
   `vserver cifs add-netbios-aliases -vserver` *`vserver_name`* `-netbios-aliases` *`NetBIOS_alias`*`,…`

```
vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases
alias_1,alias_2,alias_3
```

- Puede especificar uno o varios alias NetBIOS utilizando una lista delimitada por comas.
- Los alias NetBIOS especificados se agregan a la lista existente.
- Se crea una nueva lista de alias NetBIOS si la lista está vacía actualmente.

2. Compruebe que los alias de NetBIOS se han agregado correctamente: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

Información relacionada

- Eliminar alias NetBIOS de la lista para servidores SMB
- Mostrar la lista de alias NetBIOS para servidores SMB

Elimine los alias de NetBIOS de la lista de servidores SMB de ONTAP

Si no necesita alias NetBIOS específicos para un servidor CIFS, puede eliminar esos alias NetBIOS de la lista. También puede quitar todos los alias NetBIOS de la lista.

Acerca de esta tarea

Puede quitar más de un alias NetBIOS utilizando una lista delimitada por comas. Puede quitar todos los alias de NetBIOS de un servidor CIFS especificando - como valor para `-netbios-aliases` el parámetro.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea quitar…	Introduzca…
Alias NetBIOS específicos de la lista	`vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios -aliases _NetBIOS_alias_,...`
Todos los alias NetBIOS de la lista	`vserver cifs remove-netbios-aliases -vserver` *`vserver_name`* `-netbios-aliases -`

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

2. Verifique que se hayan eliminado los alias de NetBIOS especificados: `vserver cifs show -vserver` *`vserver_name`* `-display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_2, ALIAS_3
```

Mostrar la lista de alias de NetBIOS para los servidores SMB de ONTAP

Puede mostrar la lista de alias NetBIOS. Esto puede resultar útil cuando desea determinar la lista de nombres a través de la cual los clientes SMB pueden realizar conexiones con el servidor CIFS.

Paso

1. Ejecute una de las siguientes acciones:

Si desea mostrar información acerca de…	Introduzca…
Alias de NetBIOS de un servidor CIFS	`vserver cifs show -display-netbios -aliases`
La lista de alias NetBIOS como parte de la información detallada del servidor CIFS	`vserver cifs show -instance`

En el siguiente ejemplo, se muestra información sobre los alias NetBIOS de un servidor CIFS:

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

En el siguiente ejemplo, se muestra la lista de alias NetBIOS como parte de la información detallada del servidor CIFS:

```
vserver cifs show -instance
```

```
                                        Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_SERVER
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

Obtenga más información sobre `vserver cifs show` en el "Referencia de comandos del ONTAP".

Información relacionada

- Agregar listas de alias NetBIOS a los servidores
- Comandos para administrar servidores

Determine si los clientes SMB de ONTAP están conectados mediante alias NetBIOS

Puede determinar si los clientes SMB están conectados mediante alias NetBIOS y, si es así, qué alias NetBIOS se utiliza para realizar la conexión. Esto puede ser útil para solucionar problemas de conexión.

Acerca de esta tarea

Debe utilizar el `-instance` parámetro para mostrar el alias de NetBIOS (si existe) asociado a una conexión SMB. Si el nombre del servidor CIFS o una dirección IP se utilizan para establecer la conexión SMB, la salida del `NetBIOS Name` campo es - (guión).

Paso

1. Realice la acción deseada:

Si desea mostrar información de NetBIOS para…	Introduzca…
Conexiones SMB	`vserver cifs session show -instance`
Conexiones que utilizan un alias NetBIOS especificado:	`vserver cifs session show -instance -netbios-name` *`netbios_name`*

En el siguiente ejemplo se muestra información sobre el alias NetBIOS utilizado para establecer la conexión SMB con el ID de sesión 1:

```
vserver cifs session show -session-id 1 -instance
```

```
                        Node: node1
                     Vserver: vs1
                  Session ID: 1
                Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
                 Workstation: 10.2.2.50
    Authentication Mechanism: NTLMv2
                Windows User: EXAMPLE\user1
                   UNIX User: user1
                 Open Shares: 2
                  Open Files: 2
                  Open Other: 0
              Connected Time: 1d 1h 10m 5s
                   Idle Time: 22s
           Protocol Version: SMB3
      Continuously Available: No
          Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: ALIAS1
       SMB Encryption Status: Unencrypted
```

Administrar varias tareas del servidor SMB

Detenga o inicie los servidores SMB de ONTAP

Puede detener el servidor CIFS en una SVM, que puede ser útil a la hora de realizar tareas mientras los usuarios no acceden a datos a través de recursos compartidos SMB. Puede reiniciar el acceso SMB iniciando el servidor CIFS. Al detener el servidor CIFS, también puede modificar los protocolos permitidos en la máquina virtual de almacenamiento (SVM).

Pasos

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el comando…
Detenga el servidor CIFS	`vserver cifs stop -vserver *vserver_name* [-foreground {true
false}]`	Inicie EL servidor CIFS
`vserver cifs start -vserver *vserver_name* [-foreground {true	false}]`

`-foreground` especifica si el comando debe ejecutarse en primer plano o en segundo plano. Si no

introduce este parámetro, se establece en `true`, y el comando se ejecuta en primer plano.

2. Compruebe que el estado administrativo del servidor CIFS sea correcto mediante `vserver cifs show` el comando.

Ejemplo

Los siguientes comandos inician el servidor CIFS en la SVM vs1:

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: VS1
                    NetBIOS Domain/Workgroup Name: DOMAIN
                      Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
```

Información relacionada

- Muestra información sobre los servidores detectados
- Restablecer y volver a detectar servidores

Mueva los servidores SMB de ONTAP a distintas unidades organizativas

El proceso de creación del servidor CIFS utiliza la unidad organizativa (OU) CN=Computers predeterminada durante la instalación, a menos que especifique una unidad organizativa diferente. Puede mover servidores CIFS a unidades organizativas diferentes tras la configuración.

Pasos

1. En el servidor Windows, abra el árbol **usuarios y equipos de Active Directory**.
2. Busque el objeto de Active Directory para la máquina virtual de almacenamiento (SVM).
3. Haga clic con el botón derecho del ratón en el objeto y seleccione **mover**.
4. Seleccione la unidad organizativa que desea asociar con la SVM

Resultados

El objeto SVM se coloca en la unidad organizativa seleccionada.

Modifique el dominio DNS dinámico antes de mover los servidores SMB de ONTAP

Si desea que el servidor DNS integrado en Active Directory registre de forma dinámica los registros DNS del servidor SMB en DNS cuando mueve el servidor SMB a otro dominio, debe modificar el DNS dinámico (DDNS) en la máquina virtual de almacenamiento (SVM) antes de mover el servidor SMB.

Antes de empezar

Los servicios de nombres DNS se deben modificar en la SVM para utilizar el dominio DNS que contiene los registros de ubicación del servicio para el nuevo dominio que contendrá la cuenta de equipo del servidor SMB. Si utiliza DDNS seguro, debe utilizar servidores de nombres DNS integrados en Active Directory.

Acerca de esta tarea

Si bien DDNS (si se configura en la SVM) agrega automáticamente los registros DNS de las LIF de datos al dominio nuevo, los registros DNS del dominio original no se eliminan automáticamente del servidor DNS original. Debe eliminarlos manualmente.

Para completar las modificaciones de DDNS antes de mover el servidor SMB, consulte el siguiente tema:

"Configure los servicios DNS dinámicos"

Únase a las SVM de SMB de ONTAP a los dominios de Active Directory

Puede unir una máquina virtual de almacenamiento (SVM) a un dominio de Active Directory sin eliminar el servidor SMB existente mediante la modificación del dominio con `vserver cifs modify` el comando. Puede volver a unirse al dominio actual o unirse a uno nuevo.

Antes de empezar

- La SVM ya debe tener una configuración de DNS.
- La configuración de DNS para la SVM debe poder servir el dominio de destino.

  Los servidores DNS deben contener los registros de ubicación de servicio (SRV) para el LDAP de dominio y los servidores del controlador de dominio.

Acerca de esta tarea

- El estado administrativo del servidor CIFS debe estar configurado para `down` continuar con la modificación del dominio de Active Directory.
- Si el comando se completa correctamente, el estado administrativo se establece automáticamente en `up`. Obtenga más información sobre `up` en el "Referencia de comandos del ONTAP".
- Al unirse a un dominio, este comando puede tardar varios minutos en completarse.

Pasos

1. Una la SVM al dominio del servidor CIFS: `vserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`* `-status-admin down`

   Obtenga más información sobre `vserver cifs modify` en el "Referencia de comandos del ONTAP". Si necesita reconfigurar DNS para el nuevo dominio, obtenga más información `vserver dns modify` en el "Referencia de comandos del ONTAP".

   Para crear una cuenta de máquina de Active Directory para el servidor SMB, debe proporcionar el nombre y la contraseña de una cuenta de Windows con suficiente Privileges para agregar equipos al `ou=` *`example`* `ou` contenedor dentro del *`example`* dominio .com.

   A partir de ONTAP 9.7, el administrador de AD puede proporcionarle un URI a un archivo keytab como alternativa a proporcionarle un nombre y una contraseña a una cuenta de Windows con privilegios. Cuando reciba el URI, inclúyalo en el `-keytab-uri` parámetro con `vserver cifs` los comandos.

2. Compruebe que el servidor CIFS se encuentra en el dominio de Active Directory deseado: `vserver cifs show`

Ejemplo

En el siguiente ejemplo, el servidor SMB «'CIFSSERVER1'» de la SVM vs1 se une al dominio example.com mediante la autenticación keytab:

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab

cluster1::> vserver cifs show

          Server       Status       Domain/Workgroup  Authentication
Vserver   Name         Admin        Name              Style
--------- -----------  ---------    ----------------  --------------
vs1       CIFSSERVER1  up           EXAMPLE          domain
```

Mostrar información acerca de las conexiones SMB NetBIOS over TCP de ONTAP

Puede mostrar información acerca de las conexiones NetBIOS sobre TCP (NBT). Esto puede ser útil para solucionar problemas relacionados con NetBIOS.

Paso

1. Utilice el `vserver cifs nbtstat` comando para mostrar información acerca de las conexiones NetBIOS a través de TCP.

> No se admite el servicio de nombres NetBIOS (NBNS) sobre IPv6.

Ejemplo

En el siguiente ejemplo se muestra la información del servicio de nombres NetBIOS que se muestra para "'cluster1'":

```
cluster1::> vserver cifs nbtstat

          Vserver: vs1
          Node:    cluster1-01
          Interfaces:
                   10.10.10.32
                   10.10.10.33
         Servers:
                   17.17.1.2  (active  )
         NBT Scope:
                  [ ]
         NBT Mode:
                  [h]
         NBT Name    NetBIOS Suffix   State   Time Left   Type
         ----------- ---------------  ------- ---------   -----
         CLUSTER_1   00               wins    57
         CLUSTER_1   20               wins    57

         Vserver: vs1
         Node:    cluster1-02
         Interfaces:
                 10.10.10.35
         Servers:
                 17.17.1.2  (active  )
         CLUSTER_1          00               wins          58
         CLUSTER_1          20               wins          58
         4 entries were displayed.
```

Comandos de ONTAP para gestionar servidores SMB

Debe conocer los comandos para crear, mostrar, modificar, detener, iniciar, Y eliminando servidores SMB. También hay comandos para restablecer y volver a detectar servidores, cambiar o restablecer contraseñas de cuentas de equipo, programar cambios para contraseñas de cuentas de equipo y agregar o quitar alias de NetBIOS.

Si desea…	Se usa este comando…
Cree un servidor SMB	`vserver cifs create`
Muestra información acerca de un servidor SMB	`vserver cifs show`
Modificar un servidor SMB	`vserver cifs modify`
Mover un servidor SMB a otro dominio	`vserver cifs modify`

Detener un servidor SMB	`vserver cifs stop`
Inicie un servidor SMB	`vserver cifs start`
Suprimir un servidor SMB	`vserver cifs delete`
Restablecer y volver a detectar servidores para el servidor SMB	`vserver cifs domain discovered-servers reset-servers`
Cambiar la contraseña de la cuenta de equipo del servidor SMB	`vserver cifs domain password change`
Restablezca la contraseña de la cuenta de máquina del servidor SMB	`vserver cifs domain password change`
Programar cambios automáticos de contraseña para la cuenta de equipo del servidor SMB	`vserver cifs domain password schedule modify`
Agregue alias NetBIOS para el servidor SMB	`vserver cifs add-netbios-aliases`
Elimine los alias de NetBIOS para el servidor SMB	`vserver cifs remove-netbios-aliases`

Obtenga más información sobre `vserver cifs` en el "Referencia de comandos del ONTAP".

Información relacionada

"Qué sucede a los usuarios locales y grupos al eliminar servidores SMB"

Habilite el servicio de nombres NetBIOS SMB de ONTAP

A partir de ONTAP 9, el servicio de nombres NetBIOS (NBNS, a veces denominado Servicio de nombres Internet de Windows o WINS) está deshabilitado de forma predeterminada. Anteriormente, las máquinas virtuales de almacenamiento (SVM) habilitadas para CIFS enviaron registros de nombres independientemente de si se habilitó WINS en una red. Para limitar dichas emisiones a configuraciones en las que se necesita NBNS, debe habilitar NBNS explícitamente para servidores CIFS nuevos.

Antes de empezar

- Si ya está utilizando NBNS y actualiza a ONTAP 9, no es necesario completar esta tarea. NBNS continuará trabajando como antes.
- NBNS está habilitado en UDP (puerto 137).
- No se admite NBNS sobre IPv6.

Pasos

1. Configure el nivel de privilegio en Advanced.

```
set -privilege advanced
```

2. Habilite NBNS en un servidor CIFS.

```
vserver cifs options  modify -vserver <vserver name> -is-nbns-enabled
true
```

3. Vuelva al nivel de privilegio de administrador.

```
set -privilege admin
```

Utilice IPv6 para el acceso a SMB y los servicios SMB

Obtenga más información sobre los requisitos del bloque de mensajes del servidor de ONTAP para IPv6

Antes de poder utilizar IPv6 en el servidor SMB, debe saber qué versiones de ONTAP y SMB admiten y cuáles son los requisitos de licencia.

Requisitos para la licencia de ONTAP

No se requiere ninguna licencia especial para IPv6 cuando SMB tiene licencia. La licencia SMB se incluye con "ONTAP One". Si no tiene ONTAP One y la licencia no está instalada, póngase en contacto con su representante de ventas.

Requisitos de la versión del protocolo SMB

- Para las SVM, ONTAP es compatible con IPv6 en todas las versiones del protocolo SMB.

No se admite el servicio de nombres NetBIOS (NBNS) sobre IPv6.

Descubre el soporte para IPv6 con acceso SMB de ONTAP y servicios CIFS

Si desea usar IPv6 en el servidor CIFS, debe saber cómo ONTAP admite IPv6 para el acceso SMB y la comunicación de redes para servicios CIFS.

Compatibilidad con clientes y servidores Windows

ONTAP ofrece compatibilidad con los servidores y clientes de Windows que admiten IPv6. A continuación se describe la compatibilidad con IPv6 del cliente Microsoft Windows y el servidor:

- Windows 7, Windows 8, Windows Server 2008, Windows Server 2012 y versiones posteriores admiten IPv6 tanto para el uso compartido de archivos SMB como para los servicios de Active Directory, incluidos los servicios DNS, LDAP, CLDAP y Kerberos.

  Si se han configurado direcciones IPv6, Windows 7 y Windows Server 2008 y versiones posteriores utilizan IPv6 de forma predeterminada para los servicios de Active Directory. Se admiten tanto la autenticación NTLM como la autenticación Kerberos a través de conexiones IPv6.

Todos los clientes de Windows compatibles con ONTAP pueden conectarse a recursos compartidos de SMB mediante direcciones IPv6.

Para obtener la información más reciente sobre los clientes de Windows que admite ONTAP, consulte la "Matriz de interoperabilidad".

Los dominios NT no son compatibles con IPv6.

Compatibilidad adicional con servicios CIFS

Además de la compatibilidad con IPv6 para recursos compartidos de archivos SMB y servicios de Active Directory, ONTAP ofrece compatibilidad con IPv6 para lo siguiente:

- Servicios de cliente, incluidas carpetas sin conexión, perfiles de itinerancia, redirección de carpetas y versiones anteriores
- Servicios del lado del servidor, incluidos directorios iniciales dinámicos (funcionalidad de Home Directory), enlaces simbólicos y widgets, BranchCache, descarga de copias ODX, referencias automáticas a nodos, Y versiones anteriores
- Servicios de administración de acceso a archivos, incluido el uso de usuarios y grupos locales de Windows para el control de acceso y la administración de derechos, la configuración de permisos de archivos y políticas de auditoría mediante la CLI, el seguimiento de seguridad, la gestión de bloqueos de archivos y la supervisión de la actividad de SMB
- Auditoría multiprotocolo de NAS
- FPolicy
- Recursos compartidos disponibles de forma continua, protocolo de observación y VSS remoto (utilizado con configuraciones de Hyper-V en SMB)

Servicio de nombres y soporte del servicio de autenticación

La comunicación con los siguientes servicios de nombres se admite con IPv6:

- Controladores de dominio
- Servidores DNS
- Servidores LDAP
- Servidores KDC
- Servidores NIS

Descubra cómo los servidores SMB de ONTAP utilizan IPv6 para conectarse a servidores externos

Para crear una configuración que cumpla con sus requisitos, debe saber cómo usan IPv6 los servidores CIFS a la hora de realizar conexiones a servidores externos.

- Selección de direcciones de origen

  Si se intenta conectarse a un servidor externo, la dirección de origen seleccionada debe ser del mismo tipo que la dirección de destino. Por ejemplo, si se conecta a una dirección IPv6, la máquina virtual de almacenamiento (SVM) que aloja el servidor CIFS debe tener una LIF de datos o una LIF de gestión que tenga una dirección IPv6 que se usará como dirección de origen. Del mismo modo, si se conecta a una dirección IPv4, la SVM debe tener una LIF de datos o una LIF de gestión que tenga una dirección IPv4

que se usará como dirección de origen.

- Para los servidores detectados dinámicamente mediante DNS, la detección de servidores se realiza de la siguiente manera:
  - Si IPv6 está deshabilitado en el clúster, solo se detectan direcciones de los servidores IPv4.
  - Si IPv6 está habilitado en el clúster, se detectan tanto las direcciones de los servidores IPv4 como IPv6. Cualquiera de los dos tipos puede utilizarse en función de la idoneidad del servidor al que pertenece la dirección y de la disponibilidad de LIF de gestión o datos IPv6 o IPv4. La detección dinámica de servidores se utiliza para detectar controladores de dominio y sus servicios asociados, como LSA, NETLOGON, Kerberos y LDAP.
- Conectividad del servidor DNS

  Si la SVM utiliza IPv6 al conectarse a un servidor DNS depende de la configuración de los servicios de nombres DNS. Si los servicios DNS se configuran para utilizar direcciones IPv6, las conexiones se realizan mediante IPv6. Si lo desea, la configuración de los servicios de nombres DNS puede utilizar direcciones IPv4 para que las conexiones con los servidores DNS sigan usando direcciones IPv4. Las combinaciones de direcciones IPv4 e IPv6 pueden especificarse al configurar los servicios de nombres DNS.
- Conectividad del servidor LDAP

  Si la SVM utiliza IPv6 al conectarse a un servidor LDAP depende de la configuración del cliente LDAP. Si el cliente LDAP está configurado para usar direcciones IPv6, las conexiones se realizan mediante IPv6. Si lo desea, la configuración del cliente LDAP puede usar direcciones IPv4 a fin de que las conexiones con servidores LDAP sigan usando direcciones IPv4. Al configurar la configuración del cliente LDAP, se pueden especificar las combinaciones de direcciones IPv4 e IPv6.

  > La configuración del cliente LDAP se utiliza al configurar LDAP para los servicios de nombre de usuario, grupo y grupo de redes de UNIX.
- Conectividad del servidor NIS

  Si la SVM utiliza IPv6 al conectarse a un servidor NIS depende de la configuración de los servicios de nombres NIS. Si los servicios NIS se configuran para utilizar direcciones IPv6, las conexiones se realizan mediante IPv6. Si lo desea, la configuración de los servicios de nombres NIS puede utilizar direcciones IPv4 para que las conexiones con los servidores NIS sigan usando direcciones IPv4. Las combinaciones de direcciones IPv4 e IPv6 pueden especificarse al configurar los servicios de nombres NIS.

  > Los servicios de nombres NIS se utilizan para almacenar y administrar objetos de usuario, grupo, grupo de red y nombre de host de UNIX.

Información relacionada

- Habilitar IPv6 para servidores
- Supervisar y mostrar información sobre sesiones IPv6

Habilite IPv6 para los servidores SMB de ONTAP

Las redes IPv6 no se habilitan durante la configuración del clúster. Un administrador de clúster debe habilitar IPv6 después de que la configuración del clúster se haya completado a fin de usar IPv6 para SMB. Cuando el administrador de clúster habilita IPv6, se habilita para todo el clúster.

Paso

1. Habilitar IPv6: `network options ipv6 modify -enabled true`

   IPv6 está habilitado. Se pueden configurar LIF de datos IPv6 para el acceso SMB.

Información relacionada

- Supervisar y mostrar información sobre sesiones IPv6
- "Visualice la red mediante System Manager"
- "Habilitación de IPv6 en el clúster"
- "opciones de red ipv6 modificar"

Obtenga información sobre cómo deshabilitar IPv6 para servidores SMB de ONTAP

Aunque IPv6 esté habilitado en el clúster mediante una opción de red, no puede deshabilitar IPv6 para SMB con el mismo comando. En su lugar, ONTAP deshabilita IPv6 cuando el administrador de clúster deshabilita la última interfaz habilitada para IPv6 en el clúster. Debe comunicarse con el administrador de clúster acerca de la gestión de las interfaces IPv6 habilitadas.

Información relacionada

- "Visualizar la red de ONTAP mediante System Manager"

Supervise y muestre información acerca de las sesiones SMB de IPv6 ONTAP

Puede supervisar y mostrar información sobre las sesiones SMB conectadas mediante redes IPv6. Esta información es útil para determinar qué clientes se conectan mediante IPv6, así como otra información útil sobre las sesiones SMB de IPv6.

Paso

1. Realice la acción deseada:

Si desea determinar si…	Introduzca el comando…
Las sesiones SMB a una máquina virtual de almacenamiento (SVM) se conectan mediante IPv6	`vserver cifs session show -vserver` *`vserver_name`* `-instance`
IPv6 se utiliza para sesiones SMB a través de una dirección LIF especificada	`vserver cifs session show -vserver` *`vserver_name`* `-lif-address` *`LIF_IP_address`* `-instance` *`LIF_IP_address`* Es la dirección IPv6 de la LIF de datos.

Configurar el acceso a archivos mediante SMB

Configurar estilos de seguridad

Cómo afectan los estilos de seguridad al acceso a los datos

Obtén más información sobre los estilos de seguridad del bloque de mensajes del servidor de ONTAP y sus efectos

Hay cuatro estilos de seguridad diferentes: UNIX, NTFS, mixto y unificado. Cada estilo de seguridad tiene un efecto diferente sobre cómo se gestionan los permisos para los datos. Debe comprender los diferentes efectos para asegurarse de que selecciona el estilo de seguridad adecuado para sus propósitos.

Es importante entender que los estilos de seguridad no determinan qué tipos de clientes pueden o no pueden tener acceso a los datos. Los estilos de seguridad sólo determinan el tipo de permisos que ONTAP utiliza para controlar el acceso a los datos y qué tipo de cliente puede modificar estos permisos.

Por ejemplo, si un volumen utiliza el estilo de seguridad UNIX, los clientes SMB todavía pueden acceder a los datos (siempre y cuando estos se autentiquen y autoricen correctamente) debido a la naturaleza multiprotocolo de ONTAP. Sin embargo, ONTAP utiliza permisos UNIX que sólo los clientes UNIX pueden modificar mediante herramientas nativas.

Estilo de seguridad	Clientes que pueden modificar permisos	Permisos que pueden utilizar los clientes	El estilo de seguridad efectivo resultante	Clientes que pueden acceder a los ficheros
UNIX	NFS	Bits del modo NFSv3	UNIX	NFS y SMB
		ACL de NFSv4.x		
NTFS	SMB	ACL de NTFS	NTFS	
Mixto	NFS o SMB	Bits del modo NFSv3	UNIX	
		NFSv4.ACLs		
		ACL de NTFS	NTFS	
Unificado (solo para Infinite Volume, en ONTAP 9.4 y versiones anteriores).	NFS o SMB	Bits del modo NFSv3	UNIX	
		ACL de NFSv4.1		
		ACL de NTFS	NTFS	

Los volúmenes de FlexVol son compatibles con UNIX, NTFS y estilos de seguridad mixtos. Cuando el estilo de seguridad es mixto o unificado, los permisos efectivos dependen del tipo de cliente que modificó por última vez los permisos porque los usuarios establecen el estilo de seguridad de forma individual. Si el último cliente que modificó permisos era un cliente NFSv3, los permisos son bits del modo NFSv3 de UNIX. Si el último cliente era un cliente NFSv4, los permisos son ACL de NFSv4. Si el último cliente era un cliente SMB, los permisos son ACL de Windows NTFS.

El estilo de seguridad unificado solo está disponible en Infinite Volume, que ya no son compatibles con ONTAP 9.5 y versiones posteriores. Para obtener más información, consulte Información general de gestión de volúmenes de FlexGroup.

El `show-effective-permissions` parámetro con el `vserver security file-directory` El comando le permite mostrar los permisos efectivos otorgados a un usuario de Windows o UNIX en la ruta de archivo o carpeta especificada. Además, el parámetro opcional `-share-name` le permite mostrar el permiso de uso compartido efectivo. Obtenga más información sobre `vserver security file-directory show-effective-permissions` en el "Referencia de comandos del ONTAP".

> ONTAP establece inicialmente algunos permisos de archivo predeterminados. De forma predeterminada, el estilo de seguridad efectivo de todos los datos de los volúmenes de estilo de seguridad mixto y unificado es UNIX y el tipo de permisos efectivos es bits de modo UNIX (0755 a menos que se especifique lo contrario) hasta que un cliente lo configure como permite el estilo de seguridad predeterminado. De forma predeterminada, el estilo de seguridad efectivo en todos los datos de los volúmenes de estilo de seguridad NTFS es NTFS y tiene una ACL que permite un control total para todos.

Información relacionada

- "Referencia de comandos del ONTAP"

Obtén información sobre dónde y cuándo establecer los estilos de seguridad de SMB de ONTAP

Los estilos de seguridad se pueden establecer en volúmenes de FlexVol (tanto volúmenes raíz como de datos) y qtrees. Los estilos de seguridad se pueden configurar manualmente en el momento de la creación, heredados automáticamente o modificados posteriormente.

Decida qué estilos de seguridad de SMB se utilizarán en las SVM de ONTAP

Para ayudar a decidir qué estilo de seguridad se debe usar en un volumen, se deben tener en cuenta dos factores. El factor principal es el tipo de administrador que administra el sistema de archivos. El factor secundario es el tipo de usuario o servicio que tiene acceso a los datos del volumen.

Al configurar el estilo de seguridad en un volumen, debe tener en cuenta las necesidades del entorno para garantizar que selecciona el mejor estilo de seguridad y evitar problemas con la gestión de permisos. Las siguientes consideraciones pueden ayudarle a decidir:

Estilo de seguridad	Elija si…
UNIX	• Un administrador de UNIX gestiona el sistema de ficheros. • La mayoría de los usuarios son clientes NFS. • Una aplicación que accede a los datos utiliza un usuario UNIX como cuenta de servicio.
NTFS	• Un administrador de Windows gestiona el sistema de archivos. • La mayoría de los usuarios son clientes SMB. • Una aplicación que accede a los datos utiliza un usuario de Windows como cuenta de servicio.

Estilo de seguridad	Elija si…
Mixto	El sistema de archivos lo gestionan administradores de UNIX y Windows, y los usuarios están formados por clientes NFS y SMB.

Obtenga información sobre la herencia del estilo de seguridad del bloque de mensajes del servidor de ONTAP

Si no especifica el estilo de seguridad al crear un nuevo volumen de FlexVol o un qtree, hereda su estilo de seguridad de formas diferentes.

Los estilos de seguridad se heredan de la siguiente manera:

- Un volumen FlexVol hereda el estilo de seguridad del volumen raíz de su SVM que contiene.
- Un qtree hereda el estilo de seguridad del volumen FlexVol que contiene.
- Un archivo o un directorio hereda el estilo de seguridad de su volumen o qtree de FlexVol.

Obtenga más información sobre la conservación de permisos UNIX para volúmenes de FlexVol SMB de ONTAP

Cuando las aplicaciones Windows editan y guardan archivos de un volumen FlexVol que actualmente tienen permisos UNIX, ONTAP puede preservar los permisos UNIX.

Cuando las aplicaciones de clientes de Windows editan y guardan archivos, leen las propiedades de seguridad del archivo, crean un nuevo archivo temporal, aplican esas propiedades al archivo temporal y, a continuación, asignan al archivo temporal el nombre de archivo original.

Cuando los clientes de Windows realizan una consulta para las propiedades de seguridad, reciben una ACL construida que representa exactamente los permisos de UNIX. El único propósito de esta ACL construida es preservar los permisos UNIX del archivo a medida que las aplicaciones de Windows actualizan los archivos para garantizar que los archivos resultantes tengan los mismos permisos UNIX. ONTAP no establece ninguna ACL de NTFS usando la ACL construida.

Obtenga información sobre la gestión de permisos UNIX mediante la ficha Seguridad de Windows para servidores SMB de ONTAP

Si desea manipular los permisos de UNIX de archivos o carpetas en volúmenes o qtrees de estilo de seguridad mixtos en las SVM, puede utilizar la pestaña Seguridad en clientes de Windows. También puede utilizar aplicaciones que puedan consultar y establecer ACL de Windows.

- Modificación de permisos de UNIX

  Puede usar la pestaña Seguridad de Windows para ver y cambiar los permisos de UNIX para un volumen o un qtree de estilo de seguridad mixto. Si utiliza la ficha Seguridad de Windows principal para cambiar los permisos de UNIX, primero debe quitar la ACE existente que desea editar (esto establece los bits de modo en 0) antes de realizar los cambios. De forma alternativa, puede utilizar el editor avanzado para cambiar los permisos.

  Si se utilizan permisos de modo, puede cambiar directamente los permisos de modo para el UID, GID y

otros (todos los demás con una cuenta en el equipo) de la lista. Por ejemplo, si el UID mostrado tiene permisos r-x, puede cambiar los permisos de UID a rwx.

- Cambiar los permisos de UNIX a los permisos NTFS

  Puede usar la pestaña Seguridad de Windows para reemplazar objetos de seguridad UNIX por objetos de seguridad de Windows en un volumen o qtree de estilo de seguridad mixto donde los archivos y carpetas tienen un estilo de seguridad efectivo de UNIX.

  Primero debe quitar todas las entradas de permisos de UNIX enumeradas antes de que pueda reemplazarlas con los objetos de usuario y grupo de Windows deseados. A continuación, puede configurar ACL basados en NTFS en los objetos Usuario y Grupo de Windows. Si quita todos los objetos de seguridad de UNIX y agrega sólo usuarios y grupos de Windows a un archivo o carpeta de un volumen o qtree de estilo de seguridad mixto, cambie el estilo de seguridad efectivo del archivo o carpeta de UNIX a NTFS.

  Al cambiar los permisos de una carpeta, el comportamiento predeterminado de Windows es propagar estos cambios a todas las subcarpetas y archivos. Por lo tanto, debe cambiar la opción de propagación a la configuración deseada si no desea propagar un cambio en el estilo de seguridad a todas las carpetas secundarias, subcarpetas y archivos.

Configure los estilos de seguridad SMB en volúmenes raíz de SVM de ONTAP

El estilo de seguridad del volumen raíz de la máquina virtual de almacenamiento (SVM) se configura para determinar el tipo de permisos utilizados para los datos en el volumen raíz de la SVM.

Pasos

1. Utilice `vserver create` el comando con `-rootvolume-security-style` el parámetro para definir el estilo de seguridad.

   Las posibles opciones para el estilo de seguridad del volumen raíz son `unix` `ntfs` , , o `mixed`.

2. Muestre y verifique la configuración, incluido el estilo de seguridad del volumen raíz de la SVM que creó: `vserver show -vserver` *`vserver_name`*

Configure los estilos de seguridad de SMB en volúmenes de ONTAP FlexVol

El estilo de seguridad del volumen FlexVol se configura para determinar el tipo de permisos utilizados para los datos en volúmenes FlexVol de la máquina virtual de almacenamiento (SVM).

Pasos

1. Ejecute una de las siguientes acciones:

Si el volumen de FlexVol…	Usar el comando…
Aún no existe	`volume create` e incluya el `-security-style` parámetro para especificar el estilo de seguridad.

Ya existe	`volume modify` e incluya el `-security-style` parámetro para especificar el estilo de seguridad.

Las opciones posibles para el estilo de seguridad de FlexVol volume son `unix` `ntfs` , o `mixed`.

Si no se especifica un estilo de seguridad al crear un volumen FlexVol, el volumen hereda el estilo de seguridad del volumen raíz.

Para obtener más información acerca de los `volume create` `volume modify` comandos o, consulte "Gestión de almacenamiento lógico".

2. Para ver la configuración, incluido el estilo de seguridad del volumen FlexVol que se creó, escriba el siguiente comando:

```
volume show -volume volume_name -instance
```

Configure los estilos de seguridad de SMB en qtrees de ONTAP

El estilo de seguridad del volumen de qtrees se configura para determinar el tipo de permisos utilizados para los datos en qtrees.

Pasos

1. Ejecute una de las siguientes acciones:

Si el qtree…	Usar el comando…
Aún no existe	`volume qtree create` e incluya el `-security -style` parámetro para especificar el estilo de seguridad.
Ya existe	`volume qtree modify` e incluya el `-security -style` parámetro para especificar el estilo de seguridad.

Las posibles opciones para el estilo de seguridad de qtree son `unix` `ntfs` , o `mixed`.

Si no se especifica un estilo de seguridad al crear un qtree, el estilo de seguridad predeterminado es `mixed`.

Para obtener más información acerca de los `volume qtree create` `volume qtree modify` comandos o, consulte "Gestión de almacenamiento lógico".

2. Para mostrar la configuración, incluido el estilo de seguridad del qtree creado, escriba el siguiente comando: `volume qtree show -qtree qtree_name -instance`

Cree y gestione volúmenes de datos en espacios de nombres NAS

Obtenga más información sobre la creación y la gestión de volúmenes de datos de bloque de mensajes del servidor de ONTAP en espacios de nombres NAS

Para gestionar el acceso a archivos en un entorno NAS, debe gestionar volúmenes de datos y puntos de unión en la máquina virtual de almacenamiento (SVM). Esto incluye planificar la arquitectura de espacios de nombres, crear volúmenes con o sin puntos de unión, montar o desmontar volúmenes, y mostrar información sobre volúmenes de datos y espacios de nombres de servidores NFS o servidores CIFS.

Crear volúmenes de datos del bloque de mensajes del servidor de ONTAP con puntos de unión especificados

Puede especificar el punto de unión cuando crea un volumen de datos. El volumen resultante se monta automáticamente en el punto de unión y se puede configurar inmediatamente para el acceso NAS.

Antes de empezar

El agregado en el que desea crear el volumen ya debe existir.

> Los siguientes caracteres no se pueden utilizar en la ruta de unión: * # " > < | ? \
>
> Además, la longitud de la ruta de unión no puede ser superior a 255 caracteres.

Pasos

1. Cree el volumen con un punto de unión: `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path` *`junction_path`*

   La ruta de unión debe comenzar con la raíz (/) y puede contener tanto directorios como volúmenes con conexiones. No es necesario que la ruta de unión contenga el nombre del volumen. Las rutas de unión son independientes del nombre del volumen.

   Es opcional especificar un estilo de seguridad del volumen. Si no se especifica un estilo de seguridad, ONTAP crea el volumen con el mismo estilo de seguridad que se aplica al volumen raíz de la máquina virtual de almacenamiento (SVM). Sin embargo, es posible que el estilo de seguridad del volumen raíz no sea el estilo de seguridad que se desea aplicar al volumen de datos que se crea. La recomendación es especificar el estilo de seguridad al crear el volumen para minimizar los problemas de acceso a archivos difíciles de solucionar.

   La ruta de unión no distingue mayúsculas de minúsculas; `/ENG` es la misma que `/eng`. Si crea un recurso compartido CIFS, Windows trata la ruta de unión como si fuera sensible a mayúsculas de minúsculas. Por ejemplo, si la unión es `/ENG`, la ruta de acceso de un recurso compartido CIFS debe comenzar por `/ENG`, no por `/eng` .

   Existen muchos parámetros opcionales que se pueden usar para personalizar un volumen de datos. Obtenga más información sobre `volume create` en el "Referencia de comandos del ONTAP".

2. Compruebe que el volumen se creó con el punto de unión deseado: `volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-junction`

Ejemplo

En el ejemplo siguiente se crea un volumen llamado «`home4`» ubicado en la SVM VS1 que tiene una ruta de unión `/eng/home`:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

Crear volúmenes de datos del bloque de mensajes del servidor de ONTAP sin especificar puntos de unión

Puede crear un volumen de datos sin especificar un punto de unión. El volumen resultante no se monta automáticamente y no se puede configurar para acceso NAS. Debe montar el volumen para poder configurar los recursos compartidos de SMB o las exportaciones de NFS de ese volumen.

Antes de empezar

El agregado en el que desea crear el volumen ya debe existir.

Pasos

1. Cree el volumen sin un punto de unión mediante el siguiente comando: `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}`

   Es opcional especificar un estilo de seguridad del volumen. Si no se especifica un estilo de seguridad, ONTAP crea el volumen con el mismo estilo de seguridad que se aplica al volumen raíz de la máquina virtual de almacenamiento (SVM). Sin embargo, es posible que el estilo de seguridad del volumen raíz no sea el estilo de seguridad que se desea aplicar al volumen de datos. La recomendación es especificar el estilo de seguridad al crear el volumen para minimizar los problemas de acceso a archivos difíciles de solucionar.

   Existen muchos parámetros opcionales que se pueden usar para personalizar un volumen de datos. Obtenga más información sobre `volume create` en el "Referencia de comandos del ONTAP".

2. Compruebe que el volumen se creó sin un punto de unión: `volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-junction`

Ejemplo

En el siguiente ejemplo se crea un volumen denominado «números» ubicado en la SVM vs1 que no se monta en un punto de unión:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                    Junction                 Junction
Vserver   Volume    Active   Junction Path   Path Source
--------- --------- -------- --------------- -----------
vs1       data      true     /data           RW_volume
vs1       home4     true     /eng/home       RW_volume
vs1       vs1_root  -        /               -
vs1       sales     -        -               -
```

Monte o desmonte volúmenes SMB de ONTAP existentes en el espacio de nombres NAS

Un volumen se debe montar en el espacio de nombres NAS para poder configurar el acceso de clientes NAS a los datos contenidos en los volúmenes de la máquina virtual de almacenamiento (SVM). Puede montar un volumen en un punto de unión si no está montado actualmente. También es posible desmontar volúmenes.

Acerca de esta tarea

Si desmonta y desconecta un volumen, los clientes NAS no pueden acceder a todos los datos dentro del punto de unión, incluidos los datos en los volúmenes con puntos de unión ubicados en el espacio de nombres del volumen sin montar.

> Para interrumpir el acceso de un cliente NAS a un volumen, no basta con desmontar el volumen. Debe desconectar el volumen o realizar otros pasos para garantizar que las cachés del identificador de archivos del cliente se invaliden. Para obtener más información, consulte el siguiente artículo de la base de conocimientos: "Los clientes NFSv3 siguen teniendo acceso a un volumen después de eliminarse del espacio de nombres de ONTAP"

Cuando desmonta y desconecta un volumen, no se pierden datos dentro del volumen. Además, se conservan las políticas de exportación de volúmenes existentes y los recursos compartidos de SMB creados en el volumen o en directorios y puntos de unión dentro del volumen desmontado. Si vuelve a montar el volumen desmontado, los clientes NAS pueden acceder a los datos contenidos en el volumen mediante políticas de exportación y recursos compartidos SMB existentes.

Pasos

1. Realice la acción deseada:

Si desea…	Introduzca los comandos…
Montar un volumen	`volume mount -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction-path` *`junction_path`*

Si desea…	Introduzca los comandos…

Desmontar un volumen	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. Compruebe que el volumen esté en el estado de montaje deseado:

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

Ejemplos

El siguiente ejemplo monta un volumen llamado “sales” ubicado en SVM “VS1” al punto de unión “`/sales`”:

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

El siguiente ejemplo desmonta y desconecta un volumen llamado “data” ubicado en la SVM “VS1”:

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

Muestra la información del punto de unión y el montaje de volúmenes de SMB de ONTAP

Puede ver información sobre los volúmenes montados para las máquinas virtuales de almacenamiento (SVM) y los puntos de unión a los que están montados los volúmenes. También puede determinar qué volúmenes no están montados en un punto de unión.

Esta información se puede usar para comprender y gestionar el espacio de nombres de la SVM.

Pasos

1. Realice la acción deseada:

Si desea mostrar…	Introduzca el comando…
Información resumida sobre los volúmenes montados y desmontados en la SVM	`volume show -vserver vserver_name -junction`
Información detallada sobre los volúmenes montados y desmontados en la SVM	`volume show -vserver vserver_name -volume volume_name -instance`
Información específica sobre los volúmenes montados y desmontados en la SVM	a. Si es necesario, puede mostrar campos válidos para el `-fields` parámetro mediante el siguiente comando: `volume show -fields ?` b. Muestre la información deseada mediante `-fields` el parámetro: Volume show -vserver vserver_name -fields fieldname,…

Ejemplos

En el siguiente ejemplo, se muestra un resumen de los volúmenes montados y desmontados en la SVM vs1:

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

En el siguiente ejemplo, se muestra información sobre campos especificados para los volúmenes ubicados en la SVM vs2:

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

Configurar las asignaciones de nombres

Obtenga más información sobre ONTAP la configuración de las asignaciones de nombres del bloque de mensajes del servidor

ONTAP utiliza la asignación de nombres para asignar identidades CIFS a identidades UNIX, identidades Kerberos a identidades UNIX e identidades UNIX a identidades CIFS. Necesita esta información para obtener credenciales de usuario y proporcionar un acceso adecuado a los archivos independientemente de si se están conectando desde un cliente NFS o un cliente CIFS.

Existen dos excepciones en las que no es necesario utilizar la asignación de nombres:

- Configura un entorno UNIX puro y no planea usar el acceso CIFS o el estilo de seguridad NTFS en los volúmenes.
- En su lugar, puede configurar el usuario predeterminado que se utilizará.

  En este escenario, no es necesario asignar nombres porque en lugar de asignar cada credencial de cliente individual todas las credenciales de cliente se asignan al mismo usuario predeterminado.

Tenga en cuenta que sólo puede utilizar la asignación de nombres para usuarios, no para grupos.

Sin embargo, puede asignar un grupo de usuarios individuales a un usuario específico. Por ejemplo, puede

asignar todos los usuarios de AD que comiencen o terminen con la palabra SALES a un usuario UNIX específico y al UID del usuario.

Obtenga más información sobre la asignación de nombres SMB de ONTAP

Cuando ONTAP tiene que asignar credenciales para un usuario, primero comprueba la base de datos de asignación de nombres local y el servidor LDAP para buscar una asignación existente. Si comprueba uno o ambos y en qué orden se determina mediante la configuración del servicio de nombres de la SVM.

- Para la asignación de Windows a UNIX

  Si no se encuentra ninguna asignación, ONTAP comprueba si el nombre de usuario de Windows en minúsculas es un nombre de usuario válido en el dominio UNIX. Si esto no funciona, utiliza el usuario UNIX predeterminado siempre que esté configurado. Si el usuario UNIX predeterminado no está configurado y ONTAP no puede obtener una asignación de esta manera, se produce un error en la asignación y se devuelve un error.

- De asignación de UNIX a Windows

  Si no se encuentra ninguna asignación, ONTAP intenta encontrar una cuenta de Windows que coincida con el nombre UNIX en el dominio SMB. Si esto no funciona, utiliza el usuario SMB predeterminado, siempre que esté configurado. Si el usuario CIFS predeterminado no está configurado y ONTAP no puede obtener una asignación de esta manera, se produce un error en la asignación y se devuelve un error.

Las cuentas de equipo se asignan al usuario UNIX predeterminado especificado de forma predeterminada. Si no se especifica ningún usuario UNIX predeterminado, las asignaciones de cuentas de equipo fallan.

- A partir de ONTAP 9.5, puede asignar cuentas de equipo a usuarios distintos del usuario UNIX predeterminado.
- En ONTAP 9.4 y versiones anteriores, no es posible asignar cuentas de equipo a otros usuarios.

  Incluso si se definen las asignaciones de nombre para las cuentas de equipo, las asignaciones se omiten.

Obtenga información sobre las búsquedas multidominio de SMB de ONTAP para asignaciones de usuario de UNIX a nombre de usuario de Windows

ONTAP admite las búsquedas multidominio al asignar usuarios de UNIX a usuarios de Windows. Se buscan todos los dominios de confianza detectados para que coincidan con el patrón de reemplazo hasta que se devuelva un resultado coincidente. También puede configurar una lista de dominios de confianza preferidos, que se utiliza en lugar de la lista de dominios de confianza detectados y se busca en orden hasta que se devuelve un resultado coincidente.

Cómo afectan las confianzas de dominio a las búsquedas de asignación de nombres de usuario de UNIX a Windows

Para comprender cómo funciona la asignación de nombres de usuario multidominio, debe comprender cómo funcionan las relaciones de confianza de dominios con ONTAP. Las relaciones de confianza de Active Directory con el dominio raíz del servidor CIFS pueden ser una confianza bidireccional o pueden ser uno de los dos tipos de confianzas unidireccionales, ya sea una confianza entrante o una confianza saliente. El dominio inicial es el dominio al que pertenece el servidor CIFS en la SVM.

- *Confianza bidireccional*

  Con confianzas bidireccionales, ambos dominios confían entre sí. Si el dominio principal del servidor CIFS tiene una confianza bidireccional con otro dominio, el dominio principal puede autenticar y autorizar a un usuario que pertenece al dominio de confianza y viceversa.

  Las búsquedas de asignación de nombres de usuario de UNIX a usuario de Windows sólo se pueden realizar en dominios con relaciones de confianza bidireccionales entre el dominio principal y el otro dominio.

- *Confianza saliente*

  Con una confianza saliente, el dominio principal confía en el otro dominio. En este caso, el dominio principal puede autenticar y autorizar a un usuario que pertenezca al dominio de confianza saliente.

  Se realiza una búsqueda en un dominio con una confianza saliente con el dominio principal al realizar búsquedas de asignación de nombres de usuario de UNIX a usuario de Windows.

- *Confianza entrante*

  Con una confianza entrante, el otro dominio confía en el dominio raíz del servidor CIFS. En este caso, el dominio principal no puede autenticar ni autorizar a un usuario que pertenezca al dominio de confianza entrante.

  Se busca un dominio con una confianza entrante con el dominio principal cuando se realizan búsquedas de asignación de nombres de usuario de UNIX a nombre de usuario de Windows.

Cómo se utilizan los comodines (*) para configurar las búsquedas multidominio para la asignación de nombres

Las búsquedas de asignación de nombres multidominio se facilitan mediante el uso de caracteres comodín en la sección de dominio del nombre de usuario de Windows. En la siguiente tabla se muestra cómo utilizar comodines en la parte de dominio de una entrada de asignación de nombres para habilitar las búsquedas multidominio:

Patrón	Sustitución	Resultado
raíz	*\\administrador	El usuario UNIX «'root'» está asignado al usuario denominado «'Administrator'». Todos los dominios de confianza se buscan en orden hasta que se encuentre el primer usuario coincidente denominado «'Administrator'».

Patrón	Sustitución	Resultado
*	**	Los usuarios UNIX válidos se asignan a los usuarios de Windows correspondientes. Todos los dominios de confianza se buscan en orden hasta que se encuentre el primer usuario que coincida con ese nombre. El patrón ** sólo es válido para la asignación de nombres de UNIX a Windows, no al revés.

Cómo se realizan las búsquedas de nombres multidominio

Puede elegir uno de los dos métodos para determinar la lista de dominios de confianza utilizados para las búsquedas de nombres multidominio:

- Utilice la lista de confianza bidireccional detectada automáticamente compilada por ONTAP
- Utilice la lista de dominios de confianza preferida que compila

Si un usuario de UNIX se asigna a un usuario de Windows con un comodín utilizado para la sección de dominio del nombre de usuario, se busca al usuario de Windows en todos los dominios de confianza de la siguiente manera:

- Si se configura una lista de dominio de confianza preferido, el usuario de Windows asignado se busca sólo en esta lista de búsqueda, en orden.
- Si no se configura una lista preferida de dominios de confianza, se busca al usuario de Windows en todos los dominios de confianza bidireccionales del dominio principal.
- Si no hay dominios de confianza bidireccional para el dominio principal, se busca al usuario en el dominio principal.

Si un usuario de UNIX está asignado a un usuario de Windows sin una sección de dominio en el nombre de usuario, se busca al usuario de Windows en el dominio principal.

Obtenga más información sobre las reglas de conversión de asignación de nombres SMB de ONTAP

Un sistema ONTAP mantiene un conjunto de reglas de conversión para cada SVM. Cada regla consta de dos piezas: Un *pattern* y un *substitut*. Las conversiones comienzan al principio de la lista apropiada y realizan una sustitución basada en la primera regla de coincidencia. El patrón es una expresión regular de estilo UNIX. El reemplazo es una cadena que contiene secuencias de escape que representan subexpresiones del patrón, como en el `sed` programa UNIX.

Crear asignación de nombres de SMB de ONTAP

Puede utilizar `vserver name-mapping create` el comando para crear una asignación de nombres. Se usan asignaciones de nombres para habilitar a los usuarios de Windows a fin de acceder a los volúmenes de estilo de seguridad de UNIX y al revés.

Acerca de esta tarea

Con cada SVM, ONTAP admite hasta 12,500 asignaciones de nombres para cada dirección.

Paso

1. Crear una asignación de nombres: `vserver name-mapping create -vserver` *`vserver_name`* `-direction {krb-unix|win-unix|unix-win} -position` *`integer`* `-pattern text -replacement` *`text`*

   > Las `-pattern -replacement` declaraciones y se pueden formular como expresiones regulares. También puede utilizar `-replacement` la sentencia para denegar explícitamente una asignación al usuario mediante la cadena de sustitución nula `" "` (el carácter de espacio). Obtenga más información sobre `vserver name-mapping create` en el "Referencia de comandos del ONTAP".

   Cuando se crean las asignaciones de Windows a UNIX, todos los clientes de SMB que tengan conexiones abiertas al sistema ONTAP en el momento en el que se creen las nuevas asignaciones deben cerrar e iniciar sesión para ver las nuevas asignaciones.

Ejemplos

El siguiente comando crea un mapa de nombre en la SVM llamada vs1. La asignación es una asignación de UNIX a Windows en la posición 1 de la lista de prioridades. La asignación asigna el usuario UNIX johnd al usuario de Windows ENG\JohnDoe.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

El siguiente comando crea otra asignación de nombre en la SVM llamada vs1. La asignación es una asignación de Windows a UNIX en la posición 1 de la lista de prioridades. Aquí el patrón y reemplazo incluyen expresiones regulares. La asignación asigna cada usuario CIFS del dominio ENG a los usuarios del dominio LDAP asociado con la SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

El siguiente comando crea otra asignación de nombre en la SVM llamada vs1. Aquí el patrón incluye "'$" como elemento del nombre de usuario de Windows que debe escaparse. La asignación asigna al usuario de Windows ENG\ john$OPS al usuario UNIX john_OPS.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

Configure el usuario SMB de ONTAP predeterminado

Puede configurar un usuario predeterminado para que lo utilice si todos los demás intentos de asignación fallan para un usuario o si no desea asignar usuarios individuales entre UNIX y Windows. Si desea que la autenticación de usuarios no asignados falle, no debe configurar un usuario predeterminado.

Acerca de esta tarea

Para la autenticación CIFS, si no desea asignar cada usuario de Windows a un usuario individual de UNIX, puede especificar un usuario predeterminado de UNIX.

Para la autenticación NFS, si no desea asignar cada usuario UNIX a un usuario individual de Windows, puede especificar un usuario predeterminado de Windows.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el siguiente comando…
Configure el usuario UNIX predeterminado	`vserver cifs options modify -default -unix-user` *`user_name`*
Configure el usuario predeterminado de Windows	`vserver nfs modify -default-win-user` *`user_name`*

Comandos de la ONTAP para gestionar asignaciones de nombre del bloque de mensajes del servidor

Hay comandos de la ONTAP específicos para gestionar las asignaciones de nombres.

Si desea…	Se usa este comando…
Cree una asignación de nombres	`vserver name-mapping create`
Inserte una asignación de nombres en una posición específica	`vserver name-mapping insert`
Mostrar asignaciones de nombres	`vserver name-mapping show`

Intercambiar la posición de dos asignaciones DE nombre NOTA: No se permite un intercambio cuando se configura la asignación de nombres con una entrada de calificador ip.	`vserver name-mapping swap`
Modificar una asignación de nombres	`vserver name-mapping modify`
Eliminar una asignación de nombres	`vserver name-mapping delete`
Validar la asignación de nombre correcta	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

Obtenga más información sobre `vserver name-mapping` en el "Referencia de comandos del ONTAP".

Configurar las búsquedas de asignación de nombres multidominio

Habilitar o deshabilitar las búsquedas de asignación de nombres multidominio de SMB de ONTAP

Con las búsquedas de asignación de nombres multidominio, puede utilizar una tarjeta comodín (*) en la parte de dominio de un nombre de Windows al configurar la asignación de nombres de usuario de UNIX a Windows. El uso de un comodín (*) en la parte de dominio del nombre permite a ONTAP buscar en todos los dominios que tienen una confianza bidireccional con el dominio que contiene la cuenta de equipo del servidor CIFS.

Acerca de esta tarea

Como alternativa a la búsqueda en todos los dominios de confianza bidireccional, puede configurar una lista de dominios de confianza preferidos. Cuando se configura una lista de dominios de confianza preferidos, ONTAP utiliza la lista de dominios de confianza preferidos en lugar de los dominios de confianza en ambas direcciones detectados para realizar búsquedas de asignación de nombres multidominio.

- Las búsquedas de asignación de nombres multidominio están activadas de manera predeterminada.
- Esta opción está disponible en el nivel de privilegio avanzado.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

Si desea que las búsquedas de asignación de nombres multidominio sean…	Introduzca el comando…
Activado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-trusted-domain-enum -search-enabled true`

Si desea que las búsquedas de asignación de nombres multidominio sean…	Introduzca el comando…
Deshabilitado	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled false`

3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Información relacionada

Opciones de servidor disponibles

Restablece y vuelve a detectar dominios SMB de ONTAP de confianza

Puede forzar la redetección de todos los dominios de confianza. Esto puede ser útil cuando los servidores de dominio de confianza no responden adecuadamente o las relaciones de confianza han cambiado. Solo se detectan los dominios con una confianza bidireccional con el dominio principal, que es el dominio que contiene la cuenta de equipo del servidor CIFS.

Paso

1. Restablezca y vuelva a detectar dominios de confianza mediante el `vserver cifs domain trusts rediscover` comando.

```
vserver cifs domain trusts rediscover -vserver vs1
```

Información relacionada

Muestra información sobre los dominios de confianza detectados

Mostrar información sobre los dominios SMB de ONTAP de confianza detectados

Puede mostrar información acerca de los dominios de confianza detectados para el dominio principal del servidor CIFS, que es el dominio que contiene la cuenta de equipo del servidor CIFS. Esto puede ser útil si desea saber qué dominios de confianza se descubren y cómo se ordenan dentro de la lista de dominios de confianza detectados.

Acerca de esta tarea

Sólo se descubren los dominios con confianzas bidireccionales con el dominio principal. Dado que el controlador de dominio (DC) del dominio principal devuelve la lista de dominios de confianza en un orden determinado por el DC, no se puede predecir el orden de los dominios de la lista. Al mostrar la lista de dominios de confianza, puede determinar el orden de búsqueda para las búsquedas de asignación de nombres multidominio.

La información que se muestra sobre el dominio de confianza se agrupa por nodos y máquina virtual de almacenamiento (SVM).

Paso

1. Muestra información sobre los dominios de confianza detectados mediante `vserver cifs domain trusts show` el comando.

```
vserver cifs domain trusts show -vserver vs1
```

```
   Node: node1
Vserver: vs1

Home Domain             Trusted Domain
---------------------   ----------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM

   Node: node2
Vserver: vs1

Home Domain             Trusted Domain
---------------------   ----------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM
```

Información relacionada

Restablecer y volver a detectar dominios de confianza

Agregue, elimine o reemplace los dominios SMB de confianza de ONTAP en las listas preferidas

Puede agregar o quitar dominios de confianza de la lista de dominios de confianza preferidos para el servidor SMB o puede modificar la lista actual. Si configura una lista de dominios de confianza preferidos, esta lista se utiliza en lugar de los dominios de confianza bidireccionales detectados al realizar búsquedas de asignación de nombres multidominio.

Acerca de esta tarea

- Si va a agregar dominios de confianza a una lista existente, la nueva lista se combina con la lista existente con las nuevas entradas colocadas al final Los dominios de confianza se buscan en el orden en que aparecen en la lista de dominios de confianza.
- Si va a quitar dominios de confianza de la lista existente y no especifica una lista, se elimina toda la lista de dominios de confianza de la máquina virtual de almacenamiento (SVM) especificada.
- Si modifica la lista existente de dominios de confianza, la nueva lista sobrescribe la lista existente.

> Debe introducir solo los dominios de confianza bidireccional en la lista de dominios de confianza preferidos. Aunque puede introducir dominios de confianza de salida o de entrada en la lista de dominios preferidos, no se utilizan al realizar búsquedas de asignación de nombres multidominio. ONTAP omite la entrada para el dominio unidireccional y pasa al siguiente dominio de confianza bidireccional de la lista.

Paso

1. Ejecute una de las siguientes acciones:

Si desea hacer lo siguiente con la lista de dominios de confianza preferidos…	Usar el comando…
Agregar dominios de confianza a la lista	`vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...`
Quitar dominios de confianza de la lista	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`
Modifique la lista existente	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

Ejemplos

El siguiente comando añade dos dominios de confianza (cifs1.example.com y cifs2.example.com) a la lista de dominios de confianza preferida utilizada por SVM vs1:

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

El siguiente comando quita dos dominios de confianza de la lista utilizada por SVM vs1:

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

El siguiente comando modifica la lista de dominios de confianza utilizada por SVM vs1. La nueva lista sustituye a la lista original:

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

Información relacionada

Muestra información sobre la lista de dominios de confianza preferidos

Mostrar información sobre la lista de dominios de confianza de SMB de ONTAP preferida

Puede mostrar información acerca de los dominios de confianza que se encuentran en la lista de dominios de confianza preferidos y el orden en que se realizan búsquedas si las búsquedas de asignación de nombres multidominio están habilitadas. Puede configurar una lista de dominios de confianza preferida como alternativa al uso de la lista de

dominios de confianza detectados automáticamente.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea mostrar información sobre lo siguiente…	Usar el comando…
Todos los dominios de confianza preferidos en el clúster agrupados por máquinas virtuales de almacenamiento (SVM)	`vserver cifs domain name-mapping-search show`
Todos los dominios de confianza preferidos para una SVM especificada	`vserver cifs domain name-mapping-search show -vserver vserver_name`

El siguiente comando muestra información sobre todos los dominios de confianza preferidos en el clúster:

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver         Trusted Domains
--------------  ----------------------------------
vs1             CIFS1.EXAMPLE.COM
```

Información relacionada

Agregar, eliminar o reemplazar dominios confiables en listas preferidas

Crear y configurar recursos compartidos de SMB

Obtenga más información sobre la creación y configuración de recursos compartidos de SMB de ONTAP

Antes de que los usuarios y las aplicaciones puedan acceder a los datos en el servidor CIFS mediante SMB, debe crear y configurar recursos compartidos de SMB, que es un punto de acceso con nombre en un volumen. Puede personalizar los recursos compartidos especificando parámetros de recurso compartido y propiedades de recurso compartido. Puede modificar un recurso compartido existente en cualquier momento.

Cuando se crea un recurso compartido de SMB, ONTAP crea una ACL predeterminada para el recurso compartido con permisos de control completo para todos.

Los recursos compartidos de SMB están ligados al servidor CIFS en la máquina virtual de almacenamiento (SVM). Los recursos compartidos de SMB se eliminan si la SVM se elimina o el servidor CIFS con el que está asociado se elimina de la SVM. Si vuelve a crear el servidor CIFS en la SVM, debe volver a crear los recursos compartidos SMB.

Información relacionada

- Obtenga información sobre los usuarios y grupos locales
- "Configuración de SMB para Microsoft Hyper-V y SQL Server"
- Configurar la asignación de caracteres para la traducción de nombres de archivos en volúmenes

Obtenga información sobre los recursos compartidos administrativos predeterminados de bloques de mensajes del servidor de ONTAP

Cuando se crea un servidor CIFS en la máquina virtual de almacenamiento (SVM), los recursos compartidos administrativos predeterminados se crean automáticamente. Debe comprender cuáles son esos recursos compartidos predeterminados y cómo se utilizan.

ONTAP crea los siguientes recursos compartidos administrativos predeterminados al crear el servidor CIFS:

> A partir de ONTAP 9.8, el recurso compartido admin$ ya no se crea de forma predeterminada.

- ipc$
- Admin$ (solo ONTAP 9.7 y versiones anteriores)
- r$

Puesto que los recursos compartidos que terminan con el carácter $ son recursos compartidos ocultos, los recursos compartidos administrativos predeterminados no son visibles desde Mi PC, pero puede verlos utilizando carpetas compartidas.

Cómo se utilizan los recursos compartidos predeterminados ipc$ y admin$

Los recursos compartidos ipc$ y admin$ los utilizan ONTAP y los administradores de Windows no pueden utilizarlos para acceder a los datos que residen en la SVM.

- ipc$ share

  el recurso compartido ipc$ es un recurso que comparte las canalizaciones con nombre que son esenciales para la comunicación entre programas. el recurso compartido ipc$ se utiliza durante la administración remota de un equipo y cuando se visualizan los recursos compartidos de un equipo. No puede cambiar la configuración de recursos compartidos, las propiedades de recursos compartidos ni las ACL del recurso compartido ipc$. Tampoco puede cambiar el nombre del recurso compartido ipc$ ni eliminarlo.

- Recurso compartido admin$ (solo ONTAP 9.7 y versiones anteriores)

  > A partir de ONTAP 9.8, el recurso compartido admin$ ya no se crea de forma predeterminada.

  El recurso compartido admin$ se usa durante la administración remota de la SVM. La ruta de este recurso siempre es la ruta al raíz de SVM. No se pueden cambiar las configuraciones de recursos compartidos, las propiedades de recursos compartidos ni las ACL del recurso compartido admin$. Tampoco puede cambiar el nombre del recurso compartido admin$ ni eliminarlo.

Cómo se utiliza el recurso compartido c$ predeterminado

El recurso compartido c$ es un recurso compartido administrativo que puede usar el administrador de clústeres o SVM para acceder al volumen raíz de SVM y administrarlo.

A continuación se muestran las características de la cuota c$:

- La ruta de este recurso compartido siempre es la ruta al volumen raíz de la SVM y no se puede modificar.
- La ACL predeterminada para el recurso compartido c$ es Administrator / Full Control.

Este usuario es BUILTIN\Administrator. De forma predeterminada, BUILTIN\Administrator puede asignar al recurso compartido y ver, crear, modificar o eliminar archivos y carpetas en el directorio raíz asignado. Se debe tener cuidado al administrar archivos y carpetas en este directorio.

- Es posible cambiar la ACL del recurso compartido de c$.
- Puede cambiar la configuración de c$ share y las propiedades share.
- No se puede eliminar el recurso compartido c$.
- El administrador de SVM puede acceder al resto del espacio de nombres de la SVM desde el recurso compartido c$ asignado cruzando las uniones del espacio de nombres.
- Se puede acceder al recurso compartido c$ mediante Microsoft Management Console.

Información relacionada

Configurar permisos de archivos avanzados mediante la pestaña Seguridad de Windows

Obtenga más información sobre ONTAP los requisitos de nomenclatura para recursos compartidos de bloque de mensajes del servidor

Tenga en cuenta los requisitos de nomenclatura de los recursos compartidos de ONTAP al crear recursos compartidos de SMB en el servidor de SMB.

Las convenciones de nomenclatura de los recursos compartidos para ONTAP son las mismas que para Windows e incluyen los siguientes requisitos:

- El nombre de cada recurso compartido debe ser exclusivo para el servidor SMB.
- Los nombres de recurso compartido no distinguen mayúsculas de minúsculas.
- La longitud máxima del nombre compartido es de 80 caracteres.
- Se admiten los nombres de los recursos compartidos Unicode.
- Los nombres de los recursos compartidos que terminan con el carácter $ son recursos compartidos ocultos.
- Para ONTAP 9.7 y anteriores, los recursos compartidos administrativos admin$, ipc$ y c$ se crean automáticamente en cada servidor CIFS y son nombres de recursos compartidos reservados. A partir de ONTAP 9.8, el recurso compartido admin$ ya no se crea automáticamente.
- No se puede usar el nombre del recurso compartido ONTAP_ADMIN$ al crear un recurso compartido.
- Se admiten los nombres de uso compartido que contienen espacios:
  - No puede utilizar un espacio como primer carácter ni como último carácter en un nombre de recurso compartido.
  - Los nombres de los recursos compartidos deben escribirse entre comillas.

    Las comillas simples se consideran parte del nombre del recurso compartido y no se pueden utilizar en lugar de comillas.

- Los siguientes caracteres especiales se admiten cuando se asigna el nombre a los recursos compartidos de SMB:

```
! @ # $ % & ' _ - . ~ ( ) { }
```

- Los siguientes caracteres especiales no se admiten cuando se asigna el nombre a los recursos compartidos de SMB:

```
** [ ] " / \ : ; | < > , ? * =
```

Obtenga más información sobre los requisitos de sensibilidad de casos del directorio SMB de ONTAP al crear recursos compartidos en un entorno multiprotocolo

Si crea recursos compartidos en una SVM donde se utiliza el esquema de nomenclatura 8.3 para distinguir entre nombres de directorio donde solo hay diferencias de mayúsculas y minúsculas entre los nombres, debe utilizar el nombre 8.3 en la ruta de acceso compartido para garantizar que el cliente se conecte a la ruta de directorio deseada.

En el siguiente ejemplo, se crearon dos directorios llamados "'testdir'" y "'TESTDIR'" en un cliente Linux. La ruta de unión del volumen que contiene los directorios es `/home`. La primera salida es de un cliente Linux y la segunda es de un cliente SMB.

```
 ls -l
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:24 TESTDIR
```

```
dir

 Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

Al crear un recurso compartido en el segundo directorio, debe utilizar el nombre 8.3 en la ruta de acceso al recurso compartido. En este ejemplo, la ruta de acceso de recurso compartido al primer directorio es `/home/testdir` y la ruta de acceso de recurso compartido al segundo directorio es `/home/TESTDI~1`.

Utilizar las propiedades de recursos compartidos de SMB

Obtenga más información sobre el uso de propiedades de recursos compartidos SMB de ONTAP

Puede personalizar las propiedades de los recursos compartidos SMB.

Las propiedades de recursos compartidos disponibles son las siguientes:

Comparta propiedades	Descripción
`oplocks`	Esta propiedad especifica que el recurso compartido utiliza bloqueos oportunistas, también conocidos como almacenamiento en caché en el cliente.

Comparta propiedades	Descripción
`browsable`	Esta propiedad permite a los clientes de Windows examinar el recurso compartido.
`showsnapshot`	Esta propiedad especifica que los clientes pueden ver y recorrer las instantáneas.
`changenotify`	Esta propiedad especifica que el recurso compartido admite peticiones de notificación de cambio. Para los recursos compartidos en una SVM, esta es una propiedad inicial predeterminada.
`attributecache`	Esta propiedad permite que el atributo de archivo que almacena en caché en el recurso compartido SMB proporcione un acceso más rápido a los atributos. El valor predeterminado es deshabilitar el almacenamiento en caché de atributos. Esta propiedad debe estar habilitada sólo si hay clientes que se conectan a recursos compartidos a través de SMB 1.0. Esta propiedad de recurso compartido no es aplicable si los clientes se conectan a recursos compartidos a través de SMB 2.x o SMB 3.0.
`continuously-available`	Esta propiedad permite a los clientes SMB que lo admiten abrir archivos de una forma persistente. Los archivos abiertos de esta manera están protegidos contra eventos disruptivos, como la conmutación por error y la devolución.
`branchcache`	Esta propiedad especifica que el recurso compartido permite a los clientes solicitar hash de BranchCache en los archivos dentro de este recurso compartido. Esta opción solo es útil si se especifica «'por recurso compartido» como modo operativo en la configuración de BranchCache CIFS.
`access-based-enumeration`	Esta propiedad especifica que *Access Based Enumeration* (ABE) está habilitado en este recurso compartido. Las carpetas compartidas filtradas POR ABE son visibles para un usuario en función de los derechos de acceso de ese usuario individual, lo que impide la visualización de carpetas u otros recursos compartidos a los que el usuario no tiene derechos de acceso.

Comparta propiedades	Descripción
`namespace-caching`	Esta propiedad especifica que los clientes SMB que se conectan a este recurso compartido pueden almacenar en caché los resultados de enumeración de directorios que devuelven los servidores CIFS, lo que puede proporcionar un mejor rendimiento. De forma predeterminada, los clientes de SMB 1 no almacenan en caché los resultados de la enumeración de directorios. Dado que los resultados de enumeración de directorios de caché de los clientes SMB 2 y SMB 3 son los mismos, al especificar esta propiedad de recurso compartido, se proporcionan ventajas de rendimiento solo para las conexiones de cliente SMB 1.
`encrypt-data`	Esta propiedad especifica que se debe utilizar el cifrado SMB al acceder a este recurso compartido. Los clientes de SMB que no admiten cifrado al acceder a los datos de SMB no podrán acceder a este recurso compartido.

Agregue o elimine propiedades de recurso compartido en recursos compartidos SMB de ONTAP existentes

Puede personalizar un recurso compartido SMB existente agregando o quitando propiedades de recurso compartido. Esto puede ser útil para cambiar la configuración de recursos compartidos con el fin de satisfacer los requisitos en constante cambio del entorno.

Antes de empezar

Debe existir el recurso compartido cuyas propiedades desea modificar.

Acerca de esta tarea

Directrices para añadir propiedades de recurso compartido:

- Puede agregar una o más propiedades de recursos compartidos mediante una lista delimitada por comas.
- Todas las propiedades de recurso compartido que haya especificado anteriormente permanecen vigentes.

  Las propiedades recién agregadas se agregan a la lista existente de propiedades de recursos compartidos.

- Si especifica un nuevo valor para las propiedades de recurso compartido que ya se han aplicado al recurso compartido, el valor recién especificado reemplazará al valor original.
- No puede quitar las propiedades de recurso compartido `vserver cifs share properties add` con el comando.

  Puede utilizar el `vserver cifs share properties remove` comando para eliminar propiedades de recurso compartido.

Directrices para eliminar propiedades de recurso compartido:

- Puede quitar una o varias propiedades de recursos compartidos mediante una lista delimitada por comas.
- Las propiedades de recurso compartido que ha especificado previamente pero no las quita permanecen vigentes.

Pasos

1. Introduzca el comando correspondiente:

Si desea…	Introduzca el comando…
Añada propiedades de recurso compartido	`vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`
Quite las propiedades de uso compartido	`vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`

2. Compruebe la configuración de la propiedad de recurso compartido: `vserver cifs share show -vserver vserver_name -share-name share_name`

Ejemplos

El siguiente comando agrega la `showsnapshot` propiedad de recurso compartido a un recurso compartido denominado “hare1” en SVM VS1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share1  /share1   oplocks      -          Everyone / Full
Control
                             browsable
                             changenotify
                             showsnapshot
```

El siguiente comando elimina la `browsable` propiedad de recurso compartido de un recurso compartido denominado «hare2» en SVM VS1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share2  /share2   oplocks      -          Everyone / Full
Control
                             changenotify
```

Información relacionada

Comandos para gestionar recursos compartidos

Optimice el acceso de usuario de SMB de ONTAP con la configuración de recursos compartidos de force-group

Cuando se crea un recurso compartido desde la línea de comandos de ONTAP a datos con seguridad efectiva de UNIX, se puede especificar que todos los archivos creados por los usuarios de SMB en ese recurso compartido pertenecen al mismo grupo, conocido como el *force-group*, que debe ser un grupo predefinido en la base de datos de grupos UNIX. El uso de un grupo de fuerza facilita el acceso de los usuarios SMB que pertenecen a varios grupos a los archivos.

Especificar un grupo de fuerza solo es significativo si el recurso compartido está en un qtree UNIX o mixto. No es necesario establecer un grupo forzado para los recursos compartidos de un volumen NTFS o un qtree ya que el acceso a los archivos de estos recursos compartidos está determinado por permisos de Windows, no por GID de UNIX.

Si se ha especificado un grupo de fuerza para un recurso compartido, lo siguiente se convierte en verdadero del recurso compartido:

- Los usuarios de SMB del grupo de fuerza que acceden a este recurso compartido se cambian temporalmente al GID del grupo de fuerza.

  Este GID permite acceder a los archivos de este recurso compartido a los que no se puede acceder normalmente con su GID o UID principal.

- Todos los archivos de este recurso compartido creados por usuarios SMB pertenecen al mismo grupo de fuerzas, independientemente del GID primario del propietario del archivo.

Cuando los usuarios de SMB intentan acceder a un archivo creado por NFS, los GID principales de los usuarios de SMB determinan los derechos de acceso.

El grupo de fuerza no afecta al modo en que los usuarios NFS acceden a los archivos de este recurso compartido. Un archivo creado por NFS adquiere el GID del propietario del archivo. La determinación de los permisos de acceso se basa en el UID y el GID primario del usuario NFS que intenta acceder al archivo.

El uso de un grupo de fuerza facilita el acceso de los usuarios SMB que pertenecen a varios grupos a los archivos. Por ejemplo, si desea crear un recurso compartido para almacenar las páginas web de la empresa y proporcionar acceso de escritura a los usuarios de los departamentos de Ingeniería y Marketing, puede crear un recurso compartido y proporcionar acceso de escritura a un grupo de fuerza denominado "'webgroup1'".

Debido al grupo de fuerza, todos los archivos creados por los usuarios de SMB en este recurso compartido son propiedad del grupo "'webgroup1'". Además, a los usuarios se les asigna automáticamente el GID del grupo "'webgroup1'" al acceder al recurso compartido. Como resultado, todos los usuarios pueden escribir en este recurso compartido sin necesidad de gestionar los derechos de acceso de los usuarios en los departamentos de ingeniería y marketing.

Información relacionada

Crear recursos compartidos con la configuración de recursos compartidos de grupo forzado

Cree recursos compartidos SMB de ONTAP con la configuración de recursos compartidos force-group

Puede crear un recurso compartido de SMB con la configuración de recurso compartido de grupo forzado si desea que los usuarios de SMB que acceden a datos de volúmenes o qtrees con seguridad de archivos UNIX consideren que ONTAP pertenece al mismo grupo UNIX.

Paso

1. Cree el recurso compartido de SMB: `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path path -force-group-for-create` *`UNIX_group_name`*

   Si la ruta UNC (`\\servername\sharename\filepath`) del recurso compartido contiene más de 256 caracteres (excluyendo el valor inicial`\\` en la ruta UNC), la pestaña **Seguridad** del cuadro Propiedades de Windows no estará disponible. Se trata de un problema del cliente Windows y no de un problema de ONTAP. Para evitar este problema, no cree recursos compartidos con rutas UNC con más de 256 caracteres.

   Si desea quitar el grupo de fuerza después de crear el recurso compartido, puede modificar el recurso compartido en cualquier momento y especificar una cadena vacía como valor para `-force-group-for-create` el parámetro. Si quita el grupo de fuerza modificando el recurso compartido, todas las conexiones existentes a este recurso compartido siguen teniendo el grupo de fuerza establecido anteriormente como GID primario.

Ejemplo

El siguiente comando crea un recurso compartido 'webpages' que es accesible en la web `/corp/companyinfo` en el directorio en el que todos los archivos que los usuarios de SMB crean están asignados al grupo webgroup1:

```
vserver cifs share create -vserver vs1 -share-name webpages -path
/corp/companyinfo -force-group-for-create webgroup1
```

Información relacionada

Optimice el acceso de los usuarios con la configuración de uso compartido de grupo forzado

Ver información sobre recursos compartidos SMB de ONTAP mediante MMC

Puede ver información sobre los recursos compartidos de SMB en la SVM y realizar algunas tareas de gestión con Microsoft Management Console (MMC). Antes de ver los recursos compartidos, tiene que conectar MMC a la SVM.

Acerca de esta tarea

Puede realizar las siguientes tareas en recursos compartidos contenidos en las SVM mediante MMC:

- Ver recursos compartidos
- Ver sesiones activas
- Ver archivos abiertos
- Enumera la lista de sesiones, archivos y conexiones de árbol del sistema
- Cierre los archivos abiertos en el sistema
- Cierre las sesiones abiertas
- Cree/gestione recursos compartidos

> Las vistas que muestran las capacidades anteriores son específicas de los nodos y no del clúster. Por lo tanto, cuando utiliza MMC para conectarse al nombre de host del servidor SMB (es decir, cifs01.domain.local), se le enrutará, en función de cómo haya configurado DNS, a una única LIF dentro del clúster.

MMC para ONTAP no admite las siguientes funciones:

- Creación de nuevos usuarios/grupos locales
- Gestión/visualización de usuarios/grupos locales existentes
- Ver eventos o registros de rendimiento
- Reducida
- Servicios y aplicaciones

En las instancias en las que la operación no es compatible, es posible que se produzcan `remote procedure call failed` errores.

"Preguntas más frecuentes: Uso de MMC de Windows con ONTAP"

Pasos

1. Para abrir la MMC de Administración de equipos en cualquier servidor de Windows, en **Panel de control**, seleccione **Herramientas administrativas** > **Administración de equipos**.
2. Seleccione **Acción** > **conectar a otro ordenador**.

   Aparece el cuadro de diálogo Seleccionar equipo.
3. Escriba el nombre del sistema de almacenamiento o haga clic en **examinar** para buscar el sistema de almacenamiento.
4. Haga clic en **OK**.

   MMC se conecta a SVM.
5. En el panel de navegación, haga clic en **carpetas compartidas** > **recursos compartidos**.

   Se muestra una lista de recursos compartidos de la SVM en el panel de visualización derecho.
6. Para mostrar las propiedades de uso compartido de un recurso compartido, haga doble clic en él para abrir el cuadro de diálogo **Propiedades**.
7. Si no puede conectarse al sistema de almacenamiento mediante MMC, puede agregar al usuario al grupo BUILTIN\Administrators o BUILTIN\Power Users mediante uno de los siguientes comandos del sistema de almacenamiento:

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

Comandos de ONTAP para gestionar recursos compartidos de SMB

Se deben usar `vserver cifs share` `vserver cifs share properties` los comandos y para gestionar recursos compartidos de SMB.

Si desea…	Se usa este comando…
Cree un recurso compartido de SMB	`vserver cifs share create`
Mostrar los recursos compartidos de SMB	`vserver cifs share show`
Modificar un recurso compartido de SMB	`vserver cifs share modify`
Eliminar un recurso compartido de SMB	`vserver cifs share delete`
Agregar propiedades de recurso compartido a un recurso compartido existente	`vserver cifs share properties add`
Quitar propiedades de recurso compartido de un recurso compartido existente	`vserver cifs share properties remove`
Muestra información sobre las propiedades de uso compartido	`vserver cifs share properties show`

Obtenga más información sobre `vserver cifs` en el "Referencia de comandos del ONTAP".

Acceso seguro a archivos mediante ACL de uso compartido de SMB

Obtenga más información sobre la gestión de ACL de nivel de recurso compartido de bloque de mensajes del servidor de ONTAP

Puede cambiar las ACL de nivel compartido para otorgar a los usuarios más o menos derechos de acceso al recurso compartido. Puede configurar ACL de nivel compartido usando usuarios y grupos de Windows o usuarios y grupos de UNIX.

De forma predeterminada, la ACL de nivel de recurso compartido proporciona un control total al grupo estándar denominado Everyone. El control total en la ACL significa que todos los usuarios en el dominio y todos los dominios de confianza tienen acceso completo al recurso compartido. Puede controlar el nivel de acceso a una ACL de nivel de recurso compartido mediante Microsoft Management Console (MMC) en un cliente Windows o la línea de comandos de ONTAP. "Crear listas de control de acceso a recursos

compartidos".

Las siguientes directrices se aplican cuando se utiliza MMC:

- Los nombres de usuario y de grupo especificados deben ser nombres de Windows.
- Sólo puede especificar permisos de Windows.

Cuando se utiliza la línea de comandos de ONTAP, se aplican las siguientes directrices:

- Los nombres de usuario y de grupo especificados pueden ser nombres de Windows o nombres UNIX.

  Si no se especifica un tipo de usuario y grupo al crear o modificar ACL, el tipo predeterminado es usuarios y grupos de Windows.

- Sólo puede especificar permisos de Windows.

Cree listas de control de acceso compartido de SMB de ONTAP

La configuración de permisos de uso compartido mediante la creación de listas de control de acceso (ACL) para recursos compartidos de SMB permite controlar el nivel de acceso a un recurso compartido para usuarios y grupos.

Acerca de esta tarea

Puede configurar ACL de nivel compartido utilizando nombres de usuarios o grupos locales o de dominio de Windows o nombres de usuarios o grupos de UNIX.

Antes de crear una nueva ACL, debe suprimir la ACL de recurso compartido por defecto `Everyone / Full Control` , que representa un riesgo de seguridad.

En modo de grupo de trabajo, el nombre de dominio local es el nombre del servidor SMB.

Pasos

1. Elimine la ACL predeterminada para compartir:`Vserver cifs share access-control delete -vserver <vserver_name> -share <share_name> -user-or-group everyone`
2. Configure la nueva ACL:

Si desea configurar las ACL utilizando…	Introduzca el comando…
Usuario de Windows	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\user_name> -permission <access_right>`
Grupo Windows	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\group_name> -permission <access_right>`

Si desea configurar las ACL utilizando…	Introduzca el comando…
Usuario UNIX	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-user> -user-or-group <UNIX_user_name> -permission <access_right>`
Grupo UNIX	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-group> -user-or-group <UNIX_group_name> -permission <access_right>`

3. Verifique que la ACL aplicada al recurso compartido es correcta mediante `vserver cifs share access-control show` el comando.

Ejemplo

El siguiente comando otorga `Change` permisos al grupo de Windows “Equipo de ventas” para el recurso compartido “ventas” en la SVM “vs1.example.com”:

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
Permission
--------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\Sales Team     windows     Change
```

El siguiente comando `Read` otorga permiso al grupo UNIX «engineering» para el recurso compartido «eng» en la SVM «vs2.example.com»:

```
cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                Share       User/Group               User/Group  Access
Vserver         Name        Name                     Type
Permission
--------------- ----------- -------------------      -----------
-----------
vs2.example.com  c$         BUILTIN\Administrators   windows
Full_Control
vs2.example.com  eng        engineering              unix-group  Read
```

Los siguientes comandos dan `Change` permiso al grupo local de Windows denominado «Tiger Team» y `Full_Control` permiso al usuario local de Windows denominado «Sue Chang» para el recurso compartido «datavol5» en la SVM «VS1»:

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    Tiger Team         windows     Change
vs1            datavol5    Sue Chang          windows     Full_Control
```

Comandos ONTAP para administrar listas de control de acceso a recursos compartidos SMB

Debe conocer los comandos para gestionar las listas de control de acceso (ACL) de SMB, lo que incluye crear, mostrar, modificar y eliminar dichas listas.

Si desea…	Se usa este comando…
Cree una nueva ACL	`vserver cifs share access-control create`
Mostrar ACL	`vserver cifs share access-control show`
Modificar una ACL	`vserver cifs share access-control modify`
Eliminar una ACL	`vserver cifs share access-control delete`

Acceso seguro a archivos mediante permisos de archivo

Configurar permisos avanzados de archivos NTFS mediante la pestaña Seguridad de Windows para SVM SMB de ONTAP

Puede configurar permisos de archivo NTFS estándar en archivos y carpetas mediante la ficha **Seguridad de Windows** de la ventana Propiedades de Windows.

Antes de empezar

El administrador que realiza esta tarea debe tener suficientes permisos NTFS para cambiar los permisos en los objetos seleccionados.

Acerca de esta tarea

La configuración de los permisos de archivo NTFS se realiza en un host de Windows agregando entradas a las listas de control de acceso discrecional NTFS (DACL) asociadas con un descriptor de seguridad NTFS. El descriptor de seguridad se aplica entonces a los archivos y directorios NTFS. La interfaz gráfica de usuario de Windows se encarga automáticamente de estas tareas.

Pasos

1. En el menú **Herramientas** del Explorador de Windows, seleccione **asignar unidad de red**.
2. Complete el cuadro de diálogo **asignar unidad de red**:

   a. Seleccione una letra **Unidad**.

   b. En el cuadro **Folder**, escriba el nombre del servidor CIFS que contiene el recurso compartido que contiene los datos a los que desea aplicar los permisos y el nombre del recurso compartido.

      Si el nombre de su servidor CIFS es "CIFS_SERVER' y su recurso compartido se llama "hare1", debe escribir `\\CIFS_SERVER\share1`.

      Puede especificar la dirección IP de la interfaz de datos para el servidor CIFS en lugar del nombre del servidor CIFS.

   c. Haga clic en **Finalizar**.

   La unidad seleccionada está montada y lista con la ventana del Explorador de Windows que muestra archivos y carpetas contenidos en el recurso compartido.

3. Seleccione el archivo o directorio para el que desea establecer los permisos de archivo NTFS.
4. Haga clic con el botón secundario del ratón en el archivo o directorio y seleccione **Propiedades**.
5. Seleccione la ficha **Seguridad**.

   La ficha **Seguridad** muestra la lista de usuarios y grupos para los que se ha establecido el permiso NTFS. El cuadro **permisos para** muestra una lista de permisos permitir y denegar que están en vigor para cada usuario o grupo seleccionado.

6. Haga clic en **Avanzado**.

   La ventana Propiedades de Windows muestra información sobre los permisos de archivo existentes asignados a usuarios y grupos.

7. Haga clic en **Cambiar permisos**.

   Se abrirá la ventana permisos.

8. Realice las acciones deseadas:

Si desea…	Haga lo siguiente…
Configure permisos NTFS avanzados para un nuevo usuario o grupo	a. Haga clic en **Agregar**. b. En el cuadro **Escriba el nombre del objeto que desea seleccionar** , escriba el nombre del usuario o grupo que desea agregar. c. Haga clic en **OK**.
Cambiar los permisos NTFS avanzados de un usuario o grupo	a. En el cuadro **permisos de entrada:** , seleccione el usuario o grupo cuyos permisos avanzados desea cambiar. b. Haga clic en **Editar**.
Quitar permisos NTFS avanzados para un usuario o grupo	a. En el cuadro **Entradas de permisos:** , seleccione el usuario o grupo que desea quitar. b. Haga clic en **Quitar**. c. Vaya al paso 13.

   Si va a agregar permisos NTFS avanzados en un nuevo usuario o grupo o si va a cambiar los permisos avanzados de NTFS en un usuario o grupo existente, se abrirá el cuadro Entrada de permisos para <Object> .

9. En el cuadro **aplicar a**, seleccione cómo desea aplicar esta entrada de permiso de archivo NTFS.

   Si está configurando permisos de archivo NTFS en un solo archivo, el cuadro **aplicar a** no está activo. El valor **aplicar a** se establece de forma predeterminada en **este objeto sólo**.

10. En el cuadro **permisos** , seleccione los cuadros **permitir** o **Denegar** para los permisos avanzados que desea establecer en este objeto.

    ◦ Para permitir el acceso especificado, seleccione el cuadro **permitir**.

- Para no permitir el acceso especificado, seleccione el cuadro **Denegar**. Puede establecer permisos en los siguientes derechos avanzados:
- **Control total**

  Si elige este derecho avanzado, todos los demás derechos avanzados se seleccionan automáticamente (permitir o denegar derechos).

- **Carpeta Traverse / archivo de ejecución**
- **Lista de carpetas / lectura de datos**
- **Leer atributos**
- **Leer atributos extendidos**
- **Crear archivos / escribir datos**
- **Crear carpetas / anexar datos**
- **Escribir atributos**
- **Escriba atributos extendidos**
- **Eliminar subcarpetas y archivos**
- **Eliminar**
- **Leer permisos**
- **Cambiar permisos**
- **Tome la propiedad**

Si alguno de los cuadros de permisos avanzados no se puede seleccionar, se debe a que los permisos se heredan del objeto primario.

11. Si desea que las subcarpetas y los archivos de este objeto hereden estos permisos, seleccione la casilla **aplicar estos permisos a objetos y/o contenedores dentro de este contenedor únicamente**.
12. Haga clic en **OK**.
13. Después de terminar de agregar, quitar o editar permisos NTFS, especifique la configuración de herencia para este objeto:

    - Seleccione el cuadro **incluir permisos heredables del primario de este objeto**.

      Este es el valor predeterminado.

    - Seleccione el cuadro **Reemplazar todos los permisos de objeto secundario con permisos heredables de este objeto** .

      Esta configuración no está presente en el cuadro permisos si está estableciendo permisos de archivo NTFS en un solo archivo.

Tenga cuidado al seleccionar este ajuste. Esta configuración quita todos los permisos existentes en todos los objetos secundarios y los reemplaza con la configuración de permisos de este objeto. Podría quitar sin darse cuenta los permisos que no desea quitar. Especialmente importante cuando se configuran permisos en un volumen o un qtree de estilo de seguridad mixto. Si los objetos secundarios tienen un estilo de seguridad efectivo de UNIX, al propagar los permisos NTFS a esos objetos secundarios, ONTAP cambia estos objetos del estilo de seguridad de UNIX al estilo de seguridad NTFS y todos los permisos de UNIX de esos objetos secundarios se sustituyen por permisos NTFS.

- Seleccione ambas casillas.
- Seleccione ninguna casilla.

14. Haga clic en **Aceptar** para cerrar el cuadro **permisos**.
15. Haga clic en **Aceptar** para cerrar el cuadro **Configuración avanzada de seguridad para <Object>**.

Para obtener más información acerca de cómo establecer permisos NTFS avanzados, consulte la documentación de Windows.

Información relacionada

- Crear descriptores de seguridad NTFS en servidores
- Muestra información sobre la seguridad de archivos en volúmenes de estilo de seguridad NTFS
- Muestra información sobre la seguridad de archivos en volúmenes mixtos de estilo de seguridad
- Muestra información sobre la seguridad de archivos en volúmenes de estilo de seguridad UNIX

Comandos ONTAP para permisos de archivos SMB NTFS

Puede configurar los permisos de archivo NTFS en archivos y directorios mediante la interfaz de línea de comandos de ONTAP. Esto le permite configurar permisos de archivo NTFS sin necesidad de conectarse a los datos mediante un recurso compartido SMB en un cliente Windows.

Puede configurar los permisos de archivo NTFS agregando entradas a las listas de control de acceso discrecional (DACL) de NTFS que están asociadas con un descriptor de seguridad de NTFS. El descriptor de seguridad se aplica entonces a los archivos y directorios NTFS.

Sólo puede configurar permisos de archivo NTFS mediante la línea de comandos. No puede configurar las ACL de NFSv4 mediante la CLI.

Pasos

1. Cree un descriptor de seguridad NTFS.

```
vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
ntfs_security_descriptor_name -owner owner_name -group primary_group_name
-control-flags-raw raw_control_flags
```

2. Agregue DACL al descriptor de seguridad NTFS.

```
vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
-rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
```

```
{this-folder|sub-folders|files}
```

3. Cree una directiva de seguridad de archivos/directorios.

```
vserver security file-directory policy create -vserver svm_name -policy-name
policy_name
```

Obtenga información sobre los permisos de archivos UNIX que brindan control de acceso al acceder a archivos a través de servidores SMB de ONTAP

Un volumen FlexVol puede tener uno de los tres tipos de estilo de seguridad: NTFS, UNIX o mixto. Es posible acceder a los datos a través de SMB independientemente del estilo de seguridad; no obstante, se necesitan permisos adecuados de archivos UNIX para acceder a los datos con una seguridad efectiva de UNIX.

Cuando se accede a los datos a través de SMB, existen varios controles de acceso que se utilizan para determinar si un usuario está autorizado a realizar una acción solicitada:

- Permisos de exportación

  La configuración de los permisos de exportación para el acceso SMB es opcional.

- Comparta los permisos
- Permisos de archivo

  Los siguientes tipos de permisos de archivo se pueden aplicar a los datos en los que el usuario desea realizar una acción:

  - NTFS
  - ACL de UNIX NFSv4
  - Bits de modo UNIX

En el caso de los datos con ACL de NFSv4 o conjuntos de bits de modo UNIX, se utilizan permisos de estilo UNIX para determinar los derechos de acceso a los archivos de los datos. El administrador de SVM debe establecer el permiso de archivo adecuado para garantizar que los usuarios tienen derechos para realizar la acción deseada.

> Los datos de un volumen de estilo de seguridad mixto pueden tener un estilo de seguridad efectivo NTFS o UNIX. Si los datos tienen un estilo de seguridad efectivo de UNIX, se utilizan los permisos de NFSv4 o bits de modo UNIX al determinar los derechos de acceso a los datos.

Acceso seguro a archivos mediante control de acceso dinámico (DAC)

Obtenga información sobre la seguridad del acceso a archivos DAC para servidores SMB de ONTAP

Puede proteger el acceso mediante el control de acceso dinámico y mediante la creación de directivas de acceso central en Active Directory y su aplicación a archivos y carpetas en las SVM mediante objetos de directiva de grupo aplicados (GPO). Puede configurar la auditoría para utilizar los eventos de configuración de directivas de acceso central para ver los efectos de los cambios en las directivas de acceso central antes de aplicarlas.

Adiciones a las credenciales CIFS

Antes del control dinámico de acceso, una credencial CIFS incluía la identidad de los principales de seguridad (el usuario) y la pertenencia al grupo Windows. Con el control dinámico de acceso, se agregan tres tipos más de información a la credencial: Identidad del dispositivo, reclamos del dispositivo y reclamos del usuario:

- Identidad del dispositivo

  El análogo de la información de identidad del usuario, excepto que es la identidad y pertenencia de grupo del dispositivo desde el que el usuario inicia sesión.

- Reclamaciones de dispositivos

  Afirmaciones acerca de una entidad de seguridad del dispositivo. Por ejemplo, una reclamación de dispositivo podría ser que es miembro de una unidad organizativa específica.

- Reclamaciones del usuario

  Afirmaciones acerca de una entidad de seguridad de usuario. Por ejemplo, una reclamación de usuario podría ser que su cuenta AD es miembro de una unidad organizativa específica.

Políticas de acceso central

Las políticas de acceso central para archivos permiten a las organizaciones implementar y administrar de forma centralizada políticas de autorización que incluyen expresiones condicionales mediante grupos de usuarios, reclamaciones de usuarios, reclamaciones de dispositivos y propiedades de recursos.

Por ejemplo, para acceder a datos de alto impacto empresarial, un usuario necesita ser un empleado a tiempo completo y solo tener acceso a los datos desde un dispositivo gestionado. Las directivas de acceso central se definen en Active Directory y se distribuyen a servidores de archivos mediante el mecanismo GPO.

Configuración de directivas de acceso central con auditoría avanzada

Las políticas centrales de acceso pueden ser «más favorables», en cuyo caso se evalúan de forma «qué sucede si» durante los controles de acceso a los archivos. Los resultados de lo que habría ocurrido si la directiva estaba en vigor y cómo difiere de lo que está configurado actualmente se registran como un evento de auditoría. De esta forma, los administradores pueden utilizar registros de eventos de auditoría para estudiar el impacto de un cambio de directiva de acceso antes de poner la directiva en juego. Tras evaluar el impacto de un cambio de política de acceso, la política se puede implementar a través de GPO en las SVM deseadas.

Información relacionada

- Obtenga más información sobre los GPO compatibles
- Obtenga información sobre cómo aplicar objetos de directiva de grupo a servidores SMB
- Habilitar o deshabilitar la compatibilidad con GPO en los servidores
- Mostrar información acerca de las configuraciones de GPO
- Muestra información sobre las políticas de acceso central
- Muestra información acerca de las reglas de la política de acceso central
- Configurar políticas de acceso central para proteger los datos en los servidores
- Mostrar información sobre la seguridad de los servidores
- "Seguimiento de seguridad y auditoría de SMB y NFS"

Si desea utilizar el control de acceso dinámico (DAC) en un servidor CIFS, debe comprender cómo ONTAP admite la funcionalidad de control de acceso dinámico en entornos Active Directory.

Compatible con el control de acceso dinámico

ONTAP admite la siguiente funcionalidad cuando está habilitado el control de acceso dinámico en el servidor CIFS:

Funcionalidad	Comentarios
Reclamaciones en el sistema de archivos	Las reclamaciones son pares simples de nombre y valor que indican cierta verdad acerca de un usuario. Las credenciales de usuario contienen información de reclamación y los descriptores de seguridad de los archivos pueden realizar comprobaciones de acceso que incluyen comprobaciones de reclamaciones. De este modo, los administradores disponen de un mayor nivel de control sobre quién puede acceder a los archivos.
Expresiones condicionales para comprobaciones de acceso a archivos	Al modificar los parámetros de seguridad de un archivo, los usuarios pueden agregar expresiones condicionales arbitrariamente complejas al descriptor de seguridad del archivo. La expresión condicional puede incluir comprobaciones para las reclamaciones.
Control centralizado de acceso a ficheros mediante directivas de acceso central	Las directivas de acceso central son un tipo de ACL almacenadas en Active Directory que se pueden etiquetar a un archivo. El acceso al archivo sólo se concede si el acceso comprueba tanto el descriptor de seguridad del disco como la directiva de acceso central etiquetada permiten el acceso.esto proporciona a los administradores la capacidad de controlar el acceso a los archivos desde una ubicación central (AD) sin tener que modificar el descriptor de seguridad del disco.
Configuración de políticas de acceso central	Agrega la capacidad de probar los cambios de seguridad sin afectar el acceso real a los archivos, mediante un «envejecimiento» de las políticas de acceso centrales y viendo el efecto del cambio en un informe de auditoría.
Soporte para mostrar información sobre la seguridad de las políticas de acceso central mediante la interfaz de línea de comandos de ONTAP	Amplía el `vserver security file-directory show` comando para mostrar información sobre las políticas de acceso central aplicadas.

Funcionalidad	Comentarios
Seguimiento de la seguridad que incluye políticas de acceso central	Amplía `vserver security trace` la familia de comandos para mostrar los resultados que incluyen información sobre las políticas de acceso central aplicadas.

No compatible con el control de acceso dinámico

ONTAP no admite la siguiente funcionalidad cuando el control de acceso dinámico está habilitado en el servidor CIFS:

Funcionalidad	Comentarios
Clasificación automática de objetos del sistema de archivos NTFS	Esta es una extensión de la infraestructura de clasificación de archivos de Windows que no se admite en ONTAP.
Auditoría avanzada que no sea la configuración de políticas de acceso central	Sólo se admite la configuración de directivas de acceso central para la auditoría avanzada.

Aprenda a usar DAC y políticas de acceso central con servidores SMB de ONTAP

Hay ciertas consideraciones que debe tener en cuenta al utilizar el control de acceso dinámico (DAC) y las políticas de acceso central para proteger los archivos y las carpetas en los servidores CIFS.

Se puede denegar el acceso NFS a la raíz si la regla de directiva se aplica al usuario de dominio\administrador

En determinadas circunstancias, puede denegarse el acceso NFS a root cuando se aplica la seguridad de la política de acceso central a los datos a los que el usuario raíz intenta acceder. El problema se produce cuando la directiva de acceso central contiene una regla que se aplica al dominio\administrador y la cuenta raíz se asigna a la cuenta de dominio\administrador.

En lugar de aplicar una regla al usuario de dominio\administrador, debe aplicar la regla a un grupo con privilegios administrativos, como el dominio\grupo de administradores. De esta forma, puede asignar root a la cuenta de dominio\administrador sin que este problema afecte a root.

El grupo BUILTIN\Administrators del servidor CIFS tiene acceso a los recursos cuando la directiva de acceso central aplicada no se encuentra en Active Directory

Es posible que los recursos contenidos en el servidor CIFS tengan políticas de acceso central aplicadas a ellos, pero cuando el servidor CIFS usa el SID de la política de acceso central para intentar recuperar información de Active Directory, el SID no coincide con ningún SID de política de acceso central existente en Active Directory. En estas circunstancias, el servidor CIFS aplica la política de recuperación predeterminada local para ese recurso.

La directiva de recuperación predeterminada local permite el acceso de grupo BUILTIN\Administrators del servidor CIFS a ese recurso.

Habilitar o deshabilitar DAC para servidores SMB de ONTAP

La opción que permite utilizar el control de acceso dinámico (DAC) para proteger objetos en el servidor CIFS está deshabilitada de forma predeterminada. Debe habilitar la opción si desea utilizar el control de acceso dinámico en el servidor CIFS. Si más adelante decide que no desea utilizar el control de acceso dinámico para proteger los objetos almacenados en el servidor CIFS, puede deshabilitar la opción.

Puede encontrar información acerca de cómo configurar el control de acceso dinámico en Active Directory en la biblioteca de Microsoft TechNet.

"Microsoft TechNet: Información general sobre el escenario de control de acceso dinámico"

Acerca de esta tarea

Una vez que el control de acceso dinámico está activado, el sistema de archivos puede contener ACL con entradas relacionadas con el control de acceso dinámico. Si el control de acceso dinámico está desactivado, se ignorarán las entradas actuales del control de acceso dinámico y no se permitirán las nuevas.

Esta opción solo está disponible en el nivel de privilegios avanzado.

Paso

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

Si desea que el control de acceso dinámico sea…	Introduzca el comando…
Activado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled true`
Deshabilitado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled false`

3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Información relacionada

Configurar políticas de acceso central para proteger los datos en los servidores

Administrar ACL que contienen ACE de DAC cuando DAC está deshabilitado en servidores SMB de ONTAP

Si tiene recursos que tienen ACL aplicados a ACE de control de acceso dinámico y deshabilita el control de acceso dinámico en la máquina virtual de almacenamiento (SVM), debe quitar las ACE de control de acceso dinámico antes de poder gestionar las ACE que no son de control de acceso dinámico en ese recurso.

Acerca de esta tarea

Una vez que el control dinámico de acceso está desactivado, no puede quitar los ACE de control de acceso no dinámico existentes ni agregar nuevos ACE de control de acceso no dinámico hasta que haya eliminado los ACE de control dinámico de acceso existentes.

Puede utilizar cualquier herramienta que utilice normalmente para administrar ACL para realizar estos pasos.

Pasos

1. Determine qué ACE de control dinámico de acceso se aplican al recurso.
2. Quite los ACE de control de acceso dinámico del recurso.
3. Agregue o quite ACE de control de acceso no dinámico según lo desee del recurso.

Configurar políticas de acceso central para proteger los datos en los servidores SMB de ONTAP

Hay varios pasos que debe dar para garantizar el acceso seguro a los datos en el servidor CIFS mediante políticas de acceso centrales, incluida la habilitación del control de acceso dinámico (DAC) en el servidor CIFS, la configuración de políticas de acceso centrales en Active Directory y la aplicación de las políticas de acceso centrales a los contenedores de Active Directory con GPO, Y habilitar los GPO en el servidor CIFS.

Antes de empezar

- Active Directory debe estar configurado para utilizar las directivas de acceso central.
- Debe tener suficiente acceso en los controladores de dominio de Active Directory para crear políticas de acceso centrales y crear y aplicar GPO a los contenedores que contienen los servidores CIFS.
- Debe tener suficiente acceso administrativo en la máquina virtual de almacenamiento (SVM) para ejecutar los comandos necesarios.

Acerca de esta tarea

Las directivas de acceso central se definen y aplican a los objetos de directiva de grupo (GPO) en Active Directory. Puede encontrar información acerca de cómo configurar las políticas de acceso central en Active Directory en la biblioteca de Microsoft TechNet.

"Microsoft TechNet: Escenario de política de acceso central"

Pasos

1. Habilite el control de acceso dinámico en la SVM si todavía no se habilita mediante `vserver cifs options modify` el comando.

   ```
   vserver cifs options modify -vserver vs1 -is-dac-enabled true
   ```

2. Habilite los objetos de política de grupo (GPO) en el servidor CIFS si aún no se han habilitado mediante `vserver cifs group-policy modify` el comando.

   ```
   vserver cifs group-policy modify -vserver vs1 -status enabled
   ```

3. Crear reglas de acceso central y políticas de acceso central en Active Directory.
4. Cree un objeto de directiva de grupo (GPO) para implementar las directivas de acceso central en Active Directory.
5. Aplique el GPO al contenedor donde se encuentra la cuenta de equipo servidor CIFS.
6. Actualice manualmente los objetos de normativa de grupo aplicados al servidor CIFS mediante `vserver cifs group-policy update` el comando.

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. Compruebe que la política de acceso central de GPO se aplica a los recursos del servidor CIFS mediante `vserver cifs group-policy show-applied` el comando.

El siguiente ejemplo muestra que la política de dominio predeterminada tiene dos políticas de acceso centrales que se aplican al servidor CIFS:

```
vserver cifs group-policy show-applied
```

```
Vserver: vs1
-----------------------------
    GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
```

```
      Policies: cap1
                cap2

    GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
2 entries were displayed.
```

Información relacionada

- Obtenga información sobre cómo aplicar objetos de directiva de grupo a servidores SMB
- Mostrar información acerca de las configuraciones de GPO
- Muestra información sobre las políticas de acceso central
- Muestra información acerca de las reglas de la política de acceso central
- Habilitar o deshabilitar DAC para servidores

Mostrar información sobre la seguridad de DAC para servidores SMB de ONTAP

Puede mostrar información acerca de la seguridad DAC (Dynamic Access Control) en volúmenes NTFS y en datos con seguridad efectiva NTFS en volúmenes mixtos de estilo de seguridad. Esto incluye información sobre ACE condicionales, ACE de recursos y ACE de políticas de acceso central. Puede utilizar los resultados para validar la configuración de seguridad o solucionar problemas de acceso a archivos.

Acerca de esta tarea

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los datos cuya información de seguridad de archivo o carpeta desee mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

Paso

1. Mostrar la configuración de seguridad de archivos y directorios con el nivel de detalle deseado:

Si desea mostrar información…	Introduzca el siguiente comando…
En forma de resumen	`vserver security file-directory show -vserver vserver_name -path path`
Con detalle ampliado	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
Donde se muestra la salida con los SID de grupo y usuario	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
Acerca de la seguridad de archivos y directorios para archivos y directorios en los que la máscara de bits hexadecimal se traduce al formato de texto	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

Ejemplos

En el siguiente ejemplo, se muestra información de seguridad de Control de acceso dinámico sobre la ruta de `/vol1` SVM VS1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                           Vserver: vs1
                         File Path: /vol1
                File Inode Number: 112
                   Security Style: mixed
                  Effective Style: ntfs
                   DOS Attributes: 10
           DOS Attributes in Text: ----D---
           Expanded Dos Attribute: -
                     Unix User Id: 0
                    Unix Group Id: 1
                   Unix Mode Bits: 777
           Unix Mode Bits in Text: rwxrwxrwx
                             ACLs: NTFS Security Descriptor
                                   Control:0xbf14
                                   Owner:CIFS1\Administrator
                                   Group:CIFS1\Domain Admins
                                   SACL - ACEs
                                      ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                      RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                      POLICY ID-All resources - No Write-
0x0-OI|CI
                                   DACL - ACEs
                                      ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                      ALLOW-Everyone-0x1f01ff-OI|CI
                                      ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

Información relacionada

- Mostrar información acerca de las configuraciones de GPO
- Muestra información sobre las políticas de acceso central
- Muestra información acerca de las reglas de la política de acceso central

Consideraciones de reversión para DAC en servidores SMB de ONTAP

Debe ser consciente de lo que sucede al volver a una versión de ONTAP que no admite el control de acceso dinámico (DAC) y lo que debe hacer antes y después de revertir.

Si desea revertir el clúster a una versión de ONTAP que no admite el control de acceso dinámico y que el

control de acceso dinámico está habilitado en una o varias máquinas virtuales de almacenamiento (SVM), debe hacer lo siguiente antes de revertir:

- Debe deshabilitar el control de acceso dinámico en todas las SVM que tengan habilitado en el clúster.
- Debe modificar cualquier configuración de auditoría del clúster que contenga el `cap-staging` tipo de evento para utilizar solo el `file-op` tipo de evento.

Debe comprender y actuar sobre algunas consideraciones importantes de reversión para archivos y carpetas con los ACE de control de acceso dinámico:

- Si se revierte el clúster, los ACE existentes de Dynamic Access Control no se eliminan; sin embargo, se ignorarán en las comprobaciones de acceso a archivos.
- Dado que los ACE de control de acceso dinámico se ignoran después de la nueva versión, el acceso a los archivos cambiará en archivos con ACE de control de acceso dinámico.

  Esto podría permitir a los usuarios acceder a los archivos que no podían obtener anteriormente o no tener acceso a los que podían acceder anteriormente.

- Debería aplicar ACE de control de acceso no dinámico a los archivos afectados para restaurar su nivel anterior de seguridad.

  Esto puede hacerse antes de revertir o inmediatamente después de que finaliza la reversión.

> Puesto que los ACE de control dinámico de acceso se ignoran después de volver a verlos, no es necesario eliminarlos cuando se aplican los ACE de control de acceso no dinámico a los archivos afectados. Sin embargo, si lo desea, puede eliminarlos manualmente.

Acceso seguro a SMB mediante políticas de exportación

Aprenda a usar políticas de exportación con el acceso SMB de ONTAP

Si se habilitan las políticas de exportación para el acceso de SMB en el servidor SMB, se utilizan las políticas de exportación cuando se controla el acceso a los volúmenes de SVM mediante clientes SMB. Para acceder a los datos, puede crear una política de exportación que permita el acceso a SMB y, a continuación, asociar la política con los volúmenes que contienen recursos compartidos de SMB.

Una política de exportación tiene una o varias reglas que se le aplican para especificar qué clientes pueden acceder a los datos y qué protocolos de autenticación son compatibles con el acceso de solo lectura y de lectura y escritura. Puede configurar directivas de exportación para permitir el acceso a través de SMB a todos los clientes, a una subred de clientes o a un cliente específico y para permitir la autenticación mediante autenticación Kerberos, autenticación NTLM o autenticación Kerberos y NTLM al determinar el acceso de sólo lectura y escritura a los datos.

Tras procesar todas las reglas de exportación aplicadas a la política de exportación, ONTAP puede determinar si el cliente obtiene acceso y qué nivel de acceso se concede. Las reglas de exportación se aplican a los equipos cliente, no a los usuarios y grupos de Windows. Las reglas de exportación no reemplazan la autenticación y autorización basada en usuarios y grupos de Windows. Las reglas de exportación proporcionan otra capa de seguridad de acceso, además de permisos de uso compartido y acceso a archivos.

Se asocia exactamente una política de exportación a cada volumen para configurar el acceso de los clientes al volumen. Cada SVM puede contener varias políticas de exportación. Esto le permite hacer lo siguiente para

las SVM con varios volúmenes:

- Asigne diferentes políticas de exportación a cada volumen de la SVM para controlar el acceso de clientes individuales a cada volumen de la SVM.
- Asigne la misma política de exportación a varios volúmenes del SVM para un control de acceso de clientes idéntico sin que tenga que crear una nueva política de exportación para cada volumen.

Cada SVM tiene, como mínimo, una política de exportación denominada «default», que no contiene reglas. No puede eliminar esta política de exportación, pero puede cambiarla ni cambiar el nombre. Cada volumen de la SVM está asociado de forma predeterminada con la política de exportación predeterminada. Si en la SVM se deshabilitan las políticas de exportación de acceso SMB, la política de exportación «predeterminado» no tendrá efecto en el acceso de las pymes.

Puede configurar reglas que proporcionen acceso a los hosts NFS y SMB y asociarlos con una política de exportación, que se puede asociar al volumen que contiene datos a los que necesitan acceder los hosts NFS y SMB. De forma alternativa, si hay algunos volúmenes en los que solo los clientes SMB necesitan acceso, puede configurar una directiva de exportación con reglas que solo permitan el acceso mediante el protocolo SMB y que sólo utilice Kerberos o NTLM (o ambos) para la autenticación de solo lectura y acceso de escritura. La política de exportación se asocia entonces a los volúmenes en los que solo se desea acceso a SMB.

Si se habilitan las políticas de exportación de SMB y un cliente realiza una solicitud de acceso que no permite la política de exportación correspondiente, la solicitud genera un mensaje de permiso denegado. Si un cliente no coincide con ninguna regla de la política de exportación del volumen, se deniega el acceso. Si una política de exportación está vacía, se deniegan implícitamente todos los accesos. Esto es cierto incluso si los permisos de recurso compartido y archivo de lo contrario permitirían el acceso. Esto significa que debe configurar la política de exportación para permitir, como mínimo, el siguiente valor en los volúmenes que contengan recursos compartidos de SMB:

- Permitir el acceso a todos los clientes o al subconjunto apropiado de clientes
- Permitir el acceso a través de SMB
- Permitir el acceso de sólo lectura y escritura adecuado mediante autenticación Kerberos o NTLM (o ambos)

Obtenga más información "configuración y gestión de políticas de exportación"sobre .

Conozca las reglas de exportación de SMB de ONTAP

Las reglas de exportación son los elementos funcionales de una política de exportación. Las reglas de exportación coinciden con las solicitudes de acceso de los clientes a un volumen con los parámetros específicos que se configuran para determinar cómo se manejan las solicitudes de acceso de los clientes.

La política de exportación debe contener al menos una regla de exportación para permitir el acceso a los clientes. Si una política de exportación contiene más de una regla, se procesan las reglas en el orden en que aparecen en la política de exportación. El orden de las reglas viene determinado por el número de índice de reglas. Si una regla coincide con un cliente, se utilizan los permisos de esa regla y no se procesan otras reglas. Si no hay reglas que coincidan, se deniega el acceso al cliente.

Puede configurar reglas de exportación para determinar los permisos de acceso de clientes con los siguientes criterios:

- El protocolo de acceso a archivos que utiliza el cliente para enviar la solicitud, por ejemplo, NFSv4 o SMB.

- Un identificador de cliente, por ejemplo, un nombre de host o una dirección IP.

  El tamaño máximo del `-clientmatch` campo es de 4096 caracteres.

- Tipo de seguridad utilizado por el cliente para autenticar, por ejemplo, Kerberos v5, NTLM o AUTH_SYS.

Si una regla especifica varios criterios, el cliente debe coincidir con todos ellos para que se aplique la regla.

Ejemplo
La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La solicitud de acceso del cliente se envía con el protocolo NFSv3 y el cliente tiene la dirección IP 10,1.17,37.

Aunque el protocolo de acceso del cliente coincida, la dirección IP del cliente se encuentra en una subred diferente de la especificada en la regla de exportación. Por lo tanto, la coincidencia de cliente falla y esta regla no se aplica a este cliente.

Ejemplo
La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La solicitud de acceso del cliente se envía con el protocolo NFSv4 y el cliente tiene la dirección IP 10,1.16,54.

El protocolo de acceso del cliente coincide y la dirección IP del cliente se encuentra en la subred especificada. Por lo tanto, la coincidencia de cliente es correcta y esta regla se aplica a este cliente. El cliente obtiene acceso de lectura y escritura independientemente de su tipo de seguridad.

Ejemplo
La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

El cliente n.o 1 tiene la dirección IP 10.1.16.207, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con Kerberos v5.

El cliente #2 tiene la dirección IP 10.1.16.211, envía una solicitud de acceso con el protocolo NFSv3 y se

autentica con AUTH_SYS.

El protocolo de acceso del cliente y la dirección IP coinciden con los dos clientes. El parámetro de solo lectura permite un acceso de solo lectura a todos los clientes independientemente del tipo de seguridad con el que se autentiquen. Por lo tanto, ambos clientes obtienen acceso de solo lectura. Sin embargo, sólo el cliente #1 obtiene acceso de lectura y escritura porque utilizó el tipo de seguridad aprobado Kerberos v5 para autenticar. El cliente n.o 2 no obtiene acceso de lectura/escritura.

Ejemplos de normas de política de exportación de ONTAP que restringen o permiten el acceso a través de SMB

Los ejemplos muestran cómo crear reglas de política de exportación que restringen o permiten el acceso a través de SMB en una SVM que tiene habilitadas políticas de exportación para el acceso a SMB.

Las políticas de exportación para acceso a SMB están deshabilitadas de forma predeterminada. Debe configurar reglas de políticas de exportación que restrinjan o permitan el acceso mediante SMB solo si ha habilitado políticas de exportación para el acceso a SMB.

Regla de exportación solo para acceso SMB

El siguiente comando crea una regla de exportación en la SVM denominada "'vs1'" que tiene la siguiente configuración:

- Nombre de la directiva: Cifs1
- Número de índice: 1
- Coincidencia de cliente: Sólo coincide con los clientes de la red 192.168.1.0/24
- Protocol: Solo habilita el acceso SMB
- Acceso de sólo lectura: A clientes que utilizan autenticación NTLM o Kerberos
- Acceso de lectura y escritura: A clientes que utilizan autenticación Kerberos

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

Regla de exportación para el acceso a SMB y NFS

El siguiente comando crea una regla de exportación en el SVM denominado»' vs1'» que tiene la siguiente configuración:

- Nombre de la directiva: Cifsssnfs1
- Número de índice: 2
- Coincidencia de cliente: Coincide con todos los clientes
- Protocolo: Acceso SMB y NFS
- Acceso de sólo lectura: A todos los clientes
- Acceso de lectura y escritura: A clientes que utilizan Kerberos (NFS y SMB) o autenticación NTLM (SMB)
- Asignación para el ID de usuario de UNIX 0 (cero): Se asigna al ID de usuario 65534 (que normalmente asigna al nombre de usuario nobody)

- Acceso suid y sgid: Permite

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule any
-rwrule krb5,ntlm -anon 65534 -allow-suid true
```

Regla de exportación para acceso SMB únicamente mediante NTLM

El siguiente comando crea una regla de exportación en la SVM denominada "'vs1'" que tiene la siguiente configuración:

- Nombre de la política: Ntlm1
- Número de índice: 1
- Coincidencia de cliente: Coincide con todos los clientes
- Protocol: Solo habilita el acceso SMB
- Acceso de sólo lectura: Sólo para clientes que utilizan NTLM
- Acceso de lectura y escritura: Sólo para clientes que utilizan NTLM

> Si configura la opción de sólo lectura o la opción de lectura y escritura para el acceso NTLM, debe utilizar las entradas basadas en dirección IP en la opción de coincidencia de cliente. De lo contrario, recibirá `access denied` errores. Esto se debe a que ONTAP utiliza los nombres principales de servicios (SPN) de Kerberos al utilizar un nombre de host para comprobar los derechos de acceso del cliente. La autenticación NTLM no admite nombres SPN.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

Habilitar o deshabilitar las políticas de exportación de ONTAP para el acceso SMB

Puede habilitar o deshabilitar las políticas de exportación para acceso de SMB en máquinas virtuales de almacenamiento (SVM). El uso de políticas de exportación para controlar el acceso de SMB a los recursos es opcional.

Antes de empezar

A continuación, se muestran los requisitos para habilitar las políticas de exportación para SMB:

- El cliente debe tener un registro PTR en DNS antes de crear las reglas de exportación para ese cliente.
- Si la SVM proporciona acceso A los clientes NFS, se requiere un conjunto adicional de registros «A» y «PTR» para los nombres de host y el nombre de host que desea utilizar para el acceso NFS es diferente del nombre del servidor CIFS.

Acerca de esta tarea

Al configurar un nuevo servidor CIFS en la SVM, el uso de políticas de exportación para acceso de SMB está deshabilitado de forma predeterminada. Puede habilitar las políticas de exportación para el acceso de SMB si desea controlar el acceso en función del protocolo de autenticación o en direcciones IP de cliente o nombres

de host. Es posible habilitar o deshabilitar las políticas de exportación para el acceso de SMB en cualquier momento.

> Al habilitar políticas de exportación para CIFS/SMB en una SVM habilitada para NFS, un cliente Linux puede usar `showmount -e` el comando en la SVM para ver las rutas de unión de todos los volúmenes SMB con reglas de políticas de exportación asociadas.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Habilite o deshabilite políticas de exportación:
   - Habilite políticas de exportación: `vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled true`
   - Desactivar políticas de exportación: `vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled false`
3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Ejemplo

El siguiente ejemplo permite el uso de políticas de exportación para controlar el acceso de clientes SMB a los recursos en SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

Acceso seguro a archivos mediante Storage-Level Access Guard

Obtenga información sobre el acceso seguro a archivos SMB de ONTAP mediante Storage-Level Access Guard

Además de proteger el acceso mediante el uso nativo a nivel de archivo y la seguridad de exportación y uso compartido, puede configurar la protección de acceso a nivel de almacenamiento, una tercera capa de seguridad aplicada por ONTAP a nivel de volumen. El servicio de protección de acceso a nivel de almacenamiento se aplica para acceder desde todos los protocolos NAS al objeto de almacenamiento al que se aplica.

Sólo se admiten permisos de acceso NTFS. Para que ONTAP realice comprobaciones de seguridad en los usuarios de UNIX con el fin de acceder a los datos de los volúmenes para los que se ha aplicado la protección de acceso a nivel de almacenamiento, el usuario de UNIX debe asignar a un usuario de Windows en la SVM propietaria del volumen.

Comportamiento de protección del acceso al nivel de almacenamiento

- Storage-Level Access Guard se aplica a todos los archivos o todos los directorios de un objeto de almacenamiento.

  Puesto que todos los archivos o directorios de un volumen están sujetos a la configuración de Storage-Level Access Guard, no se requiere la herencia a través de la propagación.

- Puede configurar Storage-Level Access Guard para que se aplique sólo a archivos, sólo a directorios o a los archivos y directorios de un volumen.
  - Seguridad de archivos y directorios

    Se aplica a todos los directorios y archivos del objeto de almacenamiento. Esta es la configuración predeterminada.

  - Seguridad de archivos

    Se aplica a cada archivo dentro del objeto de almacenamiento. Aplicar esta seguridad no afecta al acceso a los directorios o a la auditoría de ellos.

  - Seguridad del directorio

    Se aplica a cada directorio dentro del objeto de almacenamiento. Aplicar esta seguridad no afecta al acceso a los archivos ni a la auditoría de ellos.

- Se utiliza Storage-Level Access Guard para restringir los permisos.

  Nunca dará permisos de acceso adicionales.

- Si ve la configuración de seguridad en un archivo o un directorio desde un cliente NFS o SMB, no verá la seguridad de Access Guard a nivel de almacenamiento.

  Se aplica en el nivel de objeto de almacenamiento y se almacena en los metadatos que se usan para determinar la efectividad de los permisos.

- La seguridad a nivel de almacenamiento no puede ser revocada desde un cliente, incluso por un administrador de sistema (Windows o UNIX)

  Está diseñado para que lo modifiquen únicamente administradores del almacenamiento.

- Se puede aplicar Access Guard en el nivel de almacenamiento a volúmenes con un estilo de seguridad NTFS o mixto.
- Es posible aplicar una protección de acceso al nivel de almacenamiento a los volúmenes con estilo de seguridad UNIX siempre que la SVM que contiene el volumen tenga configurado un servidor CIFS.
- Cuando los volúmenes se montan en una ruta de unión de volúmenes y, si existe la función Storage-Level Access Guard en esa ruta, no se propagará a los volúmenes montados bajo ella.
- El descriptor de seguridad de Storage-Level Access Guard se replica con la replicación de datos de SnapMirror y con la replicación de SVM.
- Hay una dispensación especial para los escáneres de virus.

  Estos servidores pueden acceder de forma excepcional a los archivos y directorios de pantalla, incluso si Storage-Level Access Guard deniega el acceso al objeto.

- Las notificaciones de FPolicy no se envían si se deniega el acceso debido a la protección de acceso al nivel de almacenamiento.

Orden de las comprobaciones de acceso

El acceso a un archivo o directorio se determina por el efecto combinado de los permisos de exportación o uso compartido, los permisos de Storage-Level Access Guard configurados en volúmenes y los permisos de archivo nativos aplicados a archivos y/o directorios. Se evalúan todos los niveles de seguridad para determinar los permisos efectivos que tiene un archivo o directorio. Las comprobaciones de acceso de seguridad se realizan en el siguiente orden:

1. Permisos a nivel de exportación de SMB o NFS
2. Protección de acceso al nivel de almacenamiento
3. Listas de control de acceso a carpetas/archivos NTFS (ACL), ACL de NFSv4 o bits de modo UNIX

Casos de uso para usar Storage-Level Access Guard

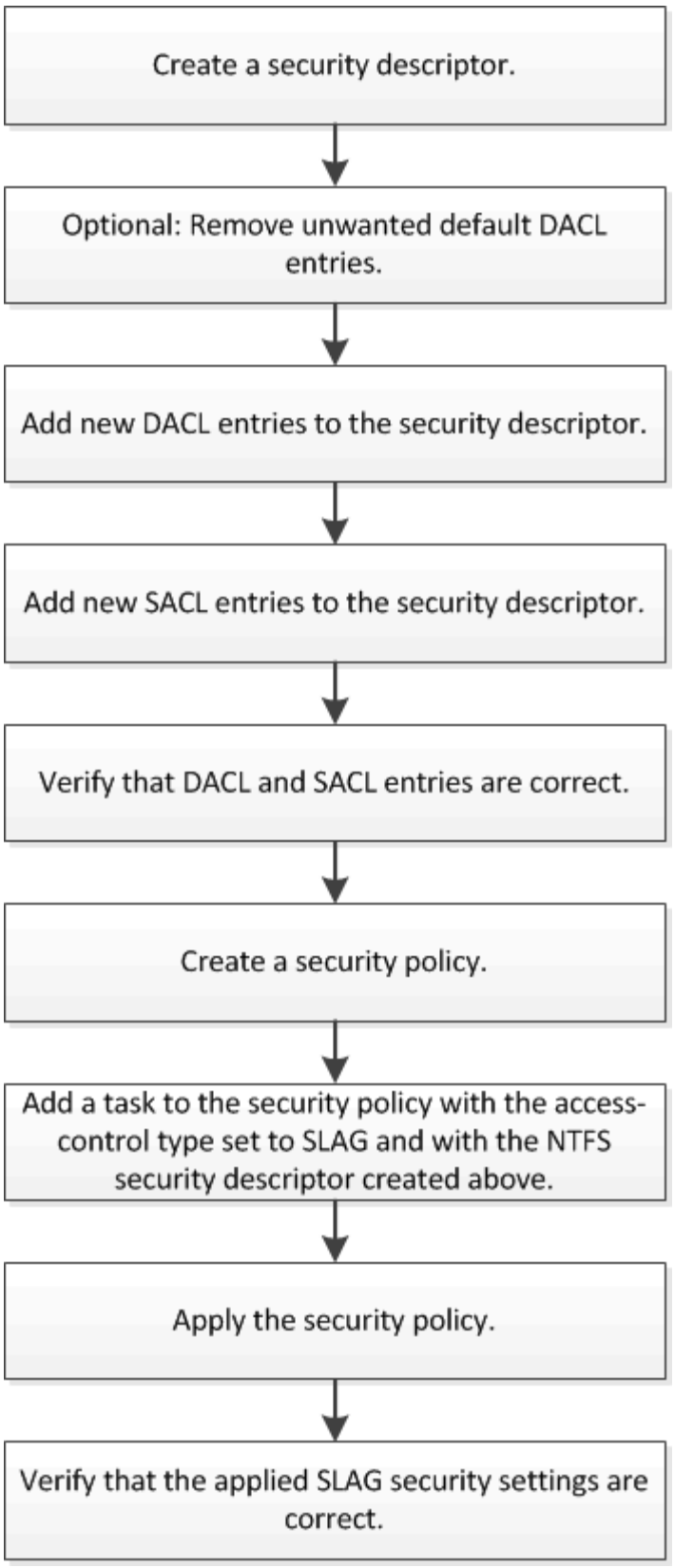
El servicio de protección de acceso a nivel de almacenamiento proporciona una seguridad adicional a nivel de almacenamiento, que no puede verse en el lado del cliente; por lo tanto, no puede ser revocado por ninguno de los usuarios o administradores de sus escritorios. Existen determinados casos de uso en los que es conveniente la capacidad de controlar el acceso en el nivel de almacenamiento.

Los casos de uso típicos de esta función incluyen las siguientes situaciones:

- Protección de la propiedad intelectual mediante la auditoría y el control del acceso de todos los usuarios a nivel de almacenamiento
- Almacenamiento para empresas de servicios financieros, incluidos grupos bancarios y comerciales
- Servicios gubernamentales con almacenamiento de ficheros independiente para departamentos individuales
- Universidades que protegen todos los archivos de los estudiantes

Flujo de trabajo de configuración para Storage-Level Access Guard en servidores SMB de ONTAP

El flujo de trabajo para configurar la protección de acceso al nivel de almacenamiento (SSLAG) utiliza los mismos comandos de la CLI de ONTAP que utiliza para configurar permisos de archivos NTFS y directivas de auditoría. En lugar de configurar el acceso a archivos y directorios en un destino designado, debe configurar SLAG en el volumen de máquina virtual de almacenamiento designado.



Información relacionada

Configurar la protección de acceso a nivel de almacenamiento en los servidores

Configurar Storage-Level Access Guard en servidores SMB de ONTAP

Hay una serie de pasos que se deben seguir para configurar la protección del acceso al nivel de almacenamiento en un volumen o un qtree. El protector de acceso al nivel de almacenamiento ofrece un nivel de seguridad de acceso que se establece en el nivel de almacenamiento. Proporciona seguridad que se aplica a todos los accesos desde todos los protocolos NAS al objeto de almacenamiento al que se ha aplicado.

Pasos

1. Cree un descriptor de seguridad con `vserver security file-directory ntfs create` el comando.

   `vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1 vserver security file-directory ntfs show -vserver vs1`

   ```
   Vserver: vs1

      NTFS Security    Owner Name
      Descriptor Name
      ------------     --------------
      sd1              -
   ```

   Se crea un descriptor de seguridad con las siguientes cuatro entradas predeterminadas de control de acceso de DACL (ACE):

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       BUILTIN\Administrators
                        allow    full-control   this-folder, sub-folders,
   files
       BUILTIN\Users    allow    full-control   this-folder, sub-folders,
   files
       CREATOR OWNER    allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   Si no desea utilizar las entradas predeterminadas al configurar Storage-Level Access Guard, puede eliminarlas antes de crear y agregar sus propias ACE al descriptor de seguridad.

2. Quite cualquiera de los ACE de DACL predeterminados del descriptor de seguridad que no desea

configurar con la seguridad Storage-Level Access Guard:

a. Elimine todas las ACE DACL no deseadas con el `vserver security file-directory ntfs dacl remove` comando.

   En este ejemplo, se quitan tres ACE de DACL predeterminados del descriptor de seguridad: BUILTIN\Administrators, BUILTIN\Users y CREATOR OWNER.

   ```
   vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
   -access-type allow -account builtin\users vserver security file-directory
   ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
   builtin\administrators vserver security file-directory ntfs dacl remove
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
   ```

b. Compruebe que las ACL DACL que no desea utilizar para la seguridad de Access Guard de nivel de almacenamiento se hayan eliminado del descriptor de seguridad mediante `vserver security file-directory ntfs dacl show` el comando.

   En este ejemplo, la salida del comando verifica que se han eliminado tres ACE de DACL predeterminados del descriptor de seguridad, dejando sólo la entrada de ACE de DACL predeterminada de NT AUTHORITY\SYSTEM:

   ```
   vserver security file-directory ntfs dacl show -vserver vs1
   ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

3. Añada una o varias entradas DACL a un descriptor de seguridad mediante `vserver security file-directory ntfs dacl add` el comando.

   En este ejemplo, se agregan dos ACE de DACL al descriptor de seguridad:

   ```
   vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
   -access-type allow -account example\engineering -rights full-control -apply-to
   this-folder,sub-folders,files vserver security file-directory ntfs dacl add
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
   -rights read -apply-to this-folder,sub-folders,files
   ```

4. Añada una o varias entradas de SACL a un descriptor de seguridad mediante `vserver security file-directory ntfs sacl add` el comando.

   En este ejemplo, se agregan dos ACE de SACL al descriptor de seguridad:

   ```
   vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
   ```

```
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. Verifique que las ACE DACL y SACL estén configuradas correctamente mediante los `vserver security file-directory ntfs dacl show` `vserver security file-directory ntfs sacl show` comandos y, respectivamente.

   En este ejemplo, el siguiente comando muestra información sobre las entradas de DACL para el descriptor de seguridad “D1”:

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   ```

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        allow    read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   En este ejemplo, el siguiente comando muestra información sobre las entradas de SACL para el descriptor de seguridad “D1”:

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    EXAMPLE\Domain Users
                     failure  read           this-folder, sub-folders,
files
    EXAMPLE\engineering
                     success  full-control   this-folder, sub-folders,
files
```

6. Cree una política de seguridad mediante `vserver security file-directory policy create` el comando.

   En el siguiente ejemplo se crea una directiva denominada «'póliza 1'»:

   ```
   vserver security file-directory policy create -vserver vs1 -policy-name
   policy1
   ```

7. Compruebe que la política se ha configurado correctamente mediante `vserver security file-directory policy show` el comando.

   ```
   vserver security file-directory policy show
   ```

   ```
      Vserver          Policy Name
      ------------     --------------
      vs1              policy1
   ```

8. Agregue una tarea con un descriptor de seguridad asociado a la política de seguridad mediante el `vserver security file-directory policy task add` comando con el `-access-control` parámetro definido en `slag`.

   Aunque una directiva puede contener más de una tarea de Storage-Level Access Guard, no puede configurar una directiva para que contenga tareas de directorio de archivos y de Storage-Level Access Guard. Una política debe contener todas las tareas de Storage-Level Access Guard o todas las tareas de directorio de archivos.

   En este ejemplo, se agrega una tarea a la política denominada "'poly1'", que se asigna al descriptor de seguridad "sD1". Se asigna a la `/datavol1` ruta con el tipo de control de acceso establecido en “Slag”.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode
   propagate -ntfs-sd sd1
   ```

9. Compruebe que la tarea está configurada correctamente mediante `vserver security file-directory policy task show` el comando.

```
vserver security file-directory policy task show -vserver vs1 -policy-name
policy1
```

```
 Vserver: vs1
  Policy: policy1

   Index  File/Folder  Access           Security  NTFS       NTFS
Security
          Path         Control          Type      Mode       Descriptor
Name
   -----  -----------  ---------------  --------  ----------
---------------
   1      /datavol1    slag             ntfs      propagate  sd1
```

10. Aplique la política de seguridad Access Guard de nivel de almacenamiento mediante `vserver security file-directory apply` el comando.

    ```
    vserver security file-directory apply -vserver vs1 -policy-name policy1
    ```

    El trabajo que se va a aplicar la directiva de seguridad está programado.

11. Verifique que la configuración de seguridad de Access Guard de nivel de almacenamiento aplicada sea correcta mediante el `vserver security file-directory show` comando.

    En este ejemplo, la salida del comando muestra que la seguridad de Storage-Level Access Guard se ha aplicado al volumen NTFS `/datavol1` . Aunque el DACL predeterminado que permite el control total para todos permanece, la seguridad de Storage-Level Access Guard restringe (y audita) el acceso a los grupos definidos en la configuración de Storage-Level Access Guard.

    ```
    vserver security file-directory show -vserver vs1 -path /datavol1
    ```

```
                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Información relacionada

- Comandos para administrar la seguridad de archivos NTFS, las políticas de auditoría de NTFS y la protección de acceso a nivel de almacenamiento
- Flujo de trabajo de configuración para Storage-Level Access Guard en servidores
- Mostrar información sobre la protección de acceso a nivel de almacenamiento en los servidores
- Eliminar la protección de acceso a nivel de almacenamiento en los servidores

Matriz SLAG eficaz en servidores SMB de ONTAP

Puede configurar SLAG en un volumen, un qtree o ambos. La matriz SLAG define en qué volumen o qtree se aplica la configuración SLAG en los distintos escenarios que se indican en la tabla.

	Volumen SLAG en un AFS	ASIGNACIÓN DE volumen en una instantánea	Qtree SLAG en un AFS	ELIMINACIÓN DE qtree en una copia snapshot
Acceso de volumen en un sistema de archivos de acceso (AFS)	SÍ	NO	N / A	N / A
Acceso del volumen en una copia de Snapshot	SÍ	NO	N / A	N / A
Acceso a Qtree en un AFS (cuando SLAG está presente en el qtree)	NO	NO	SÍ	NO
Acceso a Qtree en un AFS (cuando SLAG no está presente en qtree)	SÍ	NO	NO	NO
Acceso a Qtree en una copia de Snapshot (cuando hay UN SUFIJO en el AFS para qtree)	NO	NO	SÍ	NO
Acceso a Qtree en una copia de Snapshot (cuando no está presente LA función SLAG en el AFS para qtree)	SÍ	NO	NO	NO

Mostrar información sobre Storage-Level Access Guard en servidores SMB de ONTAP

El servicio de protección del acceso a nivel de almacenamiento es una tercera capa de seguridad aplicada en un volumen o un qtree. La configuración de Storage-Level Access Guard no se puede ver mediante la ventana Propiedades de Windows. Es necesario usar la interfaz de línea de comandos de ONTAP para ver información sobre la seguridad de protección del acceso a nivel de almacenamiento, que se puede utilizar para validar la configuración o solucionar problemas de acceso a archivos.

Acerca de esta tarea

Se debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta al volumen o qtree cuya información de seguridad de protección de acceso de nivel de almacenamiento desea mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

Paso

1. Mostrar la configuración de seguridad de protección de acceso a nivel de almacenamiento con el nivel de detalle deseado:

Si desea mostrar información…	Introduzca el siguiente comando…
En forma de resumen	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Con detalle ampliado	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Ejemplos

En el siguiente ejemplo, se muestra información de seguridad de Access Guard de nivel de almacenamiento para el volumen de estilo de seguridad NTFS con la ruta `/datavol1` en SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

En el siguiente ejemplo, se muestra información de Access Guard al nivel de almacenamiento acerca del volumen mixto de estilo de seguridad en la ruta de `/datavol5` SVM VS1. El nivel superior de este volumen tiene una seguridad efectiva para UNIX. El volumen tiene seguridad de protección de acceso en el nivel de almacenamiento.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Eliminar la protección de acceso a nivel de almacenamiento en servidores SMB de ONTAP

Puede quitar la protección de acceso al nivel de almacenamiento en un volumen o qtree si ya no desea establecer la seguridad de acceso en el nivel de almacenamiento. La eliminación de la protección de acceso a nivel de almacenamiento no modifica ni quita la seguridad normal de archivos NTFS y directorios.

Pasos

1. Compruebe que el volumen o qtree tiene la protección de acceso a nivel de almacenamiento configurada mediante `vserver security file-directory show` el comando.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

                         Storage-Level Access Guard security
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

2. Quite la protección de acceso al nivel de almacenamiento mediante `vserver security file-directory remove-slag` el comando.

   ```
   vserver security file-directory remove-slag -vserver vs1 -path /datavol2
   ```

3. Compruebe que la protección de acceso al nivel de almacenamiento se haya eliminado del volumen o qtree mediante `vserver security file-directory show` el comando.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```

Gestione el acceso a archivos mediante SMB

Utilice usuarios y grupos locales para autenticación y autorización

Cómo utiliza ONTAP usuarios y grupos locales

Obtenga información sobre los usuarios y grupos locales de ONTAP SMB

Debe saber cuáles son los usuarios y grupos locales, así como alguna información básica sobre ellos, antes de determinar si configurar y utilizar usuarios y grupos locales en su entorno.

- **Usuario local**

  Una cuenta de usuario con un identificador de seguridad único (SID) que solo tiene visibilidad en la máquina virtual de almacenamiento (SVM) donde se crea. Las cuentas de usuario local tienen un conjunto de atributos, incluidos el nombre de usuario y el SID. Una cuenta de usuario local autentica de forma local en el servidor CIFS mediante la autenticación NTLM.

  Las cuentas de usuario tienen varios usos:

  - Se utiliza para otorgar privilegios *User Rights Management* a un usuario.
  - Se usa para controlar el acceso a nivel de recurso compartido y de archivo a los recursos de archivos y carpetas que posee la SVM.

- **Grupo local**

  Un grupo con un SID exclusivo tiene visibilidad solo en la SVM donde se crea. Los grupos contienen un conjunto de miembros. Los miembros pueden ser usuarios locales, usuarios de dominio, grupos de dominio y cuentas de equipos de dominio. Los grupos se pueden crear, modificar o eliminar.

  Los grupos tienen varios usos:

  - Se utiliza para otorgar privilegios *User Rights Management* a sus miembros.
  - Se usa para controlar el acceso a nivel de recurso compartido y de archivo a los recursos de archivos y carpetas que posee la SVM.
- **Dominio local**

  Un dominio que tiene un alcance local, delimitado por la SVM. El nombre del dominio local es el nombre del servidor CIFS. Los usuarios y grupos locales se encuentran dentro del dominio local.

- **Identificador de seguridad (SID)**

  Un SID es un valor numérico de longitud variable que identifica los principios de seguridad de estilo Windows. Por ejemplo, un SID típico toma la siguiente forma: S-1-5-21-3139654847-1303905135-2517279418-123456.

- **Autenticación NTLM**

  Un método de seguridad de Microsoft Windows que se utiliza para autenticar usuarios en un servidor CIFS.

- **Base de datos replicada en cluster (RDB)**

  Base de datos replicada con una instancia en cada nodo de un clúster. Los objetos de usuario local y de grupo se almacenan en el RDB.

Razones para crear usuarios y grupos locales de ONTAP SMB

Hay varias razones para crear usuarios locales y grupos locales en la máquina virtual de almacenamiento (SVM). Por ejemplo, puede tener acceso a un servidor SMB utilizando una cuenta de usuario local si los controladores de dominio (DC) no están disponibles, es posible que desee utilizar grupos locales para asignar privilegios o que el servidor SMB esté en un grupo de trabajo.

Es posible crear una o varias cuentas de usuario locales por los siguientes motivos:

- El servidor SMB está en un grupo de trabajo y los usuarios del dominio no están disponibles.

  Los usuarios locales son necesarios en configuraciones de grupos de trabajo.

- Puede autenticar e iniciar sesión en el servidor SMB si las controladoras de dominio no están disponibles.

  Los usuarios locales pueden autenticarse con el servidor SMB mediante la autenticación NTLM cuando el controlador de dominio está inactivo o cuando los problemas de red impiden que el servidor SMB se ponga en contacto con el controlador de dominio.

- Desea asignar privilegios *User Rights Management* a un usuario local.

User Rights Management es la capacidad de un administrador de servidor SMB para controlar los derechos que tienen los usuarios y los grupos en la SVM. Puede asignar privilegios a un usuario asignando los privilegios a la cuenta del usuario o haciendo que el usuario sea miembro de un grupo local que tenga esos privilegios.

Se pueden crear uno o varios grupos locales por los siguientes motivos:

- El servidor SMB está en un grupo de trabajo y los grupos de dominio no están disponibles.

  Los grupos locales no son necesarios en las configuraciones de grupos de trabajo, pero pueden ser útiles para administrar privilegios de acceso para los usuarios de grupos de trabajo locales.

- Desea controlar el acceso a los recursos de archivos y carpetas mediante grupos locales para controlar el uso compartido y el acceso a archivos.
- Desea crear grupos locales con privilegios *User Rights Management* personalizados.

  Algunos grupos de usuarios integrados tienen privilegios predefinidos. Para asignar un conjunto personalizado de privilegios, puede crear un grupo local y asignar los privilegios necesarios a ese grupo. A continuación, puede agregar usuarios locales, usuarios de dominio y grupos de dominio al grupo local.

Información relacionada

- Obtenga más información sobre la autenticación de usuarios locales
- Lista de privilegios compatibles

Obtenga información sobre la autenticación de usuarios SMB de ONTAP local

Para que un usuario local pueda acceder a los datos en un servidor CIFS, el usuario debe crear una sesión autenticada.

Debido a que el bloque de mensajes del servidor se basa en sesiones, la identidad del usuario se puede determinar una sola vez cuando se configura la sesión por primera vez. El servidor CIFS utiliza autenticación basada en NTLM al autenticar usuarios locales. Son compatibles tanto NTLMv1 como NTLMv2.

ONTAP utiliza autenticación local en tres casos de uso. Cada caso de uso depende de si la parte del dominio del nombre de usuario (con el formato de DOMINIO\usuario) coincide con el nombre de dominio local del servidor CIFS (el nombre del servidor CIFS):

- La parte del dominio coincide

  Los usuarios que proporcionan credenciales de usuario local al solicitar acceso a los datos se autentican localmente en el servidor CIFS.

- La parte del dominio no coincide

  ONTAP intenta utilizar la autenticación NTLM con un controlador de dominio del dominio al que pertenece el servidor CIFS. Si la autenticación se realiza correctamente, se completa el inicio de sesión. Si no se realiza correctamente, lo que sucede a continuación depende de por qué la autenticación no se ha realizado correctamente.

  Por ejemplo, si el usuario existe en Active Directory pero la contraseña no es válida o ha caducado, ONTAP no intenta utilizar la cuenta de usuario local correspondiente en el servidor CIFS. En su lugar, la autenticación genera errores. Hay otros casos en los que ONTAP utiliza la cuenta local correspondiente en el servidor CIFS, si existe, para la autenticación, aunque los nombres de dominio NetBIOS no coincidan.

Por ejemplo, si existe una cuenta de dominio coincidente pero está deshabilitada, ONTAP utiliza la cuenta local correspondiente en el servidor CIFS para la autenticación.

- No se ha especificado la parte del dominio

  ONTAP intenta primero la autenticación como usuario local. Si la autenticación como usuario local falla, ONTAP autentica al usuario con una controladora de dominio en el dominio al que pertenece el servidor CIFS.

Una vez que la autenticación de usuario local o de dominio se ha completado correctamente, ONTAP crea un token de acceso de usuario completo, que tiene en cuenta la pertenencia a grupos locales y los privilegios.

Para obtener más información acerca de la autenticación NTLM para usuarios locales, consulte la documentación de Microsoft Windows.

Información relacionada

Habilitar o deshabilitar la autenticación de usuarios locales en los servidores

Obtenga más información sobre los tokens de acceso de usuario SMB de ONTAP

Cuando un usuario asigna un recurso compartido, se establece una sesión SMB autenticada y se crea un token de acceso de usuario que contiene información acerca del usuario, la pertenencia al grupo del usuario y los privilegios acumulativos, así como el usuario UNIX asignado.

A menos que la funcionalidad esté deshabilitada, la información de grupo y de usuario local también se agrega al token de acceso de usuario. La forma en que se crean los tokens de acceso depende de si el inicio de sesión es para un usuario local o un usuario de dominio de Active Directory:

- Inicio de sesión de usuario local

  Aunque los usuarios locales pueden ser miembros de diferentes grupos locales, los grupos locales no pueden ser miembros de otros grupos locales. El token de acceso de usuario local se compone de una unión de todos los privilegios asignados a grupos a los que pertenece un usuario local determinado.

- Inicio de sesión de usuario de dominio

  Cuando un usuario de dominio inicia sesión, ONTAP obtiene un token de acceso de usuario que contiene el SID y SID de usuario para todos los grupos de dominio a los que pertenece el usuario. ONTAP utiliza la unión del token de acceso de usuario de dominio con el token de acceso proporcionado por las membresías locales de los grupos de dominio del usuario (si los hay), así como todos los privilegios directos asignados al usuario de dominio o cualquiera de sus pertenencias a grupos de dominio.

Tanto para el inicio de sesión local como para el usuario de dominio, el RID de grupo principal también está configurado para el token de acceso de usuario. El RID predeterminado es `Domain Users` (RID 513). No puede cambiar el valor predeterminado.

El proceso de asignación de nombres de Windows a UNIX y UNIX a Windows sigue las mismas reglas para las cuentas locales y de dominio.

> No hay ningún mapeo implícito y automático de un usuario UNIX a una cuenta local. Si es necesario, se debe especificar una regla de asignación explícita mediante los comandos de asignación de nombres existentes.

Obtenga información sobre el uso de SnapMirror en SVM SMB de ONTAP que contienen grupos locales

Debe tener en cuenta las directrices al configurar SnapMirror en los volúmenes que son propiedad de las SVM que contienen grupos locales.

No se pueden utilizar grupos locales en ACE aplicados a archivos, directorios o recursos compartidos replicados por SnapMirror en otra SVM. Si utiliza la función SnapMirror para crear un reflejo de recuperación ante desastres en un volumen en otra SVM y el volumen tiene una ACE para un grupo local, la ACE no es válida en el reflejo. Si los datos se replican en una SVM diferente, estos se cruzan realmente en un dominio local diferente. Los permisos concedidos a los usuarios y grupos locales solo son válidos dentro del ámbito de la SVM en la que se crearon originalmente.

Conozca los efectos de eliminar servidores SMB de ONTAP en usuarios y grupos

El conjunto predeterminado de usuarios y grupos locales se crea cuando se crea un servidor CIFS y está asociado con las máquinas virtuales de almacenamiento (SVM) que alojan el servidor CIFS. Los administradores de SVM pueden crear usuarios y grupos locales en cualquier momento. Debe saber qué sucede con los usuarios locales y los grupos al eliminar el servidor CIFS.

Los usuarios y grupos locales están asociados a las SVM; por lo tanto, no se eliminan cuando los servidores CIFS se eliminan debido a consideraciones de seguridad. Aunque los usuarios y grupos locales no se eliminan al eliminar el servidor CIFS, sí se ocultan. No se pueden ver ni gestionar usuarios y grupos locales hasta que se vuelva a crear un servidor CIFS en la SVM.

> El estado administrativo del servidor CIFS no afecta a la visibilidad de los grupos o usuarios locales.

Aprenda a usar Microsoft Management Console con usuarios y grupos locales de ONTAP SMB

Puede ver información acerca de los usuarios y grupos locales desde la Consola de administración de Microsoft. Con esta versión de ONTAP, no puede realizar otras tareas de administración para usuarios y grupos locales desde la Consola de administración de Microsoft.

Obtenga información sobre cómo revertir clústeres SMB de ONTAP

Si piensa revertir el clúster a una versión de ONTAP que no da soporte a usuarios y grupos locales y se están utilizando grupos y usuarios locales para gestionar los derechos de usuario o el acceso a los archivos, debe tener en cuenta ciertas consideraciones.

- Debido a motivos de seguridad, no se elimina la información sobre usuarios locales, grupos y privilegios configurados cuando ONTAP se revierte a una versión que no admite la funcionalidad de usuarios y grupos locales.
- Al volver a una versión principal anterior de ONTAP, ONTAP no utiliza usuarios ni grupos locales durante la autenticación ni la creación de credenciales.
- Los usuarios y grupos locales no se quitan de las ACL de archivos y carpetas.

- Se deniegan las solicitudes de acceso a archivos que dependen de que se conceda el acceso debido a los permisos concedidos a los usuarios o grupos locales.

  Para permitir el acceso, debe volver a configurar los permisos de archivo para permitir el acceso basado en objetos de dominio en lugar de objetos de usuario local y de grupo.

Qué privilegios locales son

Lista de privilegios SMB de ONTAP admitidos

ONTAP tiene un conjunto predefinido de privilegios admitidos. Algunos grupos locales predefinidos tienen algunos de estos privilegios añadidos de forma predeterminada. También puede agregar o quitar privilegios de los grupos predefinidos o crear nuevos usuarios o grupos locales y agregar privilegios a los grupos que creó o a los usuarios y grupos de dominio existentes.

En la siguiente tabla se enumeran los privilegios admitidos en la máquina virtual de almacenamiento (SVM) y se proporciona una lista de los grupos BUILTIN con privilegios asignados:

Nombre del privilegio	Configuración de seguridad predeterminada	Descripción
`SeTcbPrivilege`	Ninguno	Actuar como parte del sistema operativo
`SeBackupPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Realice copias de seguridad de archivos y directorios, anulando cualquier ACL
`SeRestorePrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Restaurar archivos y directorios, anulando cualquier ACL establecer cualquier SID de usuario o grupo válido como propietario del archivo
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	Tomar posesión de archivos u otros objetos
`SeSecurityPrivilege`	`BUILTIN\Administrators`	Gestionar auditoría Esto incluye ver, volcar y borrar el registro de seguridad.
`SeChangeNotifyPrivilege`	`BUILTIN\Administrators`, , , , `BUILTIN\Backup Operators` `BUILTIN\Power Users` `BUILTIN\Users` , `Everyone`	Comprobación de desvío transversal No es necesario que los usuarios con este privilegio tengan permisos de desplazamiento (x) para recorrer carpetas, vínculos simbólicos o uniones.

Información relacionada

- Obtenga información sobre la asignación de privilegios
- Obtenga información sobre cómo configurar la comprobación de recorrido de derivación

Obtenga información sobre la asignación de privilegios SMB de ONTAP

Es posible asignar privilegios directamente a usuarios locales o a usuarios de dominio. También puede asignar usuarios a grupos locales cuyos privilegios asignados coincidan con las capacidades que desea que tengan esos usuarios.

- Puede asignar un conjunto de privilegios a un grupo que cree.

  A continuación, agregue un usuario al grupo que tenga los privilegios que desea que tenga ese usuario.

- También puede asignar usuarios locales y usuarios de dominio a grupos predefinidos cuyos privilegios predeterminados coincidan con los privilegios que desea conceder a esos usuarios.

Información relacionada

- Añada privilegios a usuarios o grupos locales o de dominio
- Quitar privilegios de usuarios o grupos locales o de dominio
- Restablecer privilegios para usuarios y grupos locales o de dominio
- Obtenga información sobre cómo configurar la comprobación de recorrido de derivación

Obtenga información sobre los grupos BUILTIN y las cuentas de administrador local en los servidores SMB de ONTAP

Hay ciertas pautas que debe tener en cuenta cuando utilice los grupos BUILTIN y la cuenta de administrador local. Por ejemplo, puede cambiar el nombre de la cuenta de administrador local, pero no puede eliminar esta cuenta.

- Se puede cambiar el nombre de la cuenta Administrador, pero no se puede eliminar.
- La cuenta de administrador no se puede quitar del grupo BUILTIN\Administrators.
- Se puede cambiar el nombre de los grupos INTEGRADOS, pero no se pueden eliminar.

  Después de cambiar el nombre del grupo BUILTIN, se puede crear otro objeto local con el nombre bien conocido; sin embargo, al objeto se le asigna UN NUEVO RID.

- No hay una cuenta de invitado local.

Información relacionada

Grupos BUILTIN predefinidos y privilegios predeterminados

Requisitos para las contraseñas de usuarios locales de ONTAP SMB

De manera predeterminada, las contraseñas de usuario local deben cumplir con los requisitos complejos. Los requisitos de complejidad de la contraseña son similares a los que se definen en la directiva de seguridad local de Microsoft Windows.

La contraseña debe cumplir los siguientes criterios:

- Debe tener al menos seis caracteres de longitud
- No se debe contener el nombre de cuenta de usuario
- Debe contener caracteres de al menos tres de las siguientes cuatro categorías:
  - Caracteres en mayúsculas (De La A a la Z)
  - Caracteres en minúscula (de la a a la z)
  - Base de 10 dígitos (de 0 a 9)
  - Caracteres especiales:

```
~ ! @ # $ % {caret} & * _ - + = ` \ | ( ) [ ] : ; " ' < > , . ? /
```

Información relacionada

- Configurar la complejidad de la contraseña para usuarios locales
- Mostrar información sobre la configuración de seguridad del servidor
- Cambiar las contraseñas de la cuenta de usuario local

Grupos BUILTIN predefinidos y privilegios SMB de ONTAP predeterminados

Puede asignar la pertenencia de un usuario local o un usuario de dominio a un conjunto predefinido de grupos BUILTIN proporcionados por ONTAP. Los grupos predefinidos tienen privilegios predefinidos asignados.

En la siguiente tabla se describen los grupos predefinidos:

Grupo BUILTIN predefinido	Privilegios predeterminados
`BUILTIN\Administrators`RID 544 Cuando se crea por primera vez, la `Administrator` cuenta local, con un RID de 500, se convierte automáticamente en miembro de este grupo. Cuando la máquina virtual de almacenamiento (SVM) se une a un dominio, `domain\Domain Admins` el grupo se añade al grupo. Si la SVM abandona el dominio, `domain\Domain Admins` el grupo se eliminará del grupo.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`

Grupo BUILTIN predefinido	Privilegios predeterminados
`BUILTIN\Power Users`RID 547 Cuando se crea por primera vez, este grupo no tiene miembros. Los miembros de este grupo tienen las siguientes características: • Puede crear y administrar usuarios y grupos locales. • No se pueden agregar ellos mismos ni ningún otro objeto al `BUILTIN\Administrators` grupo.	`SeChangeNotifyPrivilege`
`BUILTIN\Backup Operators`RID 551 Cuando se crea por primera vez, este grupo no tiene miembros. Los miembros de este grupo pueden anular los permisos de lectura y escritura en archivos o carpetas si se abren con la intención de copia de seguridad.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Users`RID 545 Cuando se crea por primera vez, este grupo no tiene ningún miembro (además del `Authenticated Users` grupo especial implícito). Cuando la SVM se une a un dominio, el `domain\Domain Users` grupo se añade a este grupo. Si la SVM abandona el dominio, `domain\Domain Users` el grupo se eliminará de este grupo.	`SeChangeNotifyPrivilege`
`Everyone`SID S-1-1-0 Este grupo incluye a todos los usuarios, incluidos invitados (pero no usuarios anónimos). Este es un grupo implícito con una membresía implícita.	`SeChangeNotifyPrivilege`

Información relacionada

- Obtenga información sobre los grupos BUILTIN y las cuentas de administrador local en los servidores
- Lista de privilegios compatibles
- Obtenga información sobre cómo configurar la comprobación de recorrido de derivación

Habilite o deshabilite la funcionalidad de grupos y usuarios locales

Obtenga información sobre la funcionalidad de los usuarios y grupos SMB locales de ONTAP

Antes de poder utilizar usuarios y grupos locales para controlar el acceso a los datos del estilo de seguridad NTFS, se debe habilitar la funcionalidad de usuario local y grupo.

Además, si desea utilizar usuarios locales para la autenticación SMB, se debe habilitar la funcionalidad de autenticación de usuarios locales.

La funcionalidad de grupos y usuarios locales y la autenticación de usuarios locales están habilitadas de forma predeterminada. Si no están habilitadas, debe habilitarlas para poder configurar y utilizar usuarios y grupos locales. La funcionalidad de grupos y usuarios locales se puede deshabilitar en cualquier momento.

Además de deshabilitar explícitamente la funcionalidad de grupo y usuario local, ONTAP deshabilita la funcionalidad de grupo y usuario local si algún nodo del clúster se revierte a una versión de ONTAP que no admite la funcionalidad. La funcionalidad de usuario local y de grupo no está habilitada hasta que todos los nodos del clúster ejecuten una versión de ONTAP que la admita.

Información relacionada

- Modifique las cuentas de usuario local
- Modificar grupos locales
- Añada privilegios a usuarios o grupos locales o de dominio

Habilitar o deshabilitar usuarios y grupos locales en servidores SMB de ONTAP

Puede habilitar o deshabilitar usuarios y grupos locales para el acceso SMB en máquinas virtuales de almacenamiento (SVM). La funcionalidad de grupos y usuarios locales está activada de forma predeterminada.

Acerca de esta tarea

Puede usar usuarios y grupos locales al configurar los permisos de archivos NTFS y compartidos de SMB, y puede usar, opcionalmente, usuarios locales para la autenticación al crear una conexión SMB. Para usar usuarios locales para la autenticación, también debe habilitar la opción de autenticación de grupos y usuarios locales.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

Si desea que los grupos y usuarios locales sean…	Introduzca el comando…
Activado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled true`
Deshabilitado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled false`

3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Ejemplo

El siguiente ejemplo habilita la funcionalidad de grupos y usuarios locales en SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

Información relacionada

- Habilitar o deshabilitar la autenticación de usuarios locales en los servidores
- Habilite o deshabilite cuentas de usuario locales

Habilitar o deshabilitar la autenticación de usuarios locales en los servidores SMB de ONTAP

Puede habilitar o deshabilitar la autenticación de usuario local para el acceso SMB en máquinas virtuales de almacenamiento (SVM). El valor predeterminado es permitir la autenticación de usuario local, que resulta útil cuando la SVM no puede ponerse en contacto con un controlador de dominio o si decide no utilizar controles de acceso a nivel de dominio.

Antes de empezar

La funcionalidad de grupos y usuarios locales debe estar habilitada en el servidor CIFS.

Acerca de esta tarea

Es posible habilitar o deshabilitar la autenticación de usuario local en cualquier momento. Si desea usar usuarios locales para la autenticación al crear una conexión SMB, también debe habilitar la opción de grupos y usuarios locales del servidor CIFS.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

Si desea que la autenticación local sea…	Introduzca el comando…
Activado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled true`
Deshabilitado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled false`

3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Ejemplo

El siguiente ejemplo habilita la autenticación de usuario local en SVM vs1:

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

Información relacionada

- Obtenga más información sobre la autenticación de usuarios locales
- Habilitar o deshabilitar usuarios y grupos locales en servidores

Permite gestionar cuentas de usuario local

Modificar cuentas de usuario SMB locales de ONTAP

Puede modificar una cuenta de usuario local si desea cambiar el nombre completo o la descripción de un usuario existente y si desea habilitar o deshabilitar la cuenta de usuario. También puede cambiar el nombre de una cuenta de usuario local si el nombre del usuario está en peligro o si se necesita un cambio de nombre con fines administrativos.

Si desea…	Introduzca el comando…
Modifique el nombre completo del usuario local	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user -name` *`user_name`* `-full-name text` Si el nombre completo contiene un espacio, debe estar entre comillas dobles.
Modifique la descripción del usuario local	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user -name` *`user_name`* `-description text` Si la descripción contiene un espacio, debe estar entre comillas dobles.
Habilite o deshabilite la cuenta de usuario local	`vserver cifs users-and-groups local-user modify -vserver` *vserver_name* -user-name *user_name* -is -account-disabled {true
false}`	Cambie el nombre de la cuenta de usuario local

Ejemplo

En el siguiente ejemplo, se cambia el nombre del usuario local «'CIFS_SERVER\sue'» a «'CIFS_SERVER\sue_new» en la máquina virtual de almacenamiento (SVM, antes conocida como Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

Habilitar o deshabilitar cuentas de usuario SMB de ONTAP locales

Es posible habilitar una cuenta de usuario local si desea que el usuario pueda acceder a los datos contenidos en la máquina virtual de almacenamiento (SVM) a través de una conexión de SMB. También puede deshabilitar una cuenta de usuario local si no desea que ese usuario acceda a los datos de SVM mediante SMB.

Acerca de esta tarea

Para habilitar un usuario local, debe modificar la cuenta de usuario.

Paso

1. Ejecute la acción adecuada:

Si desea…	Introduzca el comando…
Habilite la cuenta de usuario	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account -disabled false`
Desactive la cuenta de usuario	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account -disabled true`

Cambiar las contraseñas de las cuentas de usuario locales de ONTAP SMB

Es posible cambiar la contraseña de la cuenta de un usuario local. Esto puede ser útil si la contraseña del usuario está en peligro o si el usuario ha olvidado la contraseña.

Paso

1. Cambie la contraseña realizando la acción adecuada: `vserver cifs users-and-groups local-user set-password -vserver` *`vserver_name`* `-user-name` *`user_name`*

Ejemplo

En el siguiente ejemplo, se establece la contraseña del usuario local "'CIFS_SERVER\sue'" asociada con la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

Información relacionada

Configurar la complejidad de la contraseña para usuarios locales

Mostrar información sobre la configuración de seguridad del servidor

Mostrar información sobre los usuarios locales de ONTAP SMB

Puede mostrar una lista de todos los usuarios locales en un formulario de resumen. Si desea determinar qué configuración de cuenta está configurada para un usuario específico, puede mostrar información detallada de la cuenta para ese usuario, así como la información de la cuenta para varios usuarios. Esta información puede ayudarle a determinar si necesita modificar la configuración de un usuario y también a resolver problemas de autenticación o acceso a archivos.

Acerca de esta tarea

Nunca se muestra información sobre la contraseña de un usuario.

Paso

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el comando…
Mostrar información sobre todos los usuarios de la máquina virtual de almacenamiento (SVM)	`vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
Muestra información detallada de la cuenta de un usuario	`vserver cifs users-and-groups local-user show -instance -vserver` *`vserver_name`* `-user-name` *`user_name`*

   Hay otros parámetros opcionales que puede elegir cuando ejecuta el comando. Obtenga más información sobre `vserver cifs` en el "Referencia de comandos del ONTAP".

Ejemplo

El siguiente ejemplo muestra información sobre todos los usuarios locales en la SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name     Description
-------- -------------------------- ------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith   Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones
```

Mostrar información sobre las membresías del grupo SMB de ONTAP para usuarios locales

Puede mostrar información sobre los grupos locales a los que pertenece un usuario local. Puede utilizar esta información para determinar qué acceso debe tener el usuario a los archivos y carpetas. Esta información puede ser útil para determinar qué derechos de acceso debe tener el usuario a los archivos y carpetas o al solucionar problemas de acceso a archivos.

Acerca de esta tarea

Puede personalizar el comando para que muestre solo la información que desea ver.

Paso

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el comando…
Muestra información de pertenencia de usuario local para un usuario local específico	`vserver cifs users-and-groups local-user show-membership -user-name` *user_name*
Mostrar información de pertenencia al usuario local para el grupo local del que forma parte este usuario local	`vserver cifs users-and-groups local-user show-membership -membership` *group_name*
Mostrar información de pertenencia al usuario para los usuarios locales que están asociados a una máquina virtual de almacenamiento (SVM) especificada	`vserver cifs users-and-groups local-user show-membership -vserver` *vserver_name*
Mostrar información detallada para todos los usuarios locales en una SVM especificada	`vserver cifs users-and-groups local-user show-membership -instance -vserver` *vserver_name*

Ejemplo

En el siguiente ejemplo se muestra la información de pertenencia de todos los usuarios locales de SVM vs1; el usuario «'CIFS_SERVER\Administrator'» es miembro del grupo «'BUILTIN\Administrators'» y «'CIFS_SERVER\sue'» es miembro del grupo «'CIFS_SERVER\g1'»:

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                     Membership
---------- ----------------------------- ----------------------
vs1        CIFS_SERVER\Administrator     BUILTIN\Administrators
           CIFS_SERVER\sue               CIFS_SERVER\g1
```

Eliminar cuentas de usuario SMB de ONTAP locales

Es posible eliminar cuentas de usuario locales de la máquina virtual de almacenamiento (SVM) si ya no son necesarias para la autenticación local de SMB en el servidor CIFS o para determinar los derechos de acceso a los datos incluidos en la SVM.

Acerca de esta tarea

Tenga en cuenta lo siguiente al eliminar usuarios locales:

- El sistema de archivos no se ha modificado.

  Los descriptores de seguridad de Windows de los archivos y directorios que hacen referencia a este usuario no están ajustados.

- Todas las referencias a los usuarios locales se eliminan de las bases de datos de pertenencia y privilegios.
- No se pueden eliminar los usuarios estándar conocidos, como el Administrador.

Pasos

1. Determine el nombre de la cuenta de usuario local que desea eliminar: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
2. Elimine el usuario local: `vserver cifs users-and-groups local-user delete -vserver` *`vserver_name`* `-user-name` *`username_name`*
3. Compruebe que se ha eliminado la cuenta de usuario: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Ejemplo

En el siguiente ejemplo se elimina el usuario local "'CIFS_SERVER\sue'" asociado con SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                    Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
```

Administrar grupos locales

Modificar grupos SMB locales de ONTAP

Puede modificar los grupos locales existentes cambiando la descripción de un grupo local existente o cambiando el nombre del grupo.

Si desea…	Usar el comando…
Modifique la descripción del grupo local	`vserver cifs users-and-groups local-group modify -vserver` *`vserver_name`* `-group-name` *`group_name`* `-description text` Si la descripción contiene un espacio, debe estar entre comillas dobles.
Cambie el nombre del grupo local	`vserver cifs users-and-groups local-group rename -vserver` *`vserver_name`* `-group-name` *`group_name`* `-new-group-name` *`new_group_name`*

Ejemplos

En el ejemplo siguiente se cambia el nombre del grupo local "'CIFS_SERVER\engineering'" a "'CIFS_SERVER\engineering_new'":

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

En el siguiente ejemplo se modifica la descripción del grupo local "'CIFS_SERVER\engineering'":

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

Mostrar información sobre los grupos locales de SMB de ONTAP

Es posible mostrar una lista de todos los grupos locales configurados en el clúster o en una máquina virtual de almacenamiento (SVM) específica. Esta información puede ser útil para solucionar problemas de acceso a los archivos en la SVM o problemas de derechos de usuario (privilegios) en la SVM.

Paso

1. Ejecute una de las siguientes acciones:

Si desea información acerca de…	Introduzca el comando…
Todos los grupos locales del clúster	`vserver cifs users-and-groups local-group show`
Todos los grupos locales en la SVM	`vserver cifs users-and-groups local-group show -vserver` *`vserver_name`*

Hay otros parámetros opcionales que puede elegir cuando ejecuta este comando. Obtenga más información sobre `vserver cifs` en el "Referencia de comandos del ONTAP".

Ejemplo

En el siguiente ejemplo, se muestra información sobre todos los grupos locales en la SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                  Description
-------- --------------------------- ----------------------------
vs1      BUILTIN\Administrators      Built-in Administrators group
vs1      BUILTIN\Backup Operators    Backup Operators group
vs1      BUILTIN\Power Users         Restricted administrative privileges
vs1      BUILTIN\Users               All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

Gestionar la pertenencia a un grupo SMB de ONTAP local

Puede administrar la pertenencia a grupos locales agregando y eliminando usuarios locales o de dominio, o agregando y eliminando grupos de dominios. Esto resulta útil si desea controlar el acceso a los datos basándose en los controles de acceso colocados en el grupo o si desea que los usuarios tengan privilegios asociados a ese grupo.

Acerca de esta tarea

Directrices para agregar miembros a un grupo local:

- No puede agregar usuarios al grupo especial *Everyone*.
- El grupo local debe existir antes de poder añadir un usuario.
- El usuario debe existir antes de poder agregar el usuario a un grupo local.
- No puede agregar un grupo local a otro grupo local.
- Para agregar un usuario o grupo de dominio a un grupo local, Data ONTAP debe poder resolver el nombre a un SID.

Directrices para eliminar miembros de un grupo local:

- No puede eliminar miembros del grupo especial *Everyone*.
- El grupo del que desea quitar un miembro debe existir.
- ONTAP debe poder resolver los nombres de los miembros que desea quitar del grupo a un SID correspondiente.

Paso

1. Agregar o quitar un miembro de un grupo.

Si desea…	A continuación, se usa el comando…
Agregar un miembro a un grupo	`vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` Puede especificar una lista delimitada por comas de usuarios locales, usuarios de dominio o grupos de dominios para agregarlos al grupo local especificado.
Quitar un miembro de un grupo	`vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` Puede especificar una lista delimitada por comas de usuarios locales, usuarios de dominio o grupos de dominios para eliminarlos del grupo local especificado.

En el siguiente ejemplo, se agrega un usuario local "MB_SERVER\sue" y un grupo de dominios "'AD_DOM\dom_eng'" al grupo local "MB_SERVER\engineering" en SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

En el siguiente ejemplo se eliminan los usuarios locales «MB_SERVER\sue» y «MB_SERVER\james» del

grupo local «MB_SERVER\engineering» de SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Información relacionada

Muestra información acerca de los miembros de los grupos locales

Mostrar información de ONTAP SMB sobre los miembros de los grupos locales

Es posible mostrar una lista de todos los miembros de grupos locales configurados en el clúster o en una máquina virtual de almacenamiento (SVM) especificada. Esta información puede ser útil para solucionar problemas de acceso a archivos o problemas de derechos de usuario (privilegios).

Paso

1. Ejecute una de las siguientes acciones:

Si desea mostrar información acerca de…	Introduzca el comando…
Miembros de todos los grupos locales del cluster	`vserver cifs users-and-groups local-group show-members`
Miembros de todos los grupos locales en la SVM	`vserver cifs users-and-groups local-group show-members -vserver` *`vserver_name`*

Ejemplo

En el siguiente ejemplo, se muestra información acerca de los miembros de todos los grupos locales en la SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                    Members
--------- ----------------------------- ------------------------
vs1       BUILTIN\Administrators        CIFS_SERVER\Administrator
                                        AD_DOMAIN\Domain Admins
                                        AD_DOMAIN\dom_grp1
          BUILTIN\Users                 AD_DOMAIN\Domain Users
                                        AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering       CIFS_SERVER\james
```

Eliminar grupos SMB locales de ONTAP

Es posible eliminar un grupo local de la máquina virtual de almacenamiento (SVM) si ya no es necesario para determinar los derechos de acceso a los datos asociados con esa SVM o si ya no es necesario para asignar los derechos de usuario (privilegios) de SVM a los miembros del grupo.

Acerca de esta tarea

Tenga en cuenta lo siguiente al eliminar grupos locales:

- El sistema de archivos no se ha modificado.

  Los descriptores de seguridad de Windows de los archivos y directorios que hacen referencia a este grupo no se ajustan.

- Si el grupo no existe, se devuelve un error.
- El grupo especial *Everyone* no se puede eliminar.
- Los grupos integrados como *BUILTIN\Administrators BUILTIN\Users* no se pueden eliminar.

Pasos

1. Determine el nombre del grupo local que desea eliminar. Para ello, muestre la lista de grupos locales en la SVM: `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. Elimine el grupo local: `vserver cifs users-and-groups local-group delete -vserver` *`vserver_name`* `-group-name` *`group_name`*
3. Compruebe que el grupo se ha suprimido: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Ejemplo

En el siguiente ejemplo se elimina el grupo local "'CIFS_SERVER\sales'" asociado con SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
```

Actualizar los nombres de usuarios y grupos del dominio SMB de ONTAP en las bases de datos locales

Puede agregar usuarios y grupos de dominio a los grupos locales de un servidor CIFS. Estos objetos de dominio se registran en bases de datos locales en el clúster. Si se cambia el nombre de un objeto de dominio, las bases de datos locales deben actualizarse manualmente.

Acerca de esta tarea

Debe especificar el nombre de la máquina virtual de almacenamiento (SVM) en la que desea actualizar los nombres de dominio.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Ejecute la acción adecuada:

Si desea actualizar usuarios y grupos de dominio y…	Se usa este comando…
Muestra usuarios y grupos de dominio que se han actualizado correctamente y que no se han podido actualizar	`vserver cifs users-and-groups update-names -vserver` *vserver_name*

Si desea actualizar usuarios y grupos de dominio y…	Se usa este comando…
Muestra los usuarios y grupos de dominio que se han actualizado correctamente	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false`
Muestra sólo los usuarios y grupos de dominio que no se pueden actualizar	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true`
Suprimir toda la información de estado acerca de las actualizaciones	`vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true`

3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Ejemplo

En el siguiente ejemplo se actualizan los nombres de los usuarios y grupos de dominio asociados con la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1. Para la última actualización, hay una cadena de nombres dependiente que se debe actualizar:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin
```

Gestione los privilegios locales

Agregar privilegios a usuarios o grupos locales o de dominio de ONTAP SMB

Puede administrar los derechos de usuario para usuarios o grupos locales o de dominio mediante la adición de privilegios. Los privilegios agregados anulan los privilegios predeterminados asignados a cualquiera de estos objetos. Esto proporciona una seguridad mejorada al permitirle personalizar qué privilegios tiene un usuario o grupo.

Antes de empezar

Debe haber ya el usuario o grupo local o de dominio al que se añadirán privilegios.

Acerca de esta tarea

Al agregar un privilegio a un objeto se reemplazan los privilegios predeterminados para ese usuario o grupo. Al añadir un privilegio, no se quitan los privilegios añadidos anteriormente.

Debe tener en cuenta lo siguiente al agregar privilegios a usuarios o grupos locales o de dominio:

- Puede añadir uno o varios privilegios.
- Al agregar privilegios a un usuario o grupo de dominio, ONTAP puede validar el usuario o grupo de dominio poniéndose en contacto con el controlador de dominio.

  Es posible que se produzca un error en el comando si ONTAP no puede comunicarse con la controladora de dominio.

Pasos

1. Añada una o más Privileges a un usuario o grupo local o de dominio: `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. Compruebe que se aplican los Privileges deseados al objeto: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Ejemplo

En el siguiente ejemplo, se añaden los privilegios «ShebPrivilege» y «SeeTakeOwnershipPrivilege» al usuario «'CIFS_SERVER\sue» en la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege
```

Eliminar privilegios de usuarios o grupos locales o de dominio de ONTAP SMB

Puede administrar derechos de usuario para usuarios o grupos locales o de dominio eliminando privilegios. Esto proporciona una seguridad mejorada al permitirle

personalizar los privilegios máximos que tienen los usuarios y los grupos.

Antes de empezar

Debe haber ya el usuario o grupo local o de dominio del que se eliminarán los privilegios.

Acerca de esta tarea

Al quitar privilegios de usuarios o grupos locales o de dominio, debe tener en cuenta lo siguiente:

- Puede eliminar uno o varios privilegios.
- Al eliminar privilegios de un usuario o grupo de dominio, ONTAP puede validar el usuario o grupo de dominio poniéndose en contacto con el controlador de dominio.

  Es posible que se produzca un error en el comando si ONTAP no puede comunicarse con la controladora de dominio.

Pasos

1. Quite una o más Privileges de un usuario o grupo local o de dominio: `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. Verifique que el Privileges deseado se haya eliminado del objeto: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Ejemplo

En el siguiente ejemplo se eliminan los privilegios «DeeTcbPrivilege» y «SeeTakeOwnershipPrivilege» del usuario «'CIFS_SERVER\sue» en la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ------------------
vs1       CIFS_SERVER\sue      -
```

Restablecer privilegios para usuarios y grupos locales o de dominio de ONTAP SMB

Es posible restablecer privilegios para los grupos y usuarios locales o de dominio. Esto puede ser útil si ha realizado modificaciones a los privilegios de un usuario o grupo local o de dominio y esas modificaciones ya no se desean ni se necesitan.

Acerca de esta tarea

Al restablecer los privilegios de un usuario o grupo local o de dominio, se quitan todas las entradas de privilegios de ese objeto.

Pasos

1. Restablezca la Privileges en un usuario o grupo local o de dominio: `vserver cifs users-and-groups privilege reset-privilege -vserver vserver_name -user-or-group-name name`
2. Compruebe que los Privileges se han restablecido en el objeto: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Ejemplos

En el siguiente ejemplo, se restablecen los privilegios para el usuario «'CIFS_SERVER\sue'» en la máquina virtual de almacenamiento (SVM, anteriormente conocida como Vserver) vs1. De forma predeterminada, los usuarios normales no tienen privilegios asociados a sus cuentas:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

En el ejemplo siguiente se restablecen los privilegios para el grupo "'BUILTIN\Administrators'", eliminando de forma efectiva la entrada de privilegios:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ------------------------ --------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Mostrar información sobre las anulaciones de privilegios SMB de ONTAP

Puede mostrar información acerca de los privilegios personalizados asignados a cuentas o grupos de usuarios locales o de dominio. Esta información le ayuda a determinar si se aplican los derechos de usuario deseados.

Paso

1. Ejecute una de las siguientes acciones:

Si desea mostrar información acerca de…	Introduzca este comando…
Privilegios personalizados para todos los grupos y usuarios locales y de dominio en la máquina virtual de almacenamiento (SVM)	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`*
Privilegios personalizados para un dominio o un grupo y usuario local específicos de la SVM	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Hay otros parámetros opcionales que puede elegir cuando ejecuta este comando. Obtenga más información sobre `vserver cifs users-and-groups privilege show` en el "Referencia de comandos del ONTAP".

Ejemplo

El siguiente comando muestra todos los privilegios asociados explícitamente con los usuarios y grupos locales o de dominio para SVM vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
---------- ---------------------  ---------------
vs1        BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                   SeRestorePrivilege
vs1        CIFS_SERVER\sue         SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

Configurar la comprobación de recorrido de derivación

Obtenga información sobre cómo configurar la comprobación de travesía de derivación de SMB de ONTAP

La comprobación de recorrido de omisión es un derecho de usuario (también conocido como *Privilege*) que determina si un usuario puede recorrer todos los directorios de la ruta de acceso a un archivo incluso si el usuario no tiene permisos en el directorio de recorrido. Debe comprender lo que sucede al permitir o dejar de permitir la comprobación de recorrido por omisión, y cómo configurar la comprobación de recorrido por omisión para los usuarios en máquinas virtuales de almacenamiento (SVM).

Qué sucede cuando se permite o se despermite la comprobación de recorrido de derivación

- Si se permite, cuando un usuario intenta acceder a un archivo, ONTAP no comprueba el permiso Traverse para los directorios intermedios al determinar si se concede o deniega el acceso al archivo.
- Si no se permite, ONTAP comprueba el permiso recorrer (ejecutar) para todos los directorios de la ruta de acceso al archivo.

  Si alguno de los directorios intermedios no tiene el "'X'" (permiso de desplazamiento), ONTAP niega el acceso al archivo.

Configurar la comprobación de recorrido de derivación

Puede configurar la comprobación de recorrido de desvío mediante la interfaz de línea de comandos de ONTAP o mediante la configuración de directivas de grupo de Active Directory con este derecho de usuario.

```
`SeChangeNotifyPrivilege`El privilegio controla si los usuarios pueden
omitir la comprobación transversal.
```

- Si se la agrega a los usuarios o grupos SMB locales en la SVM o a usuarios o grupos de dominio, permite omitir el control transversal.
- Si lo elimina de usuarios o grupos SMB locales en la SVM o de usuarios o grupos de dominio, no permite omitir la comprobación cruzada.

De forma predeterminada, los siguientes grupos BUILTIN de la SVM tienen derecho a omitir la comprobación de recorrido:

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`
- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

Si no desea permitir a los miembros de uno de estos grupos omitir la comprobación de recorrido, debe quitar este privilegio del grupo.

Debe tener en cuenta lo siguiente al configurar la comprobación de derivación cruzada de usuarios y grupos de SMB locales en la SVM mediante la CLI:

- Si desea permitir que los miembros de un grupo local o de dominio personalizado omitan la comprobación transversal, debe agregar el `SeChangeNotifyPrivilege` privilegio a ese grupo.
- Si desea permitir que un usuario local o de dominio individual omita la comprobación transversal y que ese usuario no sea miembro de un grupo con ese privilegio, puede agregar el `SeChangeNotifyPrivilege` privilegio a esa cuenta de usuario.
- Puede desactivar la comprobación transversal de omisión para usuarios o grupos locales o de dominio eliminando el `SeChangeNotifyPrivilege` privilegio en cualquier momento.

Para desactivar la comprobación de bypass travers para usuarios o grupos locales o de dominio especificados, también debe eliminar el `SeChangeNotifyPrivilege` privilegio del `Everyone` grupo.

Información relacionada

- Permitir a los usuarios o grupos omitir la comprobación de recorrido del directorio
- No permitir a los usuarios o grupos omitir la comprobación de recorrido del directorio
- Configurar la asignación de caracteres para la traducción de nombres de archivos en volúmenes
- Crear listas de control de acceso a recursos compartidos
- Acceso seguro a archivos mediante Storage-Level Access Guard
- Lista de privilegios compatibles
- Añada privilegios a usuarios o grupos locales o de dominio

Permitir que los usuarios o grupos omitan la verificación del recorrido del directorio SMB de ONTAP

Si desea que un usuario pueda recorrer todos los directorios de la ruta a un archivo, aunque el usuario no tenga permisos en un directorio cruzado, puede añadir el `SeChangeNotifyPrivilege` privilegio a grupos o usuarios locales de SMB en máquinas virtuales de almacenamiento (SVM). De forma predeterminada, los usuarios pueden omitir la comprobación de recorrido del directorio.

Antes de empezar

- Debe haber un servidor SMB en la SVM.
- Debe habilitarse la opción del servidor SMB para los usuarios locales y los grupos.
- El usuario o grupo local o de dominio al que se `SeChangeNotifyPrivilege` agregará el privilegio debe existir ya.

Acerca de esta tarea

Al agregar privilegios a un usuario o grupo de dominio, ONTAP puede validar el usuario o grupo de dominio poniéndose en contacto con el controlador de dominio. Es posible que se produzca un error en el comando si ONTAP no puede comunicarse con la controladora de dominio.

Pasos

1. Active la comprobación de desvío mediante la adición `SeChangeNotifyPrivilege` del privilegio a un usuario o grupo local o de dominio: `vserver cifs users-and-groups privilege add-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`* `-privileges SeChangeNotifyPrivilege`

   El valor del `-user-or-group-name` parámetro es un usuario o un grupo local, o un usuario o un grupo de dominio.

2. Compruebe que el usuario o grupo especificado tiene activada la comprobación de desvío de desvío: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Ejemplo

El siguiente comando permite a los usuarios que pertenecen al grupo «`EJEMPLO\eng`» omitir la comprobación

de desplazamiento de directorios agregando el `SeChangeNotifyPrivilege` privilegio al grupo:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       EXAMPLE\eng          SeChangeNotifyPrivilege
```

Información relacionada

No permitir a los usuarios o grupos omitir la comprobación de recorrido del directorio

No permitir que usuarios o grupos omitan la comprobación del recorrido del directorio SMB de ONTAP

Si no desea que un usuario recorra todos los directorios de la ruta a un archivo porque el usuario no tiene permisos en el directorio cruzado, puede quitar el `SeChangeNotifyPrivilege` privilegio de los usuarios o grupos locales de SMB en las máquinas virtuales de almacenamiento (SVM).

Antes de empezar

Debe haber ya el usuario o grupo local o de dominio del que se eliminarán los privilegios.

Acerca de esta tarea

Al eliminar privilegios de un usuario o grupo de dominio, ONTAP puede validar el usuario o grupo de dominio poniéndose en contacto con el controlador de dominio. Es posible que se produzca un error en el comando si ONTAP no puede comunicarse con la controladora de dominio.

Pasos

1. No permitir la comprobación de desvío: `vserver cifs users-and-groups privilege remove-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`* `-privileges SeChangeNotifyPrivilege`

   El comando quita `SeChangeNotifyPrivilege` el privilegio del usuario o grupo local o de dominio que se especifique con el valor del `-user-or-group-name` *`name`* parámetro.

2. Compruebe que el usuario o grupo especificado tiene desactivada la comprobación de desvío: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Ejemplo

El siguiente comando evita que los usuarios que pertenecen al grupo "'EXAMPLE\eng'" pasen por alto la comprobación de recorrido del directorio:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ----------------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ----------------------
vs1       EXAMPLE\eng           -
```

Información relacionada

Permitir a los usuarios o grupos omitir la comprobación de recorrido del directorio

Muestra información acerca de las políticas de auditoría y seguridad de archivos

Obtenga información sobre cómo visualizar las políticas de seguridad y auditoría de archivos SMB de ONTAP

Puede mostrar información sobre la seguridad de los archivos y directorios contenidos en volúmenes en máquinas virtuales de almacenamiento (SVM). Puede mostrar información sobre las políticas de auditoría en los volúmenes de FlexVol. Si se configura, se puede mostrar información acerca de las opciones de seguridad Protección del acceso a nivel de almacenamiento y Control de acceso dinámico en volúmenes de FlexVol.

Mostrar información acerca de la seguridad de archivos

Puede visualizar la información sobre la seguridad de los archivos aplicada a los datos contenidos en volúmenes y qtrees (para volúmenes FlexVol) con los siguientes estilos de seguridad:

- NTFS
- UNIX
- Mixto

Visualización de información acerca de las directivas de auditoría

Puede mostrar información sobre las políticas de auditoría para auditar eventos de acceso en los volúmenes FlexVol mediante los siguientes protocolos NAS:

- SMB (todas las versiones)
- NFSv4.x

Mostrar información acerca de la seguridad de la protección de acceso a nivel de almacenamiento (SLAG)

La seguridad de protección de acceso a nivel de almacenamiento se puede aplicar en volúmenes de FlexVol y objetos de qtree con los siguientes estilos de seguridad:

- NTFS
- Mixto
- UNIX (si se configura un servidor CIFS en la SVM que contiene el volumen)

Mostrar información acerca de la seguridad del control de acceso dinámico (DAC)

La seguridad de control de acceso dinámico se puede aplicar a un objeto dentro de un volumen FlexVol con los siguientes estilos de seguridad:

- NTFS
- Mixto (si el objeto tiene seguridad efectiva NTFS)

Información relacionada

- Obtenga información sobre el acceso seguro a archivos mediante Storage-Level Access Guard
- Mostrar información sobre la protección de acceso a nivel de almacenamiento en los servidores

Mostrar información sobre la seguridad de archivos SMB de ONTAP en volúmenes de estilo de seguridad NTFS

Puede mostrar información acerca de la seguridad de archivos y directorios en volúmenes de estilo de seguridad NTFS, incluidos el estilo de seguridad y los estilos de seguridad efectivos, los permisos que se aplican e información acerca de los atributos dos. Puede utilizar los resultados para validar la configuración de seguridad o solucionar problemas de acceso a archivos.

Acerca de esta tarea

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los datos cuya información de seguridad de archivo o carpeta desee mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

- Debido a que los volúmenes y qtrees de estilo de seguridad NTFS utilizan sólo permisos de archivo NTFS y usuarios y grupos de Windows al determinar los derechos de acceso a archivos, los campos de salida relacionados con UNIX contienen información de permisos de archivo UNIX de sólo visualización.
- Se muestra la salida de ACL para archivos y carpetas con seguridad NTFS.
- Como la seguridad de Access Guard a nivel de almacenamiento se puede configurar en el volumen raíz o en el qtree, la salida de un volumen o una ruta de qtree en la que se configure la protección de acceso a nivel de almacenamiento puede mostrar tanto ACL de archivos normales como ACL de Storage-Level Access Guard.
- El resultado también muestra información acerca de los ACE de control de acceso dinámico si el Control de acceso dinámico está configurado para la ruta de acceso de archivo o directorio indicada.

Paso

1. Mostrar la configuración de seguridad de archivos y directorios con el nivel de detalle deseado:

Si desea mostrar información…	Introduzca el siguiente comando…
En forma de resumen	`vserver security file-directory show -vserver vserver_name -path path`
Con detalle ampliado	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Ejemplos

En el ejemplo siguiente se muestra información de seguridad sobre la ruta de `/vol4` SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                Vserver: vs1
                              File Path: /vol4
                      File Inode Number: 64
                         Security Style: ntfs
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                          Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                          ALLOW-Everyone-0x1f01ff
                                          ALLOW-Everyone-0x10000000-
OI|CI|IO
```

En el siguiente ejemplo, se muestra la información de seguridad con máscaras expandidas sobre la ruta de `/data/engineering` SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

               Vserver: vs1
             File Path: /data/engineering
     File Inode Number: 5544
```

```
          Security Style: ntfs
         Effective Style: ntfs
          DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
                             ...0 .... .... .... .... .... .... .... =
```

```
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
```

```
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
                              .... .... .... ..0. .... .... .... .... =
Read Control
                              .... .... .... ...0 .... .... .... .... =
Delete
                              .... .... .... .... .... ...0 .... .... =
Write Attributes
                              .... .... .... .... .... .... 0... .... =
Read Attributes
                              .... .... .... .... .... .... .0.. .... =
Delete Child
                              .... .... .... .... .... .... ..0. .... =
Execute
                              .... .... .... .... .... .... ...0 .... =
Write EA
                              .... .... .... .... .... .... .... 0... =
Read EA
                              .... .... .... .... .... .... .... .0.. =
Append
                              .... .... .... .... .... .... .... ..0. =
Write
                              .... .... .... .... .... .... .... ...0 =
Read
```

En el siguiente ejemplo, se muestra información de seguridad, incluida la información de seguridad de Storage-Level Access Guard, del volumen con la ruta `/datavol1` en SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Información relacionada

- Muestra información sobre la seguridad de archivos en volúmenes mixtos de estilo de seguridad
- Muestra información sobre la seguridad de archivos en volúmenes de estilo de seguridad UNIX

Mostrar información sobre la seguridad de los archivos SMB de ONTAP en volúmenes de estilo de seguridad mixto

Puede mostrar información acerca de la seguridad de archivos y directorios en volúmenes mixtos de estilo de seguridad, incluidos el estilo de seguridad y los estilos de seguridad efectivos, los permisos que se aplican y la información acerca de los propietarios y grupos de UNIX. Puede utilizar los resultados para validar la configuración de seguridad o solucionar problemas de acceso a archivos.

Acerca de esta tarea

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los datos cuya información de seguridad de archivo o carpeta desee mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

- Los volúmenes y qtrees de estilo de seguridad mixtos pueden contener archivos y carpetas que utilizan permisos de archivo de UNIX, bits de modo o ACL de NFSv4 y algunos archivos y directorios que utilizan permisos de archivo NTFS.
- El nivel superior de un volumen mixto de estilo de seguridad puede tener una seguridad efectiva de UNIX o NTFS.
- La salida de ACL se muestra solo para archivos y carpetas con seguridad NTFS o NFSv4.

  Este campo está vacío para archivos y directorios que utilizan la seguridad de UNIX que solo tienen aplicados permisos de bit de modo (sin ACL de NFSv4).

- Los campos de salida de propietario y grupo de la salida ACL se aplican sólo en el caso de los descriptores de seguridad NTFS.
- Debido a que la seguridad de Access Guard a nivel de almacenamiento se puede configurar en un volumen o qtree de estilo de seguridad mixto incluso si el estilo de seguridad efectivo del volumen raíz o qtree es UNIX, La salida de un volumen o una ruta de qtree en la que se configure Storage-Level Access Guard podría mostrar tanto los permisos de archivos UNIX como las ACL de Storage-Level Access Guard.
- Si la ruta de acceso introducida en el comando es a datos con seguridad efectiva de NTFS, el resultado también muestra información acerca de ACE de Control de acceso dinámico si Control de acceso dinámico está configurado para el archivo o la ruta de acceso de directorio dada.

Paso

1. Mostrar la configuración de seguridad de archivos y directorios con el nivel de detalle deseado:

Si desea mostrar información…	Introduzca el siguiente comando…
En forma de resumen	`vserver security file-directory show -vserver vserver_name -path path`
Con detalle ampliado	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Ejemplos

El siguiente ejemplo muestra la información de seguridad sobre la ruta de `/projects` SVM VS1 en formato de máscara expandida. Esta ruta mixta de estilo de seguridad tiene una seguridad efectiva de UNIX.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

               Vserver: vs1
             File Path: /projects
      File Inode Number: 78
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
          Unix User Id: 0
         Unix Group Id: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

En el ejemplo siguiente se muestra información de seguridad sobre la ruta de `/data` SVM VS1. Esta ruta mixta de estilo de seguridad tiene una seguridad NTFS efectiva.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

                                Vserver: vs1
                              File Path: /data
                      File Inode Number: 544
                         Security Style: mixed
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                            ALLOW-Everyone-0x1f01ff
                                            ALLOW-Everyone-0x10000000-
OI|CI|IO
```

En el ejemplo siguiente se muestra información de seguridad sobre el volumen en la ruta de `/datavol5` SVM VS1. El nivel superior de este volumen mixto de estilo de seguridad ofrece una seguridad efectiva para UNIX. El volumen tiene seguridad de protección de acceso en el nivel de almacenamiento.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
```

Información relacionada

- Muestra información sobre la seguridad de archivos en volúmenes de estilo de seguridad NTFS
- Muestra información sobre la seguridad de archivos en volúmenes de estilo de seguridad UNIX

Mostrar información sobre la seguridad de archivos SMB de ONTAP en volúmenes de estilo de seguridad UNIX

Puede mostrar información acerca de la seguridad de archivos y directorios en los volúmenes de estilo de seguridad de UNIX, incluidos los estilos de seguridad y los estilos de seguridad efectivos, los permisos que se aplican y la información acerca de los

propietarios y grupos de UNIX. Puede utilizar los resultados para validar la configuración de seguridad o solucionar problemas de acceso a archivos.

Acerca de esta tarea

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los datos cuyo archivo o información de seguridad de directorio desee mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

- Los volúmenes y qtrees de estilo de seguridad de UNIX solo utilizan permisos de archivos UNIX, ya sea bits de modo o ACL de NFSv4 al determinar los derechos de acceso a los archivos.
- La salida de ACL se muestra solo para los archivos y las carpetas con seguridad de NFSv4.

  Este campo está vacío para archivos y directorios que utilizan la seguridad de UNIX que solo tienen aplicados permisos de bit de modo (sin ACL de NFSv4).

- Los campos de salida de propietario y grupo de la salida de ACL no se aplican en el caso de los descriptores de seguridad de NFSv4.

  Sólo son significativos para los descriptores de seguridad NTFS.

- Como la seguridad de Access Guard en el nivel de almacenamiento se admite en un volumen UNIX o qtree si hay un servidor CIFS configurado en la SVM, el resultado puede contener información sobre la seguridad de Access Guard en el nivel de almacenamiento aplicada al volumen o qtree especificados en el `-path` parámetro.

Paso

1. Mostrar la configuración de seguridad de archivos y directorios con el nivel de detalle deseado:

Si desea mostrar información…	Introduzca el siguiente comando…
En forma de resumen	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Con detalle ampliado	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Ejemplos

En el ejemplo siguiente se muestra información de seguridad sobre la ruta de `/home` SVM VS1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

El siguiente ejemplo muestra la información de seguridad sobre la ruta de `/home` SVM VS1 en formato de máscara expandida:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: 0x10
                    ...0 .... .... .... = Offline
                    .... ..0. .... .... = Sparse
                    .... .... 0... .... = Normal
                    .... .... ..0. .... = Archive
                    .... .... ...1 .... = Directory
                    .... .... .... .0.. = System
                    .... .... .... ..0. = Hidden
                    .... .... .... ...0 = Read Only
                          Unix User Id: 0
                         Unix Group Id: 1
                        Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

Información relacionada

- Mostrar información sobre la seguridad de los archivos en volúmenes de estilo de seguridad
- Muestra información sobre la seguridad de archivos en volúmenes mixtos de estilo de seguridad

Comandos de ONTAP para mostrar información sobre las políticas de auditoría de NTFS en volúmenes SMB FlexVol

Puede mostrar información acerca de las directivas de auditoría NTFS en los volúmenes FlexVol, incluidos los estilos de seguridad y los estilos de seguridad efectivos, los permisos que se aplican e información acerca de las listas de control de acceso al sistema. Puede utilizar los resultados para validar la configuración de seguridad o para solucionar problemas de auditoría.

Acerca de esta tarea

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los archivos o carpetas cuya información de auditoría desee mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

- Los volúmenes y qtrees de estilo de seguridad NTFS sólo utilizan listas de control de acceso al sistema (SACL) NTFS para las directivas de auditoría.
- Los archivos y carpetas de un volumen mixto de estilo de seguridad con seguridad efectiva NTFS pueden tener directivas de auditoría NTFS aplicadas.

  Los volúmenes y qtrees de estilo de seguridad mixtos pueden contener archivos y directorios que utilizan permisos de archivo de UNIX, bits de modo o ACL de NFSv4 y algunos archivos y directorios que utilizan permisos de archivo NTFS.

- El nivel superior de un volumen de estilo de seguridad mixto puede tener seguridad efectiva de UNIX o NTFS y puede que no contenga SACL NTFS.
- Debido a que la seguridad de Access Guard a nivel de almacenamiento se puede configurar en un volumen o qtree de estilo de seguridad mixto incluso si el estilo de seguridad efectivo del volumen raíz o qtree es UNIX, El resultado de una ruta de volumen o qtree en la que se configuró Storage-Level Access Guard puede mostrar tanto el archivo normal como la carpeta NFSv4 SACL y Storage-Level Access Guard NTFS SACL.
- Si la ruta de acceso que se introduce en el comando es para los datos con seguridad efectiva NTFS, la salida también muestra información sobre los ACE de control dinámico de acceso si el Control dinámico de acceso está configurado para la ruta de acceso del archivo o directorio dada.
- Cuando se muestra información de seguridad sobre archivos y carpetas con seguridad efectiva NTFS, los campos de salida relacionados con UNIX contienen información de permisos de archivo UNIX de sólo visualización.

  Los archivos y carpetas de estilo de seguridad NTFS utilizan sólo permisos de archivo NTFS y usuarios y grupos de Windows al determinar los derechos de acceso a archivos.

- El resultado de ACL se muestra solo para los archivos y las carpetas con seguridad NTFS o NFSv4.

  Este campo está vacío para archivos y carpetas que utilizan la seguridad de UNIX que solo tienen aplicados permisos de bit de modo (sin ACL de NFSv4).

- Los campos de salida de propietario y grupo de la salida ACL se aplican sólo en el caso de los descriptores de seguridad NTFS.

Paso

1. Mostrar la configuración de la directiva de auditoría de archivos y directorios con el nivel de detalle deseado:

Si desea mostrar información…	Introduzca el siguiente comando…
En forma de resumen	`vserver security file-directory show -vserver vserver_name -path path`
Como una lista detallada	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Ejemplos

En el siguiente ejemplo, se muestra información de política de auditoría para la ruta `/corp` en SVM VS1. La ruta de acceso tiene seguridad efectiva NTFS. El descriptor de seguridad NTFS contiene UNA entrada SACL CORRECTA y UNA entrada SACL SUCCESS/FAIL.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

En el siguiente ejemplo, se muestra información de política de auditoría para la ruta `/datavol1` en SVM VS1. La ruta de acceso contiene tanto SACL de archivo normal como de carpeta y SACL de Storage-Level Access

Guard.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Comandos de ONTAP para mostrar información sobre las políticas de auditoría de NFSv4 en volúmenes SMB FlexVol

Puede mostrar información sobre las políticas de auditoría de NFSv4 en volúmenes de

FlexVol mediante la interfaz de línea de comandos de ONTAP, incluidos los estilos de seguridad y los estilos de seguridad efectivos, qué permisos se aplican e información sobre las listas de control de acceso del sistema (SACL). Puede utilizar los resultados para validar la configuración de seguridad o para solucionar problemas de auditoría.

Acerca de esta tarea

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los archivos o directorios cuya información de auditoría desea mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

- Los volúmenes y qtrees de estilo de seguridad de UNIX solo utilizan NFSv4 SACL para las políticas de auditoría.
- Los archivos y directorios de un volumen de estilo de seguridad mixto que sea de estilo de seguridad UNIX pueden hacer que se les apliquen las políticas de auditoría de NFSv4.

  Los volúmenes y qtrees de estilo de seguridad mixtos pueden contener archivos y directorios que utilizan permisos de archivo de UNIX, bits de modo o ACL de NFSv4 y algunos archivos y directorios que utilizan permisos de archivo NTFS.

- El nivel superior de un volumen con estilo de seguridad mixto puede tener seguridad efectiva de UNIX o NTFS y puede que contenga o no SACL de NFSv4.
- La salida de ACL se muestra solo para archivos y carpetas con seguridad NTFS o NFSv4.

  Este campo está vacío para archivos y carpetas que utilizan la seguridad de UNIX que solo tienen aplicados permisos de bit de modo (sin ACL de NFSv4).

- Los campos de salida de propietario y grupo de la salida ACL se aplican sólo en el caso de los descriptores de seguridad NTFS.
- Debido a que la seguridad de Access Guard a nivel de almacenamiento se puede configurar en un volumen o qtree de estilo de seguridad mixto incluso si el estilo de seguridad efectivo del volumen raíz o qtree es UNIX, Los resultados de una ruta de volumen o qtree en la que se configuró Storage-Level Access Guard pueden mostrar tanto el archivo NFSv4 normal como las SACL de directorio y las SACL de Storage-Level Access Guard.
- Como la seguridad de Access Guard en el nivel de almacenamiento se admite en un volumen UNIX o qtree si hay un servidor CIFS configurado en la SVM, el resultado puede contener información sobre la seguridad de Access Guard en el nivel de almacenamiento aplicada al volumen o qtree especificados en el `-path` parámetro.

Pasos

1. Mostrar la configuración de seguridad de archivos y directorios con el nivel de detalle deseado:

Si desea mostrar información…	Introduzca el siguiente comando…
En forma de resumen	`vserver security file-directory show -vserver vserver_name -path path`
Con detalle ampliado	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Ejemplos

En el ejemplo siguiente se muestra información de seguridad sobre la ruta de `/lab` SVM VS1. Esta ruta de seguridad de UNIX tiene un SACL de NFSv4.

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

Aprenda a mostrar información sobre políticas de auditoría y seguridad de archivos SMB de ONTAP

Puede utilizar el carácter comodín (*) para mostrar información acerca de las directivas de auditoría y seguridad de archivos de todos los archivos y directorios de una ruta de acceso determinada o de un volumen raíz.

El carácter comodín (**) se puede utilizar como último subcomponente de una ruta de directorio dada debajo de la cual se desea mostrar información de todos los archivos y directorios. Si desea mostrar información de un archivo o directorio concreto denominado «*»**», deberá proporcionar la ruta completa dentro de comillas dobles (»'"').

Ejemplo

El siguiente comando con carácter comodín muestra la información de todos los archivos y directorios debajo de la ruta de `/1/` SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

El siguiente comando muestra la información de un archivo llamado “*” bajo la ruta de `/vol1/a` SVM VS1. La ruta está entre comillas dobles (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                Vserver: vs1
              File Path: "/vol1/a/*"
      Security Style: mixed
     Effective Style: unix
      DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
         Unix User Id: 1002
        Unix Group Id: 65533
       Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                  ACLs: NFSV4 Security Descriptor
                        Control:0x8014
                        SACL - ACEs
                          AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                        DACL - ACEs
                          ALLOW-EVERYONE@-0x1f00a9-FI|DI
                          ALLOW-OWNER@-0x1f01ff-FI|DI
                          ALLOW-GROUP@-0x1200a9-IG
```

Gestione la seguridad de archivos NTFS, políticas de auditoría NTFS y Storage-Level Access Guard mediante la CLI

Comandos ONTAP para administrar la seguridad de archivos NTFS de SMB, las políticas de auditoría de NTFS y la protección de acceso a nivel de almacenamiento

Puede gestionar la seguridad de archivos NTFS, políticas de auditoría de NTFS y Storage-Level Access Guard en máquinas virtuales de almacenamiento (SVM) mediante la interfaz de línea de comandos.

Puede gestionar las políticas de auditoría y seguridad de archivos NTFS desde clientes SMB o mediante la CLI. Sin embargo, al utilizar la interfaz de línea de comandos para configurar las políticas de seguridad de los archivos y de auditoría, no es necesario utilizar un cliente remoto para gestionar la seguridad de los archivos. El uso de la CLI puede reducir significativamente el tiempo que lleva aplicar la seguridad en muchos archivos y carpetas mediante un único comando.

Puede configurar la protección de acceso al nivel de almacenamiento, que es otra capa de seguridad aplicada por ONTAP a los volúmenes de SVM. Storage-Level Access Guard se aplica a los accesos desde todos los protocolos NAS al objeto de almacenamiento al que se aplica la protección de acceso a nivel de almacenamiento.

El protector de acceso a nivel de almacenamiento se puede configurar y gestionar solo desde la interfaz de línea de comandos de ONTAP. No se puede gestionar la configuración de Access Guard en el nivel de almacenamiento desde clientes SMB. Además, si ve la configuración de seguridad en un archivo o un directorio desde un cliente NFS o SMB, no verá la seguridad Storage-Level Access Guard. La seguridad de protección de acceso a nivel de almacenamiento no se puede revocar de un cliente, ni siquiera por un

administrador de sistema (Windows o UNIX). Por lo tanto, Storage-Level Access Guard ofrece una capa adicional de seguridad para el acceso a los datos que el administrador de almacenamiento establece y gestiona independientemente.

> Aunque solo se admiten permisos de acceso NTFS para Storage-Level Access Guard, ONTAP puede realizar comprobaciones de seguridad para acceder a través de NFS a datos en volúmenes donde se aplica Storage-Level Access Guard si el usuario UNIX se asigna a un usuario de Windows en la SVM propietaria del volumen.

Volúmenes de estilo de seguridad de NTFS

Todos los archivos y carpetas contenidos en qtrees y volúmenes de estilo de seguridad NTFS tienen una seguridad efectiva de NTFS. Puede utilizar `vserver security file-directory` la familia de comandos para implementar los siguientes tipos de seguridad en volúmenes de estilo de seguridad NTFS:

- Los permisos de archivo y las políticas de auditoría a los archivos y las carpetas que contiene el volumen
- Seguridad para proteger el acceso al nivel de almacenamiento en los volúmenes

Volúmenes mixtos de estilo de seguridad

Los volúmenes y qtrees de estilo de seguridad mixtos pueden contener algunos archivos y carpetas con seguridad efectiva de UNIX y usar permisos de archivos de UNIX, bits de modo o ACL de NFSv4.x y políticas de auditoría de NFSv4.x, y algunos archivos y carpetas que tengan seguridad efectiva de NTFS y usen permisos de archivos NTFS y políticas de auditoría. Puede utilizar `vserver security file-directory` la familia de comandos para aplicar los siguientes tipos de seguridad a los datos mixtos de estilo de seguridad:

- Permisos de archivo y políticas de auditoría para archivos y carpetas con un estilo de seguridad NTFS efectivo en el volumen o qtree mixtos
- Protección del acceso a nivel de almacenamiento para volúmenes con seguridad efectiva de NTFS y UNIX

Volúmenes de estilo de seguridad de UNIX

Los volúmenes y qtrees de estilo de seguridad de UNIX contienen archivos y carpetas que tienen una seguridad efectiva de UNIX (bits de modo o ACL de NFSv4.x). Debe tener en cuenta lo siguiente si desea utilizar `vserver security file-directory` la familia de comandos para implementar la seguridad en volúmenes de estilo de seguridad de UNIX:

- `vserver security file-directory`La familia de comandos no se puede utilizar para gestionar las políticas de auditoría y seguridad de archivos UNIX en volúmenes y qtrees de tipo de seguridad de UNIX.
- `vserver security file-directory`La familia de comandos se puede usar para configurar Storage-Level Access Guard en volúmenes de estilo de seguridad de UNIX, siempre y cuando la SVM con el volumen de destino contenga un servidor CIFS.

Información relacionada

- Obtenga información sobre cómo visualizar las políticas de seguridad y auditoría de archivos
- Crear descriptores de seguridad NTFS en servidores
- Comandos para configurar y aplicar políticas de auditoría a archivos y carpetas
- Obtenga información sobre el acceso seguro a archivos mediante Storage-Level Access Guard

Comandos ONTAP para configurar la seguridad de archivos y carpetas SMB

Dado que puede aplicar y administrar la seguridad de archivos y carpetas localmente sin la participación de un cliente remoto, puede reducir significativamente el tiempo que tarda en establecer la seguridad masiva en un gran número de archivos o carpetas.

Puede beneficiarse del uso de la CLI para establecer la seguridad de archivos y carpetas en los siguientes casos de uso:

- Almacenamiento de ficheros en entornos empresariales de gran tamaño, como el almacenamiento de ficheros en directorios iniciales
- Migración de datos
- Cambio de dominio de Windows
- Estandarización de las políticas de auditoría y seguridad de archivos en sistemas de archivos NTFS

Conozca los límites al usar comandos ONTAP para configurar la seguridad de archivos y carpetas SMB

Debe estar al tanto de determinados límites cuando utilice la CLI para establecer la seguridad de archivos y carpetas.

- `vserver security file-directory`La familia de comandos no admite la configuración de ACL NFSv4.

  Sólo puede aplicar descriptores de seguridad NTFS a archivos y carpetas NTFS.

Utilice descriptores de seguridad para aplicar la seguridad de archivos y carpetas SMB de ONTAP

Los descriptores de seguridad contienen las listas de control de acceso que determinan qué acciones puede realizar un usuario en archivos y carpetas, y qué se audita cuando un usuario accede a archivos y carpetas.

- **Permisos**

  El propietario de un objeto permite o deniega los permisos y determina qué acciones puede realizar un objeto (usuarios, grupos u objetos de equipo) en archivos o carpetas especificados.

- **Descriptores de seguridad**

  Los descriptores de seguridad son estructuras de datos que contienen información de seguridad que definen los permisos asociados a un archivo o carpeta.

- **Listas de control de acceso (ACL)**

  Las listas de control de acceso son las listas contenidas en un descriptor de seguridad que contienen información sobre las acciones que los usuarios, grupos o objetos de equipo pueden realizar en el archivo o la carpeta a la que se aplica el descriptor de seguridad. El descriptor de seguridad puede contener los siguientes dos tipos de ACL:

  - Listas de control de acceso discrecional (DACL)
  - Listas de control de acceso del sistema (SACL)
- **Listas de control de acceso discrecional (DACL)**

Las DACL contienen la lista de SIDS para los usuarios, grupos y objetos de equipo a los que se permite o deniega el acceso para realizar acciones en archivos o carpetas. Las DACL contienen entradas de control de acceso cero o más (ACE).

- **Listas de control de acceso al sistema (SACL)**

  SACL contiene la lista de SID para los usuarios, grupos y objetos de equipo para los que se registran eventos de auditoría correctos o fallidos. Las SACL contienen entradas de control de acceso cero o más (ACE).

- **Entradas de control de acceso (ACE)**

  Las ACE son entradas individuales en DACL o SACL:

  - Una entrada de control de acceso DACL especifica los derechos de acceso que se permiten o deniegan para determinados usuarios, grupos o objetos de equipo.
  - Una entrada de control de acceso SACL especifica los eventos de éxito o de error que se deben registrar al auditar acciones especificadas realizadas por usuarios, grupos o objetos de equipo específicos.

- **Herencia de permisos**

  La herencia de permisos describe cómo los permisos definidos en los descriptores de seguridad se propagan a un objeto de un objeto primario. Sólo los objetos secundarios heredan los permisos heredables. Al establecer permisos en el objeto padre, puede decidir si las carpetas, subcarpetas y archivos pueden heredarlos con «`Aplicar a `this-folder`, `sub-folders` y `archivos`».

Información relacionada

- "Seguimiento de seguridad y auditoría de SMB y NFS"
- Comandos para configurar y aplicar políticas de auditoría a archivos y carpetas

Obtenga información sobre cómo aplicar políticas de directorio de archivos que utilizan usuarios o grupos SMB locales en el destino de recuperación ante desastres de ONTAP SVM

Hay ciertas directrices que debe tener en cuenta antes de aplicar políticas de directorio de archivos en el destino de recuperación ante desastres de la máquina virtual de almacenamiento (SVM) en una configuración de descarte de ID si la configuración de la política de directorio de archivos usa usuarios o grupos locales en el descriptor de seguridad, o en las entradas DACL o SACL.

Puede configurar una configuración de recuperación ante desastres para una SVM donde la SVM de origen en el clúster de origen replica los datos y la configuración desde la SVM de origen a una SVM de destino en un clúster de destino.

Puede configurar uno de los dos tipos de recuperación ante desastres de SVM:

- Se conserva la identidad

  Con esta configuración se conserva la identidad de la SVM y el servidor CIFS.

- Identidad descartada

  Con esta configuración, no se conserva la identidad de la SVM y el servidor CIFS. En esta situación, el

nombre de la SVM y el servidor CIFS en la SVM de destino es diferente de la SVM y del nombre del servidor CIFS en la SVM de origen.

Directrices para configuraciones de identidad descartadas

En una configuración de identidad descartada, en el caso de un origen de SVM que contenga configuraciones de usuarios locales, grupos y privilegios, se debe cambiar el nombre del dominio local (nombre del servidor CIFS local) para que coincida con el nombre del servidor CIFS en el destino de SVM. Por ejemplo, si el nombre de la SVM de origen es «'vs1'» y el nombre del servidor CIFS es «'CIFS1'» y el nombre de la SVM de destino es «'vs1_dst'» y el nombre del servidor CIFS es «'CIFS1_DST», el nombre de dominio local de un usuario local denominado «'CIFS1\user1' se cambia automáticamente a «CIFS1» en el destino».

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1_dst      CIFS1_DST\Administrator                 Built-in
administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

Aunque los nombres de usuario local y de grupos se modifican automáticamente en las bases de datos de usuario local y de grupos, los usuarios locales o los nombres de grupo no se modifican automáticamente en las configuraciones de las políticas de directorio de archivos (las políticas configuradas en la interfaz de línea de `vserver security file-directory` comandos mediante la familia de comandos).

Por ejemplo, para «`VS1`», si ha configurado una entrada DACL en la que el `-account` parámetro se establece en «`CIFS1\user1`», la configuración no se cambia automáticamente en la SVM de destino para reflejar el nombre del servidor CIFS del destino.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

Debe utilizar `vserver security file-directory modify` los comandos para cambiar manualmente el nombre del servidor CIFS al nombre del servidor CIFS de destino.

Componentes de configuración de directivas de directorio de archivos que contienen parámetros de cuenta

Existen tres componentes de configuración de directivas de directorio de archivos que pueden utilizar parámetros que pueden contener usuarios o grupos locales:

- Descriptor de seguridad

  Opcionalmente, puede especificar el propietario del descriptor de seguridad y el grupo primario del propietario del descriptor de seguridad. Si el descriptor de seguridad utiliza un usuario o grupo local para las entradas del propietario y del grupo primario, debe modificar el descriptor de seguridad para utilizar la SVM de destino en el nombre de cuenta. Puede usar el `vserver security file-directory ntfs modify` comando para realizar los cambios necesarios en los nombres de cuentas.

- Entradas de DACL

  Cada entrada de DACL debe estar asociada a una cuenta. Debe modificar todas las DACL que utilicen cuentas de usuario local o de grupo para usar el nombre de la SVM de destino. Debido a que no puede modificar el nombre de cuenta para las entradas DACL existentes, debe eliminar todas las entradas DACL con usuarios o grupos locales de los descriptores de seguridad, crear nuevas entradas DACL con los nombres de cuenta de destino corregidos y asociar estas nuevas entradas DACL con los descriptores de seguridad adecuados.

- Entradas de SACL

  Cada entrada de SACL debe estar asociada a una cuenta. Debe modificar todas las SACL que utilicen

cuentas de usuario o de grupo local para utilizar el nombre de la SVM de destino. Debido a que no puede modificar el nombre de cuenta para las entradas SACL existentes, debe eliminar todas las entradas SACL con usuarios o grupos locales de los descriptores de seguridad, crear nuevas entradas SACL con los nombres de cuenta de destino corregidos y asociar estas nuevas entradas SACL con los descriptores de seguridad adecuados.

Debe realizar los cambios necesarios en los usuarios o grupos locales utilizados en la configuración de la directiva de directorio de archivos antes de aplicar la directiva; de lo contrario, el trabajo de aplicación fallará.

Configurar y aplicar la seguridad de archivos en archivos y carpetas NTFS mediante la CLI

Crear descriptores de seguridad NTFS en servidores SMB de ONTAP

Crear un descriptor de seguridad NTFS (política de seguridad de archivos) es el primer paso para configurar y aplicar listas de control de acceso NTFS (ACL) a archivos y carpetas que residen en máquinas virtuales de almacenamiento (SVM). Puede asociar el descriptor de seguridad a la ruta de archivo o carpeta en una tarea de directiva.

Acerca de esta tarea

Puede crear descriptores de seguridad NTFS para archivos y carpetas que residen dentro de volúmenes de estilo de seguridad NTFS o para archivos y carpetas que residen en volúmenes de estilo de seguridad mixtos.

De forma predeterminada, cuando se crea un descriptor de seguridad, se agregan cuatro entradas de control de acceso de lista de control de acceso discrecional (DACL) a ese descriptor de seguridad. Los cuatro ACE predeterminados son los siguientes:

Objeto	Tipo de acceso	Derechos de acceso	Dónde aplicar los permisos
BUILTIN\Administrators	Permita	Control total	esta carpeta, subcarpetas, archivos
BUILTIN\Users	Permita	Control total	esta carpeta, subcarpetas, archivos
PROPIETARIO DEL CREADOR	Permita	Control total	esta carpeta, subcarpetas, archivos
NT AUTHORITY\SYSTEM	Permita	Control total	esta carpeta, subcarpetas, archivos

Es posible personalizar la configuración del descriptor de seguridad mediante los siguientes parámetros opcionales:

- Propietario del descriptor de seguridad
- Grupo principal del propietario
- Indicadores de control RAW

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Obtenga más información en el "Referencia de comandos del ONTAP".

Agregue entradas de control de acceso NTFS DACL a los descriptores de seguridad NTFS en servidores SMB de ONTAP

La adición de entradas de control de acceso (ACE) de DACL (lista de control de acceso discrecional) al descriptor de seguridad de NTFS es el segundo paso para configurar y aplicar ACL de NTFS a un archivo o carpeta. Cada entrada identifica qué objeto tiene permiso o acceso denegado, y define lo que el objeto puede o no puede hacer con los archivos o carpetas definidos en ACE.

Acerca de esta tarea

Puede añadir una o varias ACE a la DACL del descriptor de seguridad.

Si el descriptor de seguridad contiene una DACL que tiene ACE existentes, el comando agrega la nueva ACE a la DACL. Si el descriptor de seguridad no contiene una DACL, el comando crea la DACL y le agrega la nueva ACE.

Opcionalmente, puede personalizar las entradas DACL especificando qué derechos desea permitir o denegar para la cuenta especificada en el `-account` parámetro. Hay tres métodos mutuamente exclusivos para especificar los derechos:

- Derechos
- Derechos avanzados
- Derechos RAW (privilegio avanzado)

> Si no especifica derechos para la entrada DACL, el valor predeterminado es establecer los derechos en `Full Control`.

Opcionalmente, puede personalizar las entradas DACL especificando cómo aplicar herencia.

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

Pasos

1. Agregue una entrada DACL a un descriptor de seguridad: `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
   -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
   ```

2. Compruebe que la entrada DACL es correcta: `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

```
                Vserver: vs1
Security Descriptor Name: sd1
             Allow or Deny: deny
         Account Name or SID: DOMAIN\joe
               Access Rights: full-control
  Advanced Access Rights: -
                    Apply To: this-folder
               Access Rights: full-control
```

Obtenga más información sobre `vserver security file-directory ntfs dacl` en el "Referencia de comandos del ONTAP".

Crear políticas de seguridad de ONTAP SMB

Crear una política de seguridad de archivos para SVM es el tercer paso a la hora de configurar y aplicar ACL a un archivo o carpeta. Una directiva actúa como contenedor para varias tareas, donde cada tarea es una entrada única que se puede aplicar a archivos o carpetas. Posteriormente, puede agregar tareas a la directiva de seguridad.

Acerca de esta tarea

Las tareas que agrega a una directiva de seguridad contienen asociaciones entre el descriptor de seguridad NTFS y las rutas de acceso de archivos o carpetas. Por lo tanto, debe asociar la política de seguridad con cada SVM (que contenga volúmenes de estilo de seguridad NTFS o volúmenes mixtos de estilo de seguridad).

Pasos

1. Cree una política de seguridad: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. Verifique la política de seguridad: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Agregar tareas a la política de seguridad de ONTAP SMB

Crear y añadir una tarea de política a una política de seguridad es el cuarto paso para configurar y aplicar ACL a archivos o carpetas en SVM. Al crear la tarea de directiva, asocie la tarea a una directiva de seguridad. Puede agregar una o más entradas de tareas a una directiva de seguridad.

Acerca de esta tarea

La política de seguridad es un contenedor para una tarea. Una tarea hace referencia a una única operación que puede realizar una directiva de seguridad para archivos o carpetas con seguridad NTFS o mixta (o a un objeto de volumen si se configura Storage-Level Access Guard).

Existen dos tipos de tareas:

- Tareas de archivo y directorio

  Se utiliza para especificar tareas que aplican descriptores de seguridad a archivos y carpetas especificados. Las ACL aplicadas mediante tareas de archivo y directorio se pueden gestionar con clientes de SMB o con la interfaz de línea de comandos de ONTAP.

- Tareas de protección de acceso al nivel de almacenamiento

  Se utiliza para especificar tareas que aplican descriptores de seguridad de Access Guard de nivel de almacenamiento a un volumen especificado. Las ACL aplicadas mediante tareas de protección de acceso al nivel de almacenamiento solo se pueden gestionar a través de la interfaz de línea de comandos de ONTAP.

Una tarea contiene definiciones para la configuración de seguridad de un archivo (o carpeta) o un conjunto de archivos (o carpetas). Cada tarea de una política se identifica de forma única por la ruta. Sólo puede haber una tarea por ruta dentro de una única política. Una directiva no puede tener entradas de tareas duplicadas.

Directrices para agregar una tarea a una directiva:

- Puede haber un máximo de 10,000 entradas de tareas por directiva.
- Una política puede contener una o más tareas.

  Aunque una directiva puede contener más de una tarea, no puede configurar una directiva para que contenga tareas de directorio de archivos y de protección de acceso a nivel de almacenamiento. Una política debe contener todas las tareas de Storage-Level Access Guard o todas las tareas de directorio de archivos.

- Se utiliza Storage-Level Access Guard para restringir los permisos.

  Nunca dará permisos de acceso adicionales.

Al agregar tareas a las directivas de seguridad, debe especificar los siguientes cuatro parámetros necesarios:

- Nombre de SVM
- Nombre de la política
- Ruta
- Descriptor de seguridad que se asociará a la ruta de acceso

Es posible personalizar la configuración del descriptor de seguridad mediante los siguientes parámetros opcionales:

- Tipo de seguridad
- Modo de propagación
- Posición de índice

- Tipo de control de acceso

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

Pasos

1. Agregue una tarea con un descriptor de seguridad asociado a la política de seguridad: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` es el valor predeterminado del `-access-control` parámetro. Es opcional especificar el tipo de control de acceso cuando se configuran las tareas de acceso a archivos y directorios.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
   ```

2. Verifique la configuración de la tarea de política: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

Obtenga más información sobre `vserver security file-directory policy task` en el "Referencia de comandos del ONTAP".

Aplicar las políticas de seguridad de ONTAP SMB

Aplicar una política de seguridad de archivos a las SVM es el último paso a la hora de crear y aplicar ACL de NTFS a archivos o carpetas.

Acerca de esta tarea

Puede aplicar la configuración de seguridad definida en la política de seguridad a archivos y carpetas NTFS que residen en volúmenes FlexVol (estilo de seguridad NTFS o mixto).

Cuando se aplican una directiva de auditoría y SACL asociadas, se sobrescriben todas las DACL existentes. Cuando se aplica una directiva de seguridad y sus DACL asociados, se sobrescriben todas las DACL existentes. Debe revisar las directivas de seguridad existentes antes de crear y aplicar otras nuevas.

Paso

1. Aplicar una política de seguridad: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory apply -vserver vs1 -policy-name policy1`

   El trabajo de aplicación de política está programado y se devuelve el ID de trabajo.

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

Supervisar los trabajos de políticas de seguridad de ONTAP SMB

Al aplicar la política de seguridad a máquinas virtuales de almacenamiento (SVM), puede supervisar el progreso de la tarea supervisando el trabajo de la política de seguridad. Esto es útil si desea comprobar que la aplicación de la política de seguridad ha sido satisfactoria. Esto también resulta útil si tiene un trabajo de larga ejecución en el que está aplicando seguridad masiva a un gran número de archivos y carpetas.

Acerca de esta tarea

Para mostrar información detallada sobre un trabajo de política de seguridad, debe utilizar el `-instance` parámetro.

Paso

1. Supervise el trabajo de política de seguridad: `vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Verificar la seguridad de los archivos SMB de ONTAP

Es posible verificar la configuración de seguridad de archivos para confirmar que los archivos o las carpetas de la máquina virtual de almacenamiento (SVM) a la que aplicó la política de seguridad tienen la configuración deseada.

Acerca de esta tarea

Debe suministrar el nombre de la SVM que contenga los datos y la ruta de acceso al archivo y las carpetas en los que desea verificar la configuración de seguridad. Puede utilizar el parámetro opcional `-expand-mask` para mostrar información detallada sobre la configuración de seguridad.

Paso

1. Mostrar configuración de seguridad de archivos y carpetas: `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

   `vserver security file-directory show -vserver vs1 -path /data/engineering -expand-mask true`

```
         Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
          Unix User Id: 0
         Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
```

```
                           .... .... .... ..0. = Group Defaulted
                           .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
                             ...0 .... .... .... .... .... .... .... =
Generic All
                             .... ...0 .... .... .... .... .... .... =
System Security
                             .... .... ...1 .... .... .... .... .... =
Synchronize
                             .... .... .... 1... .... .... .... .... =
Write Owner
                             .... .... .... .1.. .... .... .... .... =
Write DAC
                             .... .... .... ..1. .... .... .... .... =
Read Control
                             .... .... .... ...1 .... .... .... .... =
Delete
                             .... .... .... .... .... ...1 .... .... =
Write Attributes
                             .... .... .... .... .... .... 1... .... =
Read Attributes
                             .... .... .... .... .... .... .1.. .... =
Delete Child
                             .... .... .... .... .... .... ..1. .... =
Execute
                             .... .... .... .... .... .... ...1 .... =
Write EA
                             .... .... .... .... .... .... .... 1... =
Read EA
                             .... .... .... .... .... .... .... .1.. =
Append
                             .... .... .... .... .... .... .... ..1. =
Write
                             .... .... .... .... .... .... .... ...1 =
Read
```

```
                           ALLOW-Everyone-0x10000000-OI|CI|IO
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
                             ...1 .... .... .... .... .... .... .... =
Generic All
                             .... ...0 .... .... .... .... .... .... =
System Security
                             .... .... ...0 .... .... .... .... .... =
Synchronize
                             .... .... .... 0... .... .... .... .... =
Write Owner
                             .... .... .... .0.. .... .... .... .... =
Write DAC
                             .... .... .... ..0. .... .... .... .... =
Read Control
                             .... .... .... ...0 .... .... .... .... =
Delete
                             .... .... .... .... .... ...0 .... .... =
Write Attributes
                             .... .... .... .... .... .... 0... .... =
Read Attributes
                             .... .... .... .... .... .... .0.. .... =
Delete Child
                             .... .... .... .... .... .... ..0. .... =
Execute
                             .... .... .... .... .... .... ...0 .... =
Write EA
                             .... .... .... .... .... .... .... 0... =
Read EA
                             .... .... .... .... .... .... .... .0.. =
Append
                             .... .... .... .... .... .... .... ..0. =
Write
                             .... .... .... .... .... .... .... ...0 =
Read
```

Configurar y aplicar directivas de auditoría a archivos y carpetas NTFS mediante la interfaz de línea de comandos

Comandos ONTAP para configurar y aplicar políticas de auditoría SMB a archivos y carpetas NTFS

Hay varios pasos que debe realizar para aplicar políticas de auditoría a archivos y carpetas NTFS cuando use la CLI de ONTAP. En primer lugar, debe crear un descriptor

de seguridad NTFS y agregar SACL al descriptor de seguridad. A continuación, cree una directiva de seguridad y agregue tareas de directiva. Luego, debe aplicar la política de seguridad a una SVM.

Acerca de esta tarea

Después de aplicar la directiva de seguridad, puede supervisar el trabajo de directiva de seguridad y, a continuación, verificar la configuración de la directiva de auditoría aplicada.

> Cuando se aplican una directiva de auditoría y SACL asociadas, se sobrescriben todas las DACL existentes. Debe revisar las directivas de seguridad existentes antes de crear y aplicar otras nuevas.

Información relacionada

- Obtenga información sobre el acceso seguro a archivos mediante Storage-Level Access Guard
- Conozca los límites al usar comandos para configurar la seguridad de archivos y carpetas SMB
- Utilice descriptores de seguridad para aplicar seguridad a archivos y carpetas
- "Seguimiento de seguridad y auditoría de SMB y NFS"
- Crear descriptores de seguridad NTFS en servidores

Crear descriptores de seguridad NTFS en servidores SMB de ONTAP

Crear una política de auditoría de descriptor de seguridad NTFS es el primer paso para configurar y aplicar listas de control de acceso NTFS (ACL) a archivos y carpetas que residen en SVM. Asociará el descriptor de seguridad a la ruta de archivo o carpeta en una tarea de directiva.

Acerca de esta tarea

Puede crear descriptores de seguridad NTFS para archivos y carpetas que residen dentro de volúmenes de estilo de seguridad NTFS o para archivos y carpetas que residen en volúmenes de estilo de seguridad mixtos.

De forma predeterminada, cuando se crea un descriptor de seguridad, se agregan cuatro entradas de control de acceso de lista de control de acceso discrecional (DACL) a ese descriptor de seguridad. Los cuatro ACE predeterminados son los siguientes:

Objeto	Tipo de acceso	Derechos de acceso	Dónde aplicar los permisos
BUILTIN\Administrators	Permita	Control total	esta carpeta, subcarpetas, archivos
BUILTIN\Users	Permita	Control total	esta carpeta, subcarpetas, archivos
PROPIETARIO DEL CREADOR	Permita	Control total	esta carpeta, subcarpetas, archivos
NT AUTHORITY\SYSTEM	Permita	Control total	esta carpeta, subcarpetas, archivos

Es posible personalizar la configuración del descriptor de seguridad mediante los siguientes parámetros opcionales:

- Propietario del descriptor de seguridad
- Grupo principal del propietario
- Indicadores de control RAW

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

Pasos

1. Si desea utilizar los parámetros avanzados, configure el nivel de privilegio en advanced: `set -privilege advanced`
2. Cree un descriptor de seguridad: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   ```
   vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe
   ```

3. Compruebe que la configuración del descriptor de seguridad es correcta: `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

   ```
   vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
   ```

   ```
                                   Vserver: vs1
                        Security Descriptor Name: sd1
                  Owner of the Security Descriptor: DOMAIN\joe
   ```

4. Si se encuentra en el nivel de privilegio avanzado, vuelva al nivel de privilegio de administrador: `set -privilege admin`

Agregue entradas de control de acceso SACL NTFS a los descriptores de seguridad NTFS en servidores SMB de ONTAP

Añadir entradas de control de acceso (ACE) SACL (lista de control de acceso del sistema) al descriptor de seguridad NTFS es el segundo paso a la hora de crear directivas de auditoría NTFS para archivos o carpetas en SVM. Cada entrada identifica el usuario o grupo que desea auditar. La entrada SACL define si desea auditar los intentos de acceso fallidos o correctos.

Acerca de esta tarea

Puede añadir una o varias ACE a la SACL del descriptor de seguridad.

Si el descriptor de seguridad contiene una SACL que tiene ACE existentes, el comando agrega la nueva ACE a la SACL. Si el descriptor de seguridad no contiene una SACL, el comando crea la SACL y le agrega la nueva ACE.

Puede configurar entradas de SACL especificando los derechos que desea auditar para eventos de éxito o fallo de la cuenta especificada en el `-account` parámetro. Hay tres métodos mutuamente exclusivos para especificar los derechos:

- Derechos
- Derechos avanzados
- Derechos RAW (privilegio avanzado)

Si no especifica derechos para la entrada SACL, el valor por defecto es `Full Control`.

Opcionalmente, puede personalizar las entradas de SACL especificando cómo aplicar la herencia con el `apply to` parámetro. Si no especifica este parámetro, el valor predeterminado es aplicar esta entrada SACL a esta carpeta, subcarpetas y archivos.

Pasos

1. Agregue una entrada SACL a un descriptor de seguridad: `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
   failure -account domain\joe -rights full-control -apply-to this-folder
   -vserver vs1
   ```

2. Compruebe que la entrada de SACL es correcta: `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

   ```
                                Vserver: vs1
                  Security Descriptor Name: sd1
   Access type for Specified Access Rights: failure
                       Account Name or SID: DOMAIN\joe
                             Access Rights: full-control
                    Advanced Access Rights: -
                                  Apply To: this-folder
                             Access Rights: full-control
   ```

Crear políticas de seguridad de ONTAP SMB

Crear una política de auditoría para máquinas virtuales de almacenamiento (SVM) es el tercer paso a la hora de configurar y aplicar ACL a un archivo o una carpeta. Una directiva actúa como contenedor para varias tareas, donde cada tarea es una entrada única que se puede aplicar a archivos o carpetas. Posteriormente, puede agregar tareas a la directiva de seguridad.

Acerca de esta tarea

Las tareas que agrega a una directiva de seguridad contienen asociaciones entre el descriptor de seguridad NTFS y las rutas de acceso de archivos o carpetas. Por lo tanto, debe asociar la política de seguridad con cada máquina virtual de almacenamiento (SVM) (que contenga volúmenes de estilo de seguridad NTFS o volúmenes mixtos de estilo de seguridad).

Pasos

1. Cree una política de seguridad: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. Verifique la política de seguridad: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Agregar tareas a la política de seguridad de ONTAP SMB

Crear y añadir una tarea de política a una política de seguridad es el cuarto paso para configurar y aplicar ACL a archivos o carpetas en SVM. Al crear la tarea de directiva, asocie la tarea a una directiva de seguridad. Puede agregar una o más entradas de tareas a una directiva de seguridad.

Acerca de esta tarea

La política de seguridad es un contenedor para una tarea. Una tarea hace referencia a una única operación que puede realizar una directiva de seguridad para archivos o carpetas con seguridad NTFS o mixta (o a un objeto de volumen si se configura Storage-Level Access Guard).

Existen dos tipos de tareas:

- Tareas de archivo y directorio

  Se utiliza para especificar tareas que aplican descriptores de seguridad a archivos y carpetas especificados. Las ACL aplicadas mediante tareas de archivo y directorio se pueden gestionar con clientes de SMB o con la interfaz de línea de comandos de ONTAP.

- Tareas de protección de acceso al nivel de almacenamiento

  Se utiliza para especificar tareas que aplican descriptores de seguridad de Access Guard de nivel de almacenamiento a un volumen especificado. Las ACL aplicadas mediante tareas de protección de acceso al nivel de almacenamiento solo se pueden gestionar a través de la interfaz de línea de comandos de ONTAP.

Una tarea contiene definiciones para la configuración de seguridad de un archivo (o carpeta) o un conjunto de archivos (o carpetas). Cada tarea de una política se identifica de forma única por la ruta. Sólo puede haber una tarea por ruta dentro de una única política. Una directiva no puede tener entradas de tareas duplicadas.

Directrices para agregar una tarea a una directiva:

- Puede haber un máximo de 10,000 entradas de tareas por directiva.
- Una política puede contener una o más tareas.

  Aunque una directiva puede contener más de una tarea, no puede configurar una directiva para que contenga tareas de directorio de archivos y de protección de acceso a nivel de almacenamiento. Una política debe contener todas las tareas de Storage-Level Access Guard o todas las tareas de directorio de archivos.

- Se utiliza Storage-Level Access Guard para restringir los permisos.

  Nunca dará permisos de acceso adicionales.

Es posible personalizar la configuración del descriptor de seguridad mediante los siguientes parámetros opcionales:

- Tipo de seguridad
- Modo de propagación
- Posición de índice
- Tipo de control de acceso

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

Pasos

1. Agregue una tarea con un descriptor de seguridad asociado a la política de seguridad: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` es el valor predeterminado del `-access-control` parámetro. Es opcional especificar el tipo de control de acceso cuando se configuran las tareas de acceso a archivos y directorios.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
   ```

2. Verifique la configuración de la tarea de política: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

```
Vserver: vs1
Policy: policy1

Index    File/Folder    Access           Security   NTFS       NTFS
Security
         Path           Control          Type       Mode
Descriptor Name
-----    --------       -----------      --------   ------
----------------
1        /home/dir1     file-directory   ntfs       propagate  sd2
```

Obtenga más información sobre `vserver security file-directory policy task` en el "Referencia de comandos del ONTAP".

Aplicar las políticas de seguridad de ONTAP SMB

Aplicar una política de auditoría a las SVM es el último paso a la hora de crear y aplicar ACL de NTFS a archivos o carpetas.

Acerca de esta tarea

Puede aplicar la configuración de seguridad definida en la política de seguridad a archivos y carpetas NTFS que residen en volúmenes FlexVol (estilo de seguridad NTFS o mixto).

> Cuando se aplican una directiva de auditoría y SACL asociadas, se sobrescriben todas las DACL existentes. Cuando se aplica una directiva de seguridad y sus DACL asociados, se sobrescriben todas las DACL existentes. Debe revisar las directivas de seguridad existentes antes de crear y aplicar otras nuevas.

Paso

1. Aplicar una política de seguridad: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory apply -vserver vs1 -policy-name policy1
   ```

   El trabajo de aplicación de política está programado y se devuelve el ID de trabajo.

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

Supervisar los trabajos de políticas de seguridad de ONTAP SMB

Al aplicar la política de seguridad a máquinas virtuales de almacenamiento (SVM), puede supervisar el progreso de la tarea supervisando el trabajo de la política de seguridad. Esto es útil si desea comprobar que la aplicación de la política de seguridad ha sido satisfactoria. Esto también resulta útil si tiene un trabajo de larga ejecución en el que

está aplicando seguridad masiva a un gran número de archivos y carpetas.

Acerca de esta tarea

Para mostrar información detallada sobre un trabajo de política de seguridad, debe utilizar el `-instance` parámetro.

Paso

1. Supervise el trabajo de política de seguridad: `vserver security file-directory job show -vserver vserver_name`

   ```
   vserver security file-directory job show -vserver vs1
   ```

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Verificar las políticas de auditoría de ONTAP SMB

Puede verificar la política de auditoría para confirmar que los archivos o las carpetas de la máquina virtual de almacenamiento (SVM) a la que aplicó la política de seguridad tienen la configuración de seguridad de auditoría deseada.

Acerca de esta tarea

El `vserver security file-directory show` comando se utiliza para mostrar información sobre la política de auditoría. Debe proporcionar el nombre de la SVM que contiene los datos y la ruta a los datos cuyo archivo o carpeta de información de la política de auditoría que desea mostrar.

Paso

1. Mostrar configuración de política de auditoría: `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

Ejemplo

El siguiente comando muestra la información de la directiva de auditoría aplicada a la ruta "'/corp" en SVM vs1. La ruta de acceso tiene aplicada UNA entrada SACL DE ÉXITO y DE FALLO:

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

                Vserver: vs1
              File Path: /corp
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Obtenga información sobre cómo administrar los trabajos de políticas de seguridad de ONTAP SMB

Si existe un trabajo de política de seguridad, en determinadas circunstancias, no puede modificar dicha política de seguridad ni las tareas asignadas a dicha política. Debe entender en qué condiciones puede o no puede modificar las directivas de seguridad para que cualquier intento que realice para modificar la directiva se realice correctamente. Las modificaciones de la directiva incluyen agregar, eliminar o modificar tareas asignadas a la directiva y eliminar o modificar la directiva.

No puede modificar una política de seguridad ni una tarea asignada a esa política si existe un trabajo para esa política y ese trabajo está en los estados siguientes:

- El trabajo está en ejecución o en curso.
- El trabajo está en pausa.
- El trabajo se reanuda y se encuentra en estado en ejecución.
- Si el trabajo está esperando a conmutar al respaldo a otro nodo.

En las siguientes circunstancias, si existe un trabajo para una política de seguridad, puede modificar correctamente dicha política de seguridad o una tarea asignada a dicha directiva:

- El trabajo de política se ha detenido.
- El trabajo de directiva ha finalizado correctamente.

Comandos ONTAP para administrar descriptores de seguridad NTFS en servidores SMB

Existen comandos ONTAP específicos para administrar descriptores de seguridad. Puede crear, modificar, eliminar y mostrar información acerca de los descriptores de seguridad.

Si desea…	Se usa este comando…
Crear descriptores de seguridad NTFS	`vserver security file-directory ntfs create`
Modifique los descriptores de seguridad NTFS existentes	`vserver security file-directory ntfs modify`
Mostrar información acerca de los descriptores de seguridad NTFS existentes	`vserver security file-directory ntfs show`
Eliminar descriptores de seguridad NTFS	`vserver security file-directory ntfs delete`

Obtenga más información sobre `vserver security file-directory ntfs` en el "Referencia de comandos del ONTAP".

Comandos ONTAP para administrar entradas de control de acceso DACL NTFS en servidores SMB

Hay comandos ONTAP específicos para administrar entradas de control de acceso DACL (ACE). Puede agregar ACE a DACL NTFS en cualquier momento. También puede administrar las DACL de NTFS existentes modificando, eliminando y mostrando información acerca de las ACE en las DACL.

Si desea…	Se usa este comando…
Cree ACE y agréguelos a DACL NTFS	`vserver security file-directory ntfs dacl add`
Modifique los ACE existentes en las DACL NTFS	`vserver security file-directory ntfs dacl modify`
Mostrar información acerca de los ACE existentes en las DACL NTFS	`vserver security file-directory ntfs dacl show`
Elimine los ACE existentes de las DACL NTFS	`vserver security file-directory ntfs dacl remove`

Obtenga más información sobre `vserver security file-directory ntfs dacl` en el "Referencia de comandos del ONTAP".

Comandos ONTAP para administrar entradas de control de acceso SACL NTFS en servidores SMB

Hay comandos ONTAP específicos para administrar entradas de control de acceso SACL (ACE). Puede agregar ACE a SACL NTFS en cualquier momento. También puede administrar SACL NTFS existentes modificando, eliminando y mostrando información acerca de ACE en SACL.

Si desea…	Se usa este comando…
Cree ACE y agréguelos a SACL NTFS	`vserver security file-directory ntfs sacl add`
Modifique los ACE existentes en SACL NTFS	`vserver security file-directory ntfs sacl modify`
Muestra información acerca de los ACE existentes en SACL NTFS	`vserver security file-directory ntfs sacl show`
Elimine los ACE existentes de SACL NTFS	`vserver security file-directory ntfs sacl remove`

Obtenga más información sobre `vserver security file-directory ntfs sacl` en el "Referencia de comandos del ONTAP".

Comandos de ONTAP para administrar políticas de seguridad SMB

Existen comandos ONTAP específicos para administrar las políticas de seguridad. Puede mostrar información acerca de las políticas y eliminarla. No puede modificar una política de seguridad.

Si desea…	Se usa este comando…
Cree políticas de seguridad	`vserver security file-directory policy create`
Mostrar información acerca de las directivas de seguridad	`vserver security file-directory policy show`
Eliminar políticas de seguridad	`vserver security file-directory policy delete`

Obtenga más información sobre `vserver security file-directory policy` en el "Referencia de comandos del ONTAP".

Comandos ONTAP para administrar tareas de políticas de seguridad SMB

Hay comandos de ONTAP para añadir, modificar, quitar y mostrar información acerca de tareas de políticas de seguridad.

Si desea…	Se usa este comando…
Agregar tareas de directiva de seguridad	`vserver security file-directory policy task add`
Modifique las tareas de las políticas de seguridad	`vserver security file-directory policy task modify`
Muestra información acerca de las tareas de directiva de seguridad	`vserver security file-directory policy task show`
Quitar tareas de directiva de seguridad	`vserver security file-directory policy task remove`

Obtenga más información sobre `vserver security file-directory policy task` en el "Referencia de comandos del ONTAP".

Comandos de ONTAP para administrar trabajos de políticas de seguridad de SMB

Hay comandos de la ONTAP para pausar, reanudar, detener y mostrar información acerca de los trabajos de políticas de seguridad.

Si desea…	Se usa este comando…
Pausar trabajos de directiva de seguridad	`vserver security file-directory job pause -vserver vserver_name -id integer`
Reanudar trabajos de directiva de seguridad	`vserver security file-directory job resume -vserver vserver_name -id integer`
Mostrar información sobre trabajos de directivas de seguridad	`vserver security file-directory job show -vserver vserver_name` Puede determinar el ID de trabajo de un trabajo mediante este comando.
Detener trabajos de directiva de seguridad	`vserver security file-directory job stop -vserver vserver_name -id integer`

Obtenga más información sobre `vserver security file-directory job` en el "Referencia de comandos del ONTAP".

Configure la caché de metadatos para los recursos compartidos de SMB

Obtenga más información sobre el almacenamiento en caché de metadatos SMB de ONTAP

El almacenamiento en caché de metadatos permite almacenar en caché atributos de archivos en clientes SMB 1.0 para proporcionar un acceso más rápido a los atributos de archivos y carpetas. Puede habilitar o deshabilitar el almacenamiento en caché de atributos por recurso compartido. También puede configurar el tiempo de espera para las entradas en caché si está activado el almacenamiento en caché de metadatos. No es necesario configurar el almacenamiento en caché de metadatos si los clientes se conectan a recursos compartidos mediante SMB 2.x o SMB 3.0.

Cuando se habilita esta opción, la caché de metadatos del SMB almacena los datos de atributos de archivos y rutas por una cantidad limitada de tiempo. Esto puede mejorar el rendimiento de SMB para los clientes de SMB 1.0 con cargas de trabajo comunes.

En determinadas tareas, SMB crea una cantidad significativa de tráfico que puede incluir varias consultas idénticas para los metadatos de archivos y rutas. Puede reducir el número de consultas redundantes y mejorar el rendimiento de clientes de SMB 1.0 utilizando el almacenamiento en caché de metadatos del SMB para recuperar información de la caché.

> Si bien es poco probable, es posible que la caché de metadatos proporcione información obsoleta a clientes SMB 1.0. Si su entorno no se puede permitir este riesgo, no debe habilitar esta función.

Habilitar la caché de metadatos SMB de ONTAP

Puede mejorar el rendimiento de SMB para los clientes de SMB 1.0 al habilitar la caché de metadatos de SMB. De manera predeterminada, el almacenamiento en caché de metadatos de SMB está deshabilitado.

Paso

1. Realice la acción deseada:

Si desea…	Introduzca el comando…
Habilite el almacenamiento en caché de metadatos de SMB cuando crea un recurso compartido	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties attributecache`
Habilite el almacenamiento en caché de metadatos de SMB en un recurso compartido existente	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties attributecache`

Información relacionada

- Configurar la duración de las entradas de caché de metadatos
- Agregar o eliminar propiedades de recursos compartidos en recursos compartidos existentes

Configurar la duración de las entradas de caché de metadatos SMB de ONTAP

Puede configurar la vida útil de las entradas de la caché de metadatos SMB para optimizar el rendimiento de la caché de metadatos de SMB en su entorno. El valor predeterminado es 10 segundos.

Antes de empezar

Debe haber habilitado la función de caché de metadatos SMB. Si el almacenamiento en caché de metadatos de SMB no está habilitado, no se utiliza la configuración TTL de la caché de SMB.

Paso

1. Realice la acción deseada:

Si desea configurar la vida útil de las entradas de la caché de metadatos SMB al…	Introduzca el comando…
Crear un recurso compartido	`vserver cifs share -create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-attribute-cache-ttl [integerh][integerm][integers]`
Modifique un recurso compartido existente	`vserver cifs share -modify -vserver` *`vserver_name`* `-share-name` *`share_name`* `-attribute-cache-ttl [integerh][integerm][integers]`

Puede especificar propiedades y opciones de configuración de recursos compartidos adicionales al crear o modificar recursos compartidos. Obtenga más información sobre `vserver cifs share` en el "Referencia de comandos del ONTAP".

Administrar bloqueos de archivos

Obtenga información sobre el bloqueo de archivos SMB de ONTAP entre protocolos

El bloqueo de archivos es un método que utilizan las aplicaciones cliente para evitar que un usuario acceda a un archivo abierto previamente por otro usuario. La forma en que ONTAP bloquea los archivos depende del protocolo del cliente.

Si el cliente es NFS, los bloqueos son consultivos; si el cliente es un cliente SMB, los bloqueos son obligatorios.

Debido a las diferencias entre los bloqueos de archivos NFS y SMB, es posible que un cliente NFS no pueda acceder a un archivo que abrió previamente una aplicación SMB.

Lo siguiente se produce cuando un cliente NFS intenta acceder a un archivo bloqueado por una aplicación SMB:

- En volúmenes mixtos o NTFS, las operaciones de manipulación de archivos `rm` como , , `rmdir` y `mv` pueden provocar el fallo de la aplicación NFS.
- Las operaciones de lectura y escritura de NFS se deniegan en los modos abiertos Deny-Read y Deny-

write de SMB, respectivamente.

- Error en las operaciones de escritura de NFS cuando el rango escrito del archivo está bloqueado por un bytelock exclusivo de SMB.
- Desenlazar
  - En el caso de los sistemas de archivos NTFS, se admiten las operaciones de eliminación de SMB y CIFS.

    El archivo se eliminará después del último cierre.
  - No se admiten las operaciones de desenlace de NFS.

    No es compatible porque la semántica NTFS y SMB es necesaria, y la última operación Delete-on-Close no es compatible con NFS.
  - Para los sistemas de archivos UNIX, se admite la operación de desvinculación.

    Es compatible porque se necesitan semántica NFS y UNIX.
- Cambiar el nombre
  - Para los sistemas de archivos NTFS, si el archivo de destino se abre desde SMB o CIFS, se puede cambiar el nombre del archivo de destino.
  - No se admite el cambio de nombre de NFS.

    No es compatible porque se requieren semánticas NTFS y SMB.

En los volúmenes de estilo de seguridad de UNIX, las operaciones de desenlace y cambio de nombre de NFS ignoran el estado de bloqueo de SMB y permiten el acceso al archivo. Todas las demás operaciones de NFS en volúmenes de estilo de seguridad de UNIX honran el estado de bloqueo de SMB.

Obtenga información sobre los bits de solo lectura de ONTAP SMB

El bit de sólo lectura se establece en base a archivo para reflejar si un archivo es grabable (deshabilitado) o de sólo lectura (habilitado).

Los clientes SMB que usan Windows pueden establecer un bit de solo lectura por archivo. Los clientes NFS no establecen un bit de solo lectura por archivo, ya que los clientes NFS no tienen ninguna operación de protocolo que utilice un bit de solo lectura por archivo.

ONTAP puede establecer un bit de solo lectura en un archivo cuando un cliente SMB que utiliza Windows crea ese archivo. ONTAP también puede establecer un bit de solo lectura cuando se comparte un archivo entre los clientes NFS y los clientes SMB. Parte del software, cuando lo utilizan los clientes NFS y clientes SMB, requiere que se habilite el bit de solo lectura.

Para que ONTAP mantenga los permisos de lectura y escritura adecuados en un archivo compartido entre clientes NFS y clientes SMB, trata el bit de solo lectura de acuerdo con las siguientes reglas:

- NFS trata cualquier archivo con el bit de solo lectura habilitado como si no tiene bits de permiso de escritura habilitados.
- Si un cliente NFS deshabilita todos los bits de permiso de escritura y al menos uno de esos bits se había habilitado anteriormente, ONTAP habilita el bit de solo lectura para ese archivo.
- Si un cliente NFS habilita algún bit de permiso de escritura, ONTAP deshabilita el bit de solo lectura para

ese archivo.

- Si se habilita el bit de solo lectura de un archivo y un cliente NFS intenta detectar permisos para el archivo, los bits de permiso del archivo no se envían al cliente NFS; en su lugar, ONTAP envía los bits de permiso al cliente NFS con los bits de permiso de escritura enmascarados.
- Si se habilita el bit de solo lectura de un archivo y un cliente SMB deshabilita el bit de solo lectura, ONTAP habilita el bit de permiso de escritura del propietario para el archivo.
- Los archivos con el bit de sólo lectura activado sólo son grabables por raíz.

El bit de solo lectura interactúa con los bits de modo ACL y Unix de las siguientes maneras:

Cuando el bit de solo lectura está configurado en un archivo:

- No se realizan cambios en la ACL de ese archivo. Los clientes NFS verán la misma ACL que antes de configurar el bit de solo lectura.
- Se ignoran todos los bits del modo Unix que permiten acceso de escritura al archivo.
- Tanto los clientes NFS como SMB pueden leer el archivo, pero no pueden modificarlo.
- Las ACL y los bits de modo UNIX se ignoran en favor del bit de solo lectura. Esto significa que, incluso si la ACL permite el acceso de escritura, el bit de solo lectura impide las modificaciones.

Cuando el bit de solo lectura no está configurado en un archivo:

- ONTAP determina el acceso según los bits de modo ACL y UNIX.
  - Si los bits del modo ACL o UNIX niegan el acceso de escritura, los clientes NFS y SMB no pueden modificar el archivo.
  - Si ni los bits del modo ACL ni los del modo UNIX niegan el acceso de escritura, los clientes NFS y SMB pueden modificar el archivo.

> Los cambios en los permisos de archivo se aplican inmediatamente en los clientes SMB, pero es posible que no se apliquen de inmediato en los clientes NFS si el cliente NFS habilita el almacenamiento de atributos en caché.

Diferencias entre ONTAP y Windows en el manejo de bloqueos en componentes de ruta de acceso compartida

A diferencia de Windows, ONTAP no bloquea cada componente de la ruta de acceso a un archivo abierto mientras el archivo está abierto. Este comportamiento también afecta a las rutas de recursos compartidos de SMB.

Como ONTAP no bloquea cada componente de la ruta, es posible cambiar el nombre de un componente de ruta por encima del archivo o el recurso compartido abierto, lo que puede provocar problemas en determinadas aplicaciones o hacer que la ruta del recurso compartido en la configuración del SMB no sea válida. Esto puede hacer que el recurso compartido sea inaccesible.

Para evitar problemas causados por el cambio de nombre de los componentes de la ruta de acceso, puede aplicar configuraciones de seguridad que impidan que los usuarios o aplicaciones cambien el nombre de los directorios críticos.

Mostrar información sobre los bloqueos SMB de ONTAP

Puede mostrar información acerca de los bloqueos de archivos actuales, incluidos los tipos de bloqueos que se conservan y el estado de bloqueo, detalles sobre bloqueos de

rango de bytes, modos sharelock, bloqueos de delegación y bloqueos oportunistas, y si se abren bloqueos con identificadores duraderos o persistentes.

Acerca de esta tarea

No se puede mostrar la dirección IP del cliente para los bloqueos establecidos a través de NFSv4 o NFSv4.1.

De forma predeterminada, el comando muestra información sobre todos los bloqueos. Puede usar los parámetros del comando para mostrar información sobre los bloqueos de una máquina virtual de almacenamiento (SVM) específica o para filtrar el resultado del comando según otros criterios.

El `vserver locks show` comando muestra información sobre cuatro tipos de bloqueos:

- Bloqueos de rango de bytes, que bloquean sólo una parte de un archivo.
- Bloqueos de uso compartido, que bloquean los archivos abiertos.
- Bloqueos oportunistas, que controlan el almacenamiento en caché en el cliente a través de SMB.
- Delegaciones, que controlan el almacenamiento en caché en el cliente a través de NFSv4.x.

Al especificar parámetros opcionales, puede determinar información importante sobre cada tipo de bloqueo. Obtenga más información sobre `vserver locks show` en el "Referencia de comandos del ONTAP".

Paso

1. Muestra información sobre los bloqueos mediante `vserver locks show` el comando.

Ejemplos

El siguiente ejemplo muestra información de resumen para un bloqueo NFSv4 en un archivo con la ruta `/vol1/file1`. El modo de acceso sharelock es write-deny_none, y el bloqueo se concedió mediante la delegación de escritura:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                         delegation  -
               Delegation Type: write
```

El siguiente ejemplo muestra información detallada sobre el bloqueo operativo y el bloqueo compartido sobre el bloqueo SMB en un archivo con la ruta de acceso `/data2/data2_2/intro.pptx`. Se concede un identificador duradero en el archivo con un modo de acceso de bloqueo compartido de Write-Deny_none a un cliente con una dirección IP de 10.3.1.3. Un plock de arrendamiento se concede con un nivel de plock por lotes:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx
```

```
                  Vserver: vs1
                   Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
             Lock Protocol: cifs
                 Lock Type: share-level
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                  Vserver: vs1
                   Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/test.pptx
                 Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
             Lock Protocol: cifs
                 Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
```

```
              SMB Open Type: -
          SMB Connect State: connected
SMB Expiration Time (Secs): -
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Romper los bloqueos SMB de ONTAP

Cuando los bloqueos de archivos impiden que los clientes accedan a los archivos, puede mostrar información sobre los bloqueos retenidos actualmente y romperán bloqueos específicos. Entre los ejemplos de escenarios en los que es posible que necesite romper los bloqueos se incluyen las aplicaciones de depuración.

Acerca de esta tarea

`vserver locks break`El comando solo está disponible en el nivel de privilegios avanzado y superior. Obtenga más información sobre `vserver locks break` en el link:https://docs.netapp.com/us-en/ontap-cli/vserver-locks-break.html["Referencia de comandos del ONTAP"^].

Pasos

1. Para encontrar la información que necesita para romper un bloqueo, utilice el `vserver locks show` comando.

   Obtenga más información sobre `vserver locks show` en el "Referencia de comandos del ONTAP".

2. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
3. Ejecute una de las siguientes acciones:

Si desea romper un bloqueo especificando…	Introduzca el comando…
El nombre de SVM, el nombre del volumen, el nombre de LIF y la ruta de archivo	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
El ID del bloqueo	`vserver locks break -lockid UUID`

4. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

Supervise la actividad del SMB

Mostrar información de la sesión SMB de ONTAP

Puede mostrar información acerca de las sesiones SMB establecidas, incluidos la

conexión SMB y el ID de sesión y la dirección IP de la estación de trabajo mediante la sesión. Es posible mostrar información sobre la versión del protocolo SMB de la sesión y el nivel de protección disponible continuamente, lo que ayuda a identificar si la sesión admite operaciones no disruptivas.

Acerca de esta tarea

Puede mostrar información de todas las sesiones de la SVM en formato de resumen. Sin embargo, en muchos casos, la cantidad de producción que se devuelve es grande. Puede personalizar la información que se muestra en el resultado especificando parámetros opcionales:

- Puede utilizar el parámetro opcional `-fields` para mostrar resultados sobre los campos seleccionados.

  Puede introducir `-fields ?` para determinar qué campos puede utilizar.

- Puede usar el `-instance` parámetro para mostrar información detallada acerca de las sesiones SMB establecidas.
- Puede usar `-fields` el parámetro o el `-instance` parámetro solo o en combinación con otros parámetros opcionales.

Paso

1. Ejecute una de las siguientes acciones:

Si desea mostrar información de la sesión SMB…	Introduzca el siguiente comando…
Para todas las sesiones del SVM en formato de resumen	`vserver cifs session show -vserver vserver_name`
En un ID de conexión especificado	`vserver cifs session show -vserver vserver_name -connection-id integer`
Desde una dirección IP de estación de trabajo especificada	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
En una dirección IP de LIF especificada	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
En un nodo especificado	`vserver cifs session show -vserver vserver_name -node {node_name
local}`	Desde un usuario de Windows especificado
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	Con un mecanismo de autenticación especificado

Si desea mostrar información de la sesión SMB…	Introduzca el siguiente comando…
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1	NTLMv2
Kerberos	Anonymous}`
Con una versión de protocolo especificada	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1
SMB2	SMB2_1
SMB3	SMB3_1}`  [NOTE] ==== Protección de disponibilidad continua y multicanal de SMB solo están disponibles en sesiones SMB 3.0 y posteriores. Para ver su estado en todas las sesiones de calificación, debe especificar este parámetro con el valor definido en `SMB3` o posterior. ====
Con un nivel especificado de protección continua disponible	`vserver cifs session show -vserver vserver_name -continuously-available {No
Yes	Partial}`  [NOTE] ==== Si el estado de disponibilidad continua es `Partial`, significa que la sesión contiene al menos un archivo abierto continuamente disponible, pero la sesión tiene algunos archivos que no están abiertos con protección disponible continuamente. Puede usar el `vserver cifs sessions file show` comando para determinar qué archivos de la sesión establecida no están abiertos con la protección disponible continuamente. ====
Con un estado de sesión de firma SMB especificado	`vserver cifs session show -vserver vserver_name -is-session-signed {true

Ejemplos

El siguiente comando muestra información de sesión para las sesiones en SVM vs1 establecidas desde una estación de trabajo con dirección IP 10.1.1.1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

El siguiente comando muestra información detallada de la sesión para las sesiones con protección continuamente disponible en SVM vs1. La conexión se realizó mediante la cuenta de dominio.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                      Node: node1
                   Vserver: vs1
                Session ID: 1
             Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
              Windows User: DOMAIN\SERVER1$
                 UNIX User: pcuser
               Open Shares: 1
                Open Files: 1
                Open Other: 0
            Connected Time: 10m 43s
                 Idle Time: 1m 19s
          Protocol Version: SMB3
      Continuously Available: Yes
          Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

El siguiente comando muestra información de sesión en una sesión mediante SMB 3.0 y SMB MultiChannel en SVM vs1. En el ejemplo, el usuario se conectó a este recurso compartido desde un cliente con capacidad para SMB 3.0 mediante la dirección IP de LIF; por lo tanto, el mecanismo de autenticación se estableció de forma predeterminada en NTLMv2. La conexión se debe realizar mediante la autenticación Kerberos para conectarse con la protección disponible continuamente.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Información relacionada

Mostrar información acerca de los archivos SMB abiertos

Mostrar información sobre archivos SMB de ONTAP abiertos

Es posible ver información sobre los archivos SMB abiertos, incluidos la conexión de SMB y el ID de sesión, el volumen de host, el nombre del recurso compartido y la ruta del recurso compartido. Es posible mostrar información acerca del nivel de protección disponible continuamente de un archivo, lo cual es útil para determinar si un archivo abierto está en un estado que admite operaciones no disruptivas.

Acerca de esta tarea

Puede ver información sobre los archivos abiertos en una sesión de SMB establecida. La información que se muestra es útil cuando necesita determinar la información de la sesión SMB para determinados archivos dentro de una sesión SMB.

Por ejemplo, si tiene una sesión SMB en la que algunos de los archivos abiertos están abiertos con protección disponible continuamente y otros no están abiertos con protección disponible continuamente (el valor `-continuously-available` del campo en `vserver cifs session show` la salida del comando es `Partial`), puede determinar qué archivos no están disponibles continuamente mediante este comando.

Puede mostrar información de todos los archivos abiertos en sesiones SMB establecidas en máquinas virtuales de almacenamiento (SVM) de forma resumida, mediante `vserver cifs session file show` el

comando sin ningún parámetro opcional.

Sin embargo, en muchos casos, la cantidad de producción devuelta es grande. Puede personalizar la información que se muestra en el resultado especificando parámetros opcionales. Esto puede resultar útil si desea ver información sólo de un pequeño subconjunto de archivos abiertos.

- Puede utilizar el parámetro opcional `-fields` para mostrar la salida en los campos seleccionados.

  Es posible usar este parámetro de forma independiente o combinada con otros parámetros opcionales.

- Puede utilizar el `-instance` parámetro para mostrar información detallada sobre los archivos SMB abiertos.

  Es posible usar este parámetro de forma independiente o combinada con otros parámetros opcionales.

Paso

1. Ejecute una de las siguientes acciones:

Si desea mostrar archivos SMB abiertos…	Introduzca el siguiente comando…
En la SVM de forma resumida	`vserver cifs session file show -vserver vserver_name`
En un nodo especificado	`vserver cifs session file show -vserver vserver_name -node {node_name`
local}`	En un ID de archivo especificado
`vserver cifs session file show -vserver vserver_name -file-id integer`	En un ID de conexión de SMB especificado
`vserver cifs session file show -vserver vserver_name -connection-id integer`	En un ID de sesión de SMB especificado
`vserver cifs session file show -vserver vserver_name -session-id integer`	En el agregado de host especificado
`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`	En el volumen especificado
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	En el recurso compartido de SMB especificado

Si desea mostrar archivos SMB abiertos…	Introduzca el siguiente comando…
`vserver cifs session file show -vserver vserver_name -share share_name`	En la ruta del bloque de mensajes del servidor especificada
`vserver cifs session file show -vserver vserver_name -path path`	Con el nivel especificado de protección continua disponible
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}`  [NOTE] ==== Si el estado de disponibilidad continua es `No`, esto significa que estos archivos abiertos no pueden recuperarse sin interrupciones de la toma de control y la devolución. Tampoco pueden recuperarse de la reubicación general de agregados entre partners en una relación de alta disponibilidad. ====
Con el estado reconectado especificado	`vserver cifs session file show -vserver vserver_name -reconnected {No

Existen parámetros opcionales adicionales que se pueden utilizar para refinar los resultados de la salida. Obtenga más información sobre `vserver cifs session file show` en el "Referencia de comandos del ONTAP".

Ejemplos

En el siguiente ejemplo, se muestra información sobre los archivos abiertos en la SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

En el siguiente ejemplo, se muestra información detallada sobre los archivos SMB abiertos con el ID de archivo 82 en la SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
             CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

Información relacionada

Mostrar información de la sesión

Determinar qué estadísticas, objetos y contadores están disponibles en los servidores SMB de ONTAP

Para poder obtener información acerca de las estadísticas de CIFS, SMB, auditoría y BranchCache hash, y supervisar el rendimiento, debe conocer los objetos y contadores disponibles desde los cuales puede obtener datos.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

Si desea determinar…	Introduzca…
Qué objetos están disponibles	`statistics catalog object show`
Objetos específicos disponibles	`statistics catalog object show -object object_name`
Qué contadores están disponibles	`statistics catalog counter show -object object_name`

Obtenga más información sobre `statistics catalog object show`, incluidos los objetos y contadores disponibles, en la "Referencia de comandos del ONTAP"sección .

3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Ejemplos

El siguiente comando muestra descripciones de los objetos de estadísticas seleccionados relacionados con CIFS y acceso SMB en el clúster tal y como se ve en el nivel de privilegio avanzado:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

El siguiente comando muestra información acerca de algunos de los contadores del `cifs` objeto como se ve

en el nivel de privilegio avanzado:

> En este ejemplo no se muestran todos los contadores disponibles para `cifs` el objeto; la salida se trunca.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
-----------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                                vserver_1:10.72.205.179
    instance_uuid                                       2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

Información relacionada

- Mostrar estadísticas
- "Catálogo de estadísticas Contador Mostrar objeto"

- "Las estadísticas comienzan"

Mostrar estadísticas de ONTAP SMB

Puede mostrar varias estadísticas, incluidas estadísticas sobre CIFS y SMB, auditoría y hash de BranchCache, para supervisar el rendimiento y diagnosticar problemas.

Antes de empezar

Debe haber recogido muestras de datos mediante los `statistics start` `statistics stop` comandos y antes de poder mostrar información sobre los objetos.

Obtenga más información sobre `statistics start` y `statistics stop` en el "Referencia de comandos del ONTAP" .

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

Si desea mostrar estadísticas de…	Introduzca…
Todas las versiones de SMB	`statistics show -object cifs`
SMB 1,0	`statistics show -object smb1`
SMB 2.x y SMB 3.0	`statistics show -object smb2`
Subsistema CIFS del nodo	`statistics show -object nblade_cifs`
Auditoría multiprotocolo	`statistics show -object audit_ng`
Servicio hash de BranchCache	`statistics show -object hashd`
DNS dinámico	`statistics show -object ddns_update`

   Obtenga más información sobre `statistics show` en el "Referencia de comandos del ONTAP".

3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Información relacionada

- Determinar qué estadísticas, objetos y contadores están disponibles en los servidores
- Supervisar estadísticas de sesión firmada por SMB
- Muestra las estadísticas de BranchCache
- Utilice estadísticas para supervisar la actividad de referencia automática de nodos
- "Configuración de SMB para Microsoft Hyper-V y SQL Server"
- "Configuración de supervisión del rendimiento"

Ponga en marcha servicios basados en cliente de SMB

Utilice archivos sin conexión para permitir el almacenamiento en caché de archivos para su uso sin conexión

Obtenga información sobre el uso de archivos sin conexión para permitir el almacenamiento en caché de archivos SMB de ONTAP para su uso sin conexión

ONTAP es compatible con la característica Archivos sin conexión de Microsoft, o con la función de almacenamiento en caché del cliente_, que permite almacenar los archivos en caché en el host local para su uso sin conexión. Los usuarios pueden utilizar la funcionalidad de archivos sin conexión para seguir trabajando en archivos incluso cuando están desconectados de la red.

Puede especificar si los documentos y programas de usuario de Windows se almacenan automáticamente en caché en un recurso compartido o si los archivos deben seleccionarse manualmente para almacenar en caché. El almacenamiento en caché manual está habilitado de forma predeterminada para nuevos recursos compartidos. Los archivos que están disponibles sin conexión se sincronizan con el disco local del cliente de Windows. La sincronización se produce cuando se restaura la conectividad de red a un recurso compartido de sistema de almacenamiento específico.

Puesto que los archivos y carpetas sin conexión conservan los mismos permisos de acceso que la versión de los archivos y carpetas guardados en el servidor CIFS, el usuario debe tener suficientes permisos en los archivos y carpetas guardados en el servidor CIFS para realizar acciones en los archivos y carpetas sin conexión.

Cuando el usuario y otra persona de la red realizan cambios en el mismo archivo, el usuario puede guardar la versión local del archivo en la red, conservar la otra versión o guardar ambas. Si el usuario conserva ambas versiones, se guarda localmente un nuevo archivo con los cambios del usuario local y el archivo almacenado en caché se sobrescribe con cambios de la versión del archivo guardado en el servidor CIFS.

Puede configurar archivos sin conexión de forma compartida mediante las opciones de configuración de recursos compartidos. Puede elegir una de las cuatro configuraciones de carpetas sin conexión al crear o modificar recursos compartidos:

- Sin almacenamiento en caché

  Deshabilita el almacenamiento en caché en el cliente para el recurso compartido. Los archivos y carpetas no se almacenan automáticamente en caché local en clientes y los usuarios no pueden optar por almacenar en caché archivos o carpetas localmente.

- Almacenamiento en caché manual

  Permite la selección manual de archivos para almacenar en caché en el recurso compartido. Esta es la configuración predeterminada. De forma predeterminada, no se almacenan en caché archivos ni carpetas en el cliente local. Los usuarios pueden elegir los archivos y carpetas que desean almacenar en caché localmente para utilizarlos sin conexión.

- Almacenamiento automático de documentos en caché

  Permite que los documentos de usuario se almacenen automáticamente en caché en el recurso compartido. Sólo los archivos y carpetas a los que se tiene acceso se almacenan en caché localmente.

- Almacenamiento automático de programas en caché

Permite que los programas y los documentos de usuario se almacenen automáticamente en caché en el recurso compartido. Sólo los archivos, carpetas y programas a los que se tiene acceso se almacenan en caché localmente. Además, esta configuración permite al cliente ejecutar ejecutables almacenados localmente en caché incluso cuando se conecta a la red.

Para obtener más información acerca de la configuración de archivos sin conexión en servidores y clientes de Windows, consulte la biblioteca de Microsoft TechNet.

Información relacionada

- Uso de perfiles de itinerancia para almacenar perfiles de usuario de forma centralizada en un servidor CIFS asociado con la SVM
- Aprenda a utilizar la redirección de carpetas para almacenar datos en servidores
- Obtenga información sobre cómo usar BranchCache para almacenar en caché contenido compartido en una sucursal
- "Biblioteca de Microsoft TechNet: technet.microsoft.com/en-us/library/"

Conozca los requisitos para usar archivos SMB de ONTAP sin conexión

Antes de poder utilizar la función Microsoft Offline Files con el servidor CIFS, debe conocer las versiones de ONTAP y SMB y los clientes Windows que admiten la función.

Requisitos de versión de ONTAP

Las versiones ONTAP admiten archivos sin conexión.

Requisitos de la versión del protocolo SMB

Para las máquinas virtuales de almacenamiento (SVM), ONTAP admite archivos sin conexión en todas las versiones de SMB.

Requisitos del cliente Windows

El cliente Windows debe admitir los archivos sin conexión.

Para obtener la información más reciente sobre los clientes de Windows que admiten la función Archivos sin conexión, consulte la matriz de interoperabilidad.

"mysupport.netapp.com/matrix"

Pautas para implementar archivos SMB de ONTAP sin conexión

Hay algunas directrices importantes que debe comprender al implementar archivos sin conexión en recursos compartidos del directorio principal que tienen la `showsnapshot` propiedad de recurso compartido establecida en los directorios principales.

Si la `showsnapshot` propiedad Compartir se establece en un recurso compartido de directorio principal que tiene configurados archivos sin conexión, los clientes de Windows almacenan en caché todas las instantáneas de `~snapshot` la carpeta en el directorio raíz del usuario.

Los clientes de Windows almacenan en caché todas las snapshots en el directorio inicial si se cumple alguna de las siguientes opciones:

- El usuario hace que el directorio inicial esté disponible sin conexión desde el cliente.

  El contenido de `~snapshot` la carpeta en el directorio principal se incluye y se pone a disposición fuera de línea.

- El usuario configura el redireccionamiento de carpetas para redirigir una carpeta, como `My Documents` la raíz de un directorio inicial que reside en el recurso compartido del servidor CIFS.

  Es posible que algunos clientes de Windows hagan que la carpeta redirigida esté disponible sin conexión automáticamente. Si la carpeta se redirige a la raíz del directorio principal, la `~snapshot` carpeta se incluye en el contenido sin conexión almacenado en caché.

> `~snapshot`Se deben evitar los despliegues de archivos fuera de línea en los que la carpeta se incluya en archivos fuera de línea. Las instantáneas de `~snapshot` la carpeta contienen todos los datos del volumen en el momento en el que ONTAP creó la instantánea. Por lo tanto, la creación de una copia sin conexión de la `~snapshot` carpeta consume un almacenamiento local importante en el cliente, consume ancho de banda de red durante la sincronización de archivos sin conexión y aumenta el tiempo que se tarda en sincronizar los archivos sin conexión.

Comandos ONTAP para configurar la compatibilidad con archivos SMB sin conexión

Puede configurar la compatibilidad de archivos sin conexión mediante la interfaz de línea de comandos de ONTAP especificando una de las cuatro archivos sin conexión al crear recursos compartidos de SMB o en cualquier momento modificando los recursos compartidos de SMB existentes. La compatibilidad con archivos manuales sin conexión es la configuración predeterminada.

Acerca de esta tarea

Al configurar el soporte de archivos sin conexión, puede elegir una de las siguientes cuatro opciones de archivos sin conexión:

Ajuste	Descripción
`none`	Despermite a los clientes de Windows almacenar en caché cualquier archivo en este recurso compartido.
`manual`	Permite a los usuarios de clientes de Windows seleccionar manualmente los archivos que se van a almacenar en caché.
`documents`	Permite a los clientes de Windows almacenar en caché los documentos de usuario utilizados por el usuario para el acceso sin conexión.

Ajuste	Descripción
`programs`	Permite a los clientes de Windows almacenar en caché programas que utilizan el usuario para el acceso sin conexión. Los clientes pueden utilizar los archivos de programa almacenados en caché en modo sin conexión incluso si el recurso compartido está disponible.

Sólo puede seleccionar una configuración de archivo sin conexión. Si modifica una configuración de archivos sin conexión en un recurso compartido SMB existente, la opción nuevos archivos sin conexión reemplaza la configuración original. Las demás opciones de configuración y propiedades de uso compartido de SMB existentes no se eliminan ni se reemplazan. Permanecen vigentes hasta que se eliminan o cambian explícitamente.

Pasos

1. Ejecute la acción adecuada:

Si desea configurar archivos sin conexión en…	Introduzca el comando…
Un nuevo recurso compartido de SMB	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none
manual	documents
programs}`	Un recurso compartido de SMB existente
`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none	manual
documents	programs}`

2. Compruebe que la configuración del recurso compartido de SMB sea correcta: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Ejemplo

El siguiente comando crea un recurso compartido SMB denominado «ata1» con los archivos fuera de línea establecidos en `documents`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                Share Properties: oplocks
                                  browsable
                                  changenotify
              Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: Offline files
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: documents
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

El siguiente comando modifica un recurso compartido SMB existente llamado “ata1” cambiando la configuración de archivos fuera de línea a `manual` y agregando valores para la máscara de creación de modo de archivo y directorio:

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
          CIFS Server NetBIOS Name: VS1
                             Path: /data1
                  Share Properties: oplocks
                                    browsable
                                    changenotify
                Symlink Properties: enable
           File Mode Creation Mask: 644
      Directory Mode Creation Mask: 777
                   Share Comment: Offline files
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                      Volume Name: -
                   Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Información relacionada

Agregar o eliminar propiedades de recursos compartidos en recursos compartidos existentes

Configurar la compatibilidad de archivos sin conexión en los recursos compartidos SMB de ONTAP mediante la MMC de administración del equipo

Si desea permitir a los usuarios almacenar en caché archivos localmente para su uso sin conexión, puede configurar la compatibilidad con archivos sin conexión mediante la MMC de Administración de equipos (Microsoft Management Console).

Pasos

1. Para abrir el MMC en el servidor de Windows, en el Explorador de Windows, haga clic con el botón secundario del mouse (ratón) en el icono del equipo local y, a continuación, seleccione **Administrar**.
2. En el panel izquierdo, seleccione **Administración de equipos**.
3. Seleccione **Acción** > **conectar a otro ordenador**.

   Aparece el cuadro de diálogo Seleccionar equipo.

4. Escriba el nombre del servidor CIFS o haga clic en **examinar** para buscar el servidor CIFS.

   Si el nombre del servidor CIFS es el mismo que el nombre de host de máquina virtual de almacenamiento (SVM), escriba el nombre de SVM. Si el nombre del servidor CIFS es diferente del nombre de host de la

SVM, escriba el nombre del servidor CIFS.

5. Haga clic en **OK**.
6. En el árbol de la consola, haga clic en **Herramientas del sistema** > **carpetas compartidas**.
7. Haga clic en **comparticiones**.
8. En el panel de resultados, haga clic con el botón derecho en el recurso compartido.
9. Haga clic en **Propiedades**.

   Se mostrarán las propiedades del recurso compartido seleccionado.

10. En la ficha **General**, haga clic en **Configuración sin conexión**.

    Se muestra el cuadro de diálogo Configuración sin conexión.

11. Configure las opciones de disponibilidad sin conexión según corresponda.
12. Haga clic en **OK**.

Use perfiles de itinerancia para almacenar perfiles de usuario de forma centralizada en un servidor SMB asociado con la SVM

Obtenga información sobre el uso de perfiles móviles para almacenar perfiles de usuarios de ONTAP SMB de forma centralizada

ONTAP admite el almacenamiento de perfiles de itinerancia de Windows en un servidor CIFS asociado con la máquina virtual de almacenamiento (SVM). La configuración de perfiles de itinerancia de usuario ofrece ventajas al usuario, como la disponibilidad automática de recursos, independientemente de dónde se conecte el usuario. Los perfiles de itinerancia también simplifican la administración y gestión de los perfiles de usuario.

Los perfiles de usuario móviles tienen las siguientes ventajas:

- Disponibilidad de recursos automática

  El perfil único de un usuario está automáticamente disponible cuando ese usuario inicia sesión en cualquier equipo de la red que ejecuta Windows 8, Windows 7, Windows 2000 o Windows XP. Los usuarios no necesitan crear un perfil en cada equipo que utilizan en una red.

- Sustitución simplificada del ordenador

  Dado que toda la información del perfil del usuario se mantiene por separado en la red, el perfil de un usuario se puede descargar fácilmente en un equipo nuevo y de repuesto. Cuando el usuario inicia sesión en el nuevo equipo por primera vez, la copia del servidor del perfil del usuario se copia en el nuevo equipo.

Información relacionada

- Obtenga información sobre el uso de archivos sin conexión para permitir el almacenamiento en caché de archivos para su uso sin conexión
- Aprenda a utilizar la redirección de carpetas para almacenar datos en servidores

Conozca los requisitos para usar perfiles SMB de roaming de ONTAP

Antes de poder utilizar los perfiles de itinerancia de Microsoft en su servidor CIFS, necesita saber qué versiones de ONTAP y SMB y qué clientes de Windows admiten esta función.

Requisitos de versión de ONTAP

ONTAP admite perfiles de itinerancia.

Requisitos de la versión del protocolo SMB

En el caso de máquinas virtuales de almacenamiento (SVM), ONTAP admite perfiles de itinerancia en todas las versiones de SMB.

Requisitos del cliente Windows

Para que un usuario pueda utilizar los perfiles de itinerancia, el cliente de Windows debe admitir la función.

Para obtener la información más reciente acerca de los clientes de Windows que admiten perfiles de itinerancia, consulte matriz de interoperabilidad.

"Herramienta de matriz de interoperabilidad de NetApp"

Configurar perfiles SMB de ONTAP móviles a través de la MMC Usuarios y equipos de Active Directory

Si desea que el perfil de un usuario esté disponible automáticamente cuando este inicie sesión en cualquier equipo de la red, puede configurar perfiles de itinerancia a través del complemento MMC Usuarios y equipos de Active Directory. Si está configurando perfiles de itinerancia en Windows Server, puede utilizar el Centro de administración de Active Directory.

Pasos

1. En el servidor Windows, abra el MMC de Usuarios y equipos de Active Directory (o el Centro de administración de Active Directory en servidores Windows).
2. Busque el usuario para el que desea configurar un perfil de itinerancia.
3. Haga clic con el botón derecho del ratón en el usuario y haga clic en **Propiedades**.
4. En la pestaña **Perfil**, ingresa la ruta de perfil al recurso compartido donde deseas almacenar el perfil de roaming del usuario, seguido de `%username%`.

   Por ejemplo, una ruta de acceso de perfil puede ser la siguiente `\\vs1.example.com\profiles\%username%`: . La primera vez que un usuario inicia sesión, `%username%` se sustituye por el nombre del usuario.

   > En la ruta `\\vs1.example.com\profiles\%username%`, `profiles` es el nombre compartido de un recurso compartido en una máquina virtual de almacenamiento (SVM) VS1 que tiene derechos de control total para todos.

5. Haga clic en **OK**.

Utilice la redirección de carpetas para almacenar datos en un servidor SMB

Aprenda a usar la redirección de carpetas para almacenar datos en servidores SMB de ONTAP

ONTAP admite la redirección de carpetas de Microsoft, lo que permite que los usuarios o administradores redirijan la ruta de una carpeta local a una ubicación en el servidor CIFS. Parece que si las carpetas redirigidas se almacenan en el cliente local de Windows, aunque los datos se almacenen en un recurso compartido de SMB.

La redirección de carpetas está destinada principalmente a las empresas que ya han implementado directorios iniciales y que desean mantener la compatibilidad con su entorno de directorio raíz existente.

- `Documents`, , `Desktop` y `Start Menu` son ejemplos de carpetas que puede redirigir.
- Los usuarios pueden redirigir carpetas desde su cliente Windows.
- Los administradores pueden configurar y administrar centralmente la redirección de carpetas configurando GPO en Active Directory.
- Si los administradores han configurado perfiles de itinerancia, la redirección de carpetas permite a los administradores dividir los datos de usuario de los datos de perfil.
- Los administradores pueden usar la redirección de carpetas y los archivos sin conexión juntos para redirigir el almacenamiento de datos de carpetas locales al servidor CIFS, permitiendo a los usuarios almacenar el contenido en la memoria caché localmente.

Información relacionada

- Obtenga información sobre el uso de archivos sin conexión para permitir el almacenamiento en caché de archivos para su uso sin conexión
- Uso de perfiles de itinerancia para almacenar perfiles de usuario de forma centralizada en un servidor CIFS asociado con la SVM

Conozca los requisitos para usar la redirección de carpetas SMB de ONTAP

Para poder utilizar la redirección de carpetas de Microsoft con el servidor CIFS, debe conocer las versiones de ONTAP y SMB y los clientes de Windows que admiten la función.

Requisitos de versión de ONTAP

ONTAP admite redirección de carpetas de Microsoft.

Requisitos de la versión del protocolo SMB

Para la máquina virtual de almacenamiento (SVM), ONTAP admite el redireccionamiento de carpetas de Microsoft en todas las versiones de SMB.

Requisitos del cliente Windows

Para que un usuario pueda utilizar la redirección de carpetas de Microsoft, el cliente de Windows debe admitir la función.

Para obtener la información más reciente acerca de los clientes de Windows que admiten la redirección de carpetas, consulte la matriz de interoperabilidad.

"mysupport.netapp.com/matrix"

Configurar la redirección de carpetas SMB de ONTAP mediante las Propiedades de Windows

Puede configurar la redirección de carpetas mediante la ventana Propiedades de Windows. La ventaja de utilizar este método es que el usuario de Windows puede configurar la redirección de carpetas sin la ayuda del administrador de SVM.

Pasos

1. En el Explorador de Windows, haga clic con el botón secundario en la carpeta que desea redirigir a un recurso compartido de red.
2. Haga clic en **Propiedades**.

   Se mostrarán las propiedades del recurso compartido seleccionado.

3. En la ficha **acceso directo**, haga clic en **destino** y especifique la ruta de acceso a la ubicación de red en la que desea redirigir la carpeta seleccionada.

   Por ejemplo, si desea redirigir una carpeta a la `data` carpeta en un directorio principal asignado a `Q:\`, especifique `Q:\data` como destino.

4. Haga clic en **OK**.

   Para obtener más información acerca de la configuración de carpetas sin conexión, consulte la Biblioteca de Microsoft TechNet.

Información relacionada

"Biblioteca de Microsoft TechNet: technet.microsoft.com/en-us/library/"

Obtenga información sobre cómo acceder al directorio ~snapshot de ONTAP desde clientes Windows mediante SMB 2.x

El método que utiliza para acceder al `~snapshot` directorio desde clientes de Windows con SMB 2.x es diferente del método utilizado para SMB 1,0. Es necesario entender cómo acceder al `~snapshot` directorio cuando se utilizan conexiones SMB 2.x para acceder correctamente a los datos almacenados en instantáneas.

El administrador de SVM controla si los usuarios de clientes de Windows pueden ver `~snapshot` el directorio en un recurso compartido y acceder a él; para ello, habilita o deshabilita la `showsnapshot` propiedad de recurso compartido mediante comandos de las familias de propiedades de recurso compartido cifs de Vserver.

Cuando `showsnapshot` se deshabilita la propiedad Compartir, un usuario de un cliente Windows que utiliza SMB 2.x no puede ver `~snapshot` el directorio y no puede acceder a las instantáneas dentro del `~snapshot` directorio, incluso cuando se introduce manualmente la ruta de acceso al `~snapshot` directorio o a instantáneas específicas dentro del directorio.

Cuando `showsnapshot` se habilita la propiedad de recurso compartido, un usuario en un cliente de Windows que utiliza SMB 2.x aún no puede ver `~snapshot` el directorio en la raíz del recurso compartido ni dentro de ninguna unión o directorio debajo de la raíz del recurso compartido. Sin embargo, después de conectarse a un recurso compartido, el usuario puede acceder al `~snapshot` directorio oculto anexando manualmente `\~snapshot` al final de la ruta de acceso al recurso compartido. `~snapshot`Se puede acceder al directorio oculto desde dos puntos de entrada:

- En la raíz del recurso compartido
- En cada punto de unión del espacio compartido

> `~snapshot`No se puede acceder al directorio oculto desde subdirectorios que no son de unión dentro del recurso compartido.

Ejemplo

Con la configuración que se muestra en el siguiente ejemplo, un usuario en un cliente Windows con una conexión SMB 2.x al recurso compartido «`eng`» puede acceder al `~snapshot` directorio agregando manualmente `\~snapshot` a la ruta de acceso de recurso compartido en la raíz del recurso compartido y en cada punto de unión de la ruta. `~snapshot`Se puede acceder al directorio oculto desde las tres rutas siguientes:

- `\\vs1\eng\~snapshot`
- `\\vs1\eng\projects1\~snapshot`
- `\\vs1\eng\projects2\~snapshot`

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume       junction-path
------- ------------ ----------------------------------------
vs1     vs1_root      /
vs1     vs1_vol1      /eng
vs1     vs1_vol2      /eng/projects1
vs1     vs1_vol3      /eng/projects2

cluster1::> vserver cifs share show
Vserver  Share   Path     Properties    Comment  ACL
-------- ------  -------  ----------    -------- ----------
vs1      eng     /eng     oplocks       -        Everyone / Full Control
                          changenotify
                          browsable
                          showsnapshot
```

Recupere archivos y carpetas con versiones anteriores

Obtenga información sobre cómo recuperar archivos y carpetas SMB de ONTAP usando versiones anteriores

La posibilidad de utilizar versiones anteriores de Microsoft es aplicable a sistemas de archivos que admitan instantáneas de algún tipo y las tienen habilitadas. La tecnología Snapshot forma parte de ONTAP. Los usuarios pueden recuperar archivos y carpetas de snapshots desde su cliente de Windows usando la función de versiones anteriores de Microsoft.

La funcionalidad de versiones anteriores ofrece un método para que los usuarios naveguen por las

instantáneas o restauren datos desde una snapshot sin intervención de un administrador de almacenamiento. Las versiones anteriores no se pueden configurar. Está siempre habilitada. Si el administrador de almacenamiento ha puesto instantáneas disponibles en un recurso compartido, el usuario puede utilizar versiones anteriores para realizar las siguientes tareas:

- Recuperar archivos eliminados accidentalmente.
- Recuperación de la sobrescritura accidental de un archivo.
- Compare las versiones del archivo mientras está trabajando.

Los datos almacenados en snapshots son de solo lectura. Los usuarios deben guardar una copia de un archivo en otra ubicación para realizar cualquier cambio en el archivo. Las instantáneas se eliminan periódicamente; por lo tanto, los usuarios necesitan crear copias de los archivos contenidos en versiones anteriores si desean conservar indefinidamente una versión anterior de un archivo.

Requisitos de ONTAP SMB para usar versiones anteriores de Microsoft

Antes de poder utilizar las versiones anteriores con el servidor CIFS, debe conocer qué versiones de ONTAP y SMB, y qué clientes de Windows, admiten. También debe conocer el requisito de configuración de la snapshot.

Requisitos de versión de ONTAP

Admite versiones anteriores.

Requisitos de la versión del protocolo SMB

Para las máquinas virtuales de almacenamiento (SVM), ONTAP admite las versiones anteriores de todas las versiones de SMB.

Requisitos del cliente Windows

Para que un usuario pueda utilizar versiones anteriores para acceder a los datos en instantáneas, el cliente Windows debe admitir la función.

Para obtener la información más reciente sobre los clientes de Windows compatibles con versiones anteriores, consulte matriz de interoperabilidad.

"Herramienta de matriz de interoperabilidad de NetApp"

Requisitos para la configuración de Snapshot

Para usar versiones anteriores para acceder a los datos de las snapshots, se debe asociar una política Snapshot habilitada al volumen que contiene los datos, los clientes deben poder acceder a los datos de las snapshots y deben existir snapshots.

Vea y administre datos de instantáneas de ONTAP SMB con la pestaña Versiones anteriores de Windows

Los usuarios de máquinas cliente Windows pueden usar la pestaña Versiones anteriores de la ventana Propiedades de Windows para restaurar los datos almacenados en snapshots sin necesidad de involucrar al administrador de máquinas virtuales de almacenamiento (SVM).

Acerca de esta tarea

Solo puede utilizar la pestaña Versiones anteriores para ver y gestionar datos en instantáneas de datos almacenados en la SVM si el administrador ha habilitado snapshots en el volumen que contiene el recurso compartido y si el administrador configura el recurso compartido para mostrar las snapshots.

Pasos

1. En el Explorador de Windows, muestre el contenido de la unidad asignada de los datos almacenados en el servidor CIFS.
2. Haga clic con el botón derecho en el archivo o carpeta de la unidad de red asignada cuyas instantáneas desea ver o gestionar.
3. Haga clic en **Propiedades**.

   Se muestran las propiedades del archivo o carpeta seleccionado.

4. Haga clic en la ficha **versiones anteriores**.

   En el cuadro Versiones de carpeta se muestra una lista de instantáneas disponibles del archivo o carpeta seleccionado. Las copias de Snapshot enumeradas se identifican con el prefijo del nombre de la snapshot y la fecha/hora de creación.

5. En el cuadro **versiones de carpeta:**, haga clic con el botón secundario del mouse (ratón) en la copia del archivo o carpeta que desee administrar.
6. Ejecute la acción adecuada:

Si desea…	Haga lo siguiente…
Ver datos de esa instantánea	Haga clic en **Abrir**.
Cree una copia de datos a partir de esa instantánea	Haga clic en **Copiar**.

   Los datos de las copias Snapshot son de solo lectura. Si desea realizar modificaciones en los archivos y carpetas enumerados en la ficha versiones anteriores, debe guardar una copia de los archivos y carpetas que desea modificar en una ubicación editable y realizar modificaciones en las copias.

7. Cuando termine de administrar los datos de las instantáneas, cierre el cuadro de diálogo **Propiedades** haciendo clic en **Aceptar**.

   Para obtener más información sobre el uso de la pestaña Versiones anteriores para ver y administrar datos de instantáneas, consulte la biblioteca de Microsoft TechNet.

Información relacionada

"Biblioteca de Microsoft TechNet: technet.microsoft.com/en-us/library/"

Determinar si las instantáneas SMB de ONTAP están disponibles para el uso de versiones anteriores

Las snapshots se pueden ver en la pestaña Versiones anteriores solo si se aplica una política de Snapshot habilitada al volumen que contiene el recurso compartido y si la configuración del volumen permite el acceso a las instantáneas. Determinar la disponibilidad de instantáneas es útil cuando se ayuda a un usuario con acceso a versiones anteriores.

Pasos

1. Determine si el volumen en el que residen los datos compartidos tiene snapshots automáticas habilitadas y si los clientes tienen acceso a los directorios de snapshots: `volume show -vserver vserver-name -volume volume-name -fields vserver,volume,snapdir-access,snapshot-policy,snapshot-count`

   La salida muestra qué política de instantáneas está asociada con el volumen, si el acceso al directorio de instantáneas del cliente está habilitado y el número de instantáneas disponibles.

2. Determinar si la política de snapshots asociada está habilitada: `volume snapshot policy show -policy policy-name`
3. Enumere las instantáneas disponibles: `volume snapshot show -volume volume_name`

   Para obtener más información sobre la configuración y gestión de políticas de snapshot y programaciones de snapshot, consulte "Protección de datos".

Ejemplo

El siguiente ejemplo muestra información sobre las políticas de instantáneas asociadas con el volumen denominado «ata1» que contiene los datos compartidos y las instantáneas disponibles en «ata1».

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-------- ------ -------------- --------------- --------------
vs1      data1  true           default         10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1
                   Number of Is
Policy Name        Schedules Enabled Comment
------------------ --------- ------- ---------------------------------
default                   3 true    Default policy with hourly, daily &
weekly schedules.
    Schedule         Count     Prefix                  SnapMirror Label
    ---------------- -----     ----------------------- -------------------
    hourly               6     hourly                  -
    daily                2     daily                   daily
    weekly               2     weekly                  weekly

cluster1::> volume snapshot show -volume data1
                                                                 ---Blocks---
Vserver  Volume  Snapshot                  State        Size Total% Used%
-------- ------- ------------------------- -------- -------- ------ -----
vs1      data1
                 weekly.2012-12-16_0015    valid       408KB     0%    1%
                 daily.2012-12-22_0010     valid       420KB     0%    1%
                 daily.2012-12-23_0010     valid       192KB     0%    0%
                 weekly.2012-12-23_0015    valid       360KB     0%    1%
                 hourly.2012-12-23_1405    valid       196KB     0%    0%
                 hourly.2012-12-23_1505    valid       196KB     0%    0%
                 hourly.2012-12-23_1605    valid       212KB     0%    0%
                 hourly.2012-12-23_1705    valid       136KB     0%    0%
                 hourly.2012-12-23_1805    valid       200KB     0%    0%
                 hourly.2012-12-23_1905    valid       184KB     0%    0%
```

Información relacionada

- Crear configuraciones de instantáneas para habilitar el acceso a versiones anteriores
- "Protección de datos"

Cree configuraciones de instantáneas de ONTAP SMB para habilitar el acceso a versiones anteriores

La funcionalidad de las versiones anteriores está siempre disponible, siempre que el acceso del cliente a las instantáneas esté activado y siempre que existan instantáneas. Si la configuración de Snapshot no cumple estos requisitos, puede crear una configuración de Snapshot que sí lo cumpla.

Pasos

1. Si el volumen que contiene el recurso compartido al que desea permitir el acceso a las versiones anteriores no tiene una política Snapshot asociada, asocie una política de Snapshot al volumen y habilite dicha política con el `volume modify` comando.

   Obtenga más información sobre `volume modify` en el "Referencia de comandos del ONTAP".

2. Permita el acceso a las instantáneas mediante `volume modify` el comando para establecer `-snap-dir` la opción en `true`.

   Obtenga más información sobre `volume modify` en el "Referencia de comandos del ONTAP".

3. Comprobar que las políticas de Snapshot están habilitadas y que el acceso a los directorios de snapshots está habilitado mediante `volume show` los comandos y. `volume snapshot policy show`

   Obtenga más información sobre `volume show` y `volume snapshot policy show` en el "Referencia de comandos del ONTAP".

   Para obtener más información sobre la configuración y gestión de políticas de snapshot y programaciones de snapshot, consulte "Protección de datos".

Información relacionada

"Protección de datos"

Obtenga información sobre cómo restaurar directorios de versiones anteriores que contienen uniones SMB de ONTAP

Hay ciertas directrices que debe tener en cuenta al utilizar versiones anteriores para restaurar carpetas que contienen puntos de unión.

Al utilizar versiones anteriores para restaurar carpetas que tienen carpetas secundarias que son puntos de unión, la restauración puede fallar y `Access Denied` generar un error.

Puede determinar si la carpeta que intenta restaurar contiene una unión mediante `vol show` el uso del comando con `-parent` la opción. También puede usar `vserver security trace` los comandos para crear registros detallados sobre problemas de acceso a archivos y carpetas.

Información relacionada

Crear y gestionar volúmenes de datos en espacios de nombres NAS

Ponga en marcha servicios basados en servidor de SMB

Administrar directorios iniciales

Obtenga información sobre cómo habilitar directorios de inicio dinámicos en servidores SMB de ONTAP

Los directorios iniciales de ONTAP permiten configurar un recurso compartido de SMB que se asigna a directorios diferentes en función del usuario que se conecta a él y a un conjunto de variables. En lugar de crear recursos compartidos independientes para cada usuario, puede configurar un recurso compartido con algunos parámetros del directorio inicial para definir la relación de un usuario entre un punto de entrada (el recurso compartido) y el directorio inicial (un directorio en la SVM).

Un usuario que ha iniciado sesión como usuario invitado no tiene un directorio principal y no puede acceder a los directorios iniciales de otros usuarios. Existen cuatro variables que determinan cómo se asigna un usuario a un directorio:

- **Nombre del recurso compartido**

  Éste es el nombre del recurso compartido que se crea al que se conecta el usuario. Debe establecer la propiedad del directorio principal para este recurso compartido.

  El nombre del recurso compartido puede utilizar los siguientes nombres dinámicos:

  - `%w` (Nombre de usuario de Windows del usuario)
  - `%d` (Nombre de dominio de Windows del usuario)
  - `%u` (Nombre de usuario UNIX asignado al usuario) Para que el nombre del recurso compartido sea único en todos los directorios raíz, el nombre del recurso compartido debe contener/`%w` `%u` la variable o. El nombre del recurso compartido puede contener tanto la `%d`/`%w` variable como la variable (por ejemplo, `%d`/`%w`), o el nombre del recurso compartido puede contener una parte estática y una parte variable (por ejemplo, home_/`%w`).

- **Compartir ruta**

  Esta es la ruta relativa, que define el recurso compartido y, por lo tanto, está asociada con uno de los nombres de recurso compartido, que se anexa a cada ruta de búsqueda para generar toda la ruta de directorio inicial del usuario desde la raíz de la SVM. Puede ser estático (por ejemplo `home`,), dinámico (por ejemplo, `%w`) o una combinación de ambos (por ejemplo, `eng/%w`).

- **Rutas de búsqueda**

  Este es el conjunto de rutas absolutas desde la raíz de la SVM que especifique que dirige la búsqueda ONTAP de directorios iniciales. Puede especificar una o más rutas de búsqueda mediante `vserver cifs home-directory search-path add` el comando. Si especifica varias rutas de búsqueda, ONTAP las intenta en el orden especificado hasta que encuentre una ruta válida. Obtenga más información sobre `vserver cifs home-directory search-path add` en el "Referencia de comandos del ONTAP".

- **Directorio**

  Éste es el directorio principal del usuario que se crea para el usuario. El nombre del directorio suele ser el nombre del usuario. Debe crear el directorio principal en uno de los directorios definidos por las rutas de búsqueda.

Por ejemplo, considere la siguiente configuración:

- Usuario: John Smith
- Dominio de usuario: acme
- Nombre de usuario: Jsmith
- Nombre de SVM: vs1
- Nombre compartido del directorio inicial #1: Home_ `%w` - Ruta de acceso compartida: `%w`
- Nombre compartido del directorio inicial #2: `%w` - Ruta de acceso compartida: `%d/%w`
- Ruta de búsqueda #1: `/vol0home/home`

- Ruta de búsqueda #2: `/vol1home/home`
- Ruta de búsqueda #3: `/vol2home/home`
- Directorio inicial: `/vol1home/home/jsmith`

Escenario 1: El usuario se conecta a `\\vs1\home_jsmith`. Esto coincide con el primer nombre compartido del directorio raíz y genera la ruta de acceso relativa `jsmith` . ONTAP ahora busca un directorio llamado `jsmith` comprobando cada ruta de búsqueda en orden:

- `/vol0home/home/jsmith` no existe; pasando a la ruta de búsqueda #2.
- `/vol1home/home/jsmith` existe; por lo tanto, la ruta de búsqueda #3 no está seleccionada; el usuario está ahora conectado a su directorio principal.

Escenario 2: El usuario se conecta a `\\vs1\jsmith`. Esto coincide con el segundo nombre compartido del directorio raíz y genera la ruta de acceso relativa `acme/jsmith` . ONTAP ahora busca un directorio llamado `acme/jsmith` comprobando cada ruta de búsqueda en orden:

- `/vol0home/home/acme/jsmith` no existe; pasando a la ruta de búsqueda #2.
- `/vol1home/home/acme/jsmith` no existe; pasando a la ruta de búsqueda #3.
- `/vol2home/home/acme/jsmith` no existe; el directorio principal no existe; por lo tanto, la conexión falla.

Recursos compartidos de directorios iniciales

Agregar recursos compartidos del directorio de inicio SMB de ONTAP

Si desea utilizar la característica de directorio inicial SMB, debe agregar al menos un recurso compartido con la propiedad de directorio principal incluida en las propiedades de recurso compartido.

Acerca de esta tarea

Puede crear un recurso compartido de directorio inicial en el momento de crear el recurso compartido mediante `vserver cifs share create` el comando, o bien puede cambiar un recurso compartido existente en un recurso compartido de directorio inicial en cualquier momento con `vserver cifs share modify` el comando.

Para crear un recurso compartido de directorio inicial, debe incluir `homedirectory` el valor en `-share -properties` la opción al crear o modificar un recurso compartido. Puede especificar el nombre de recurso compartido y la ruta de acceso compartida mediante variables que se amplían dinámicamente cuando los usuarios se conectan a sus directorios iniciales. Las variables disponibles que puede utilizar en la ruta de acceso son `%w`, `%d`, y `%u`, correspondientes al nombre de usuario de Windows, dominio y nombre de usuario UNIX asignado, respectivamente.

Pasos

1. Añadir un recurso compartido de directorio principal:
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties homedirectory[,…]`

   `-vserver vserver` Especifica la máquina virtual de almacenamiento (SVM) habilitada para CIFS en la que se añadirá la ruta de búsqueda.

`-share-name` *share-name* especifica el nombre del recurso compartido del directorio principal.

Además de contener una de las variables necesarias, si el nombre del recurso compartido contiene una de las cadenas literales `%w` , , `%u` o `%d`, debe preceder la cadena literal con un carácter % (porcentaje) para evitar que ONTAP trate la cadena literal como una variable (por ejemplo, `%%w`).

- El nombre del recurso compartido debe contener la `%w` `%u` variable o.
- El nombre del recurso compartido puede contener además la `%d` variable (por ejemplo, `%d/%w`) o una parte estática en el nombre del recurso compartido (por ejemplo, home1_/`%w`).
- Si los administradores utilizan el recurso compartido para conectarse a los directorios principales de otros usuarios o para permitir que los usuarios se conecten a los directorios principales de otros usuarios, el patrón de nombre de recurso compartido dinámico debe ir precedido de una tilde (~).

  El `vserver cifs home-directory modify` se utiliza para activar este acceso estableciendo `-is-home-dirs-access-for-admin-enabled` la opción en `true`) o estableciendo la opción avanzada `-is-home-dirs-access-for-public-enabled` en `true`.

`-path` `path` especifica la ruta relativa al directorio raíz.

`-share-properties homedirectory[,…]` especifica las propiedades de recurso compartido para ese recurso compartido. Debe especificar `homedirectory` el valor. Puede especificar propiedades de recursos compartidos adicionales mediante una lista delimitada por comas.

1. Compruebe que ha agregado correctamente el recurso compartido del directorio inicial mediante `vserver cifs share show` el comando.

Ejemplo

El siguiente comando crea un recurso compartido de directorio raíz denominado `%w`. Las `oplocks` `browsable` `changenotify` propiedades , y share se establecen además de definir la `homedirectory` propiedad share.

> Este ejemplo no muestra el resultado de todos los recursos compartidos de la SVM. La salida está truncada.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory

vs1::> vserver cifs share show -vserver vs1
Vserver    Share    Path         Properties     Comment  ACL
---------- -------- ------------ -------------- -------- -----------
vs1        %w       %w           oplocks        -        Everyone / Full
Control
                                 browsable
                                 changenotify
                                 homedirectory
```

Información relacionada

- Agregar rutas de búsqueda del directorio de inicio
- Requisitos y pautas para el uso de referencias automáticas de nodos en servidores
- Administrar la accesibilidad a los directorios personales de los usuarios

Obtenga información sobre los requisitos únicos de nombre de usuario SMB de ONTAP para recursos compartidos del directorio de inicio

Tenga cuidado de asignar nombres de usuario únicos al crear recursos compartidos de directorios principales mediante las `%w` `%u` variables (nombre de usuario de Windows) o (nombre de usuario de UNIX) para generar recursos compartidos de forma dinámica. El nombre del recurso compartido está asignado al nombre de usuario.

Pueden ocurrir dos problemas cuando el nombre de un recurso compartido estático y el nombre de un usuario son iguales:

- Cuando el usuario enumera los recursos compartidos en un clúster con `net view` el comando, se muestran dos recursos compartidos con el mismo nombre de usuario.
- Cuando el usuario se conecta a ese nombre de recurso compartido, el usuario siempre está conectado al recurso compartido estático y no puede acceder al recurso compartido del directorio principal con el mismo nombre.

Por ejemplo, hay un recurso compartido denominado «'Administrator'» y usted tiene un nombre de usuario «'Administrator'» de Windows. Si crea un recurso compartido de directorio principal y se conecta a dicho recurso compartido, se conecta a la unidad estática "'Administrator'", no a su directorio principal "'Administrator'".

Puede resolver el problema con nombres de recursos compartidos duplicados siguiendo cualquiera de estos pasos:

- Cambiar el nombre del recurso compartido estático para que deje de estar en conflicto con el recurso compartido del directorio principal del usuario.
- Dar al usuario un nuevo nombre de usuario para que no entre en conflicto con el nombre de recurso compartido estático.
- Crear un recurso compartido de directorio raíz CIFS con un nombre estático como «`home`» en lugar de utilizar el `%w` parámetro para evitar conflictos con los nombres del recurso compartido.

Obtenga información sobre qué sucede con los nombres de recursos compartidos del directorio de inicio SMB de ONTAP estático después de la actualización

Los nombres compartidos del directorio inicial deben contener `%w` `%u` la variable dinámica o la variable dinámica. Debe saber qué ocurre con los nombres de recursos compartidos de directorios iniciales estáticos existentes después de actualizar a una versión de ONTAP con el nuevo requisito.

Si la configuración del directorio raíz contiene nombres de recursos compartidos estáticos y se actualiza a ONTAP, los nombres de recursos compartidos de directorio raíz estáticos no se modifican y siguen siendo válidos. Sin embargo, no puede crear ningún recurso compartido nuevo del directorio inicial que no contenga `%w` `%u` la variable o.

Al requerir que se incluya una de estas variables en el nombre del recurso compartido del directorio principal

del usuario se garantiza que cada nombre de recurso compartido sea único en la configuración del directorio principal. Si lo desea, puede cambiar los nombres compartidos del directorio principal estático por nombres que contengan la `%w` `%u` variable o.

Agregar rutas de búsqueda del directorio de inicio de ONTAP SMB

Si desea utilizar directorios iniciales SMB de ONTAP, debe agregar al menos una ruta de búsqueda de directorio raíz.

Acerca de esta tarea

Puede agregar una ruta de búsqueda del directorio inicial utilizando `vserver cifs home-directory search-path add` el comando.

El `vserver cifs home-directory search-path add` comando comprueba la ruta especificada en la `-path` opción durante la ejecución del comando. Si la ruta especificada no existe, el comando genera un mensaje solicitando si desea continuar. Usted elige `y` o `n`. Si decide `y` continuar, ONTAP creará la ruta de búsqueda. Sin embargo, debe crear la estructura de directorios para poder utilizar la ruta de búsqueda en la configuración del directorio principal. Si elige no continuar, el comando falla; no se crea la ruta de búsqueda. A continuación, puede crear la estructura de directorios PATH y volver a ejecutar `vserver cifs home-directory search-path add` el comando.

Pasos

1. Agregar una ruta de búsqueda del directorio inicial: `vserver cifs home-directory search-path add -vserver vserver -path path`
2. Compruebe que ha agregado correctamente la ruta de búsqueda mediante el `vserver cifs home-directory search-path show` comando.

Ejemplo

En el siguiente ejemplo, se agrega la ruta `/home1` a la configuración del directorio inicial en la SVM VS1.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

vs1::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

En el siguiente ejemplo, se intenta añadir la ruta `/home2` a la configuración del directorio inicial en la SVM VS1. La ruta no existe. Se decide no continuar.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home2
Warning: The specified path "/home2" does not exist in the namespace
         belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

Información relacionada

Agregar recursos compartidos del directorio de inicio

Cree configuraciones de directorio de inicio SMB de ONTAP utilizando las variables %w y %d

Puede crear una configuración del directorio inicial mediante `%w` `%d` las variables y. Los usuarios pueden conectarse a su propio recurso compartido mediante recursos compartidos creados dinámicamente.

Pasos

1. Cree un qtree que contenga los directorios iniciales de usuario: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Compruebe que el qtree esté utilizando el estilo de seguridad correcto: `volume qtree show`
3. Si el qtree no está usando el estilo de seguridad deseado, cambie el estilo de seguridad con el `volume qtree security` comando.
4. Añadir un recurso compartido de directorio inicial: `vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory\[,...\]`

   `-vserver vserver` Especifica la máquina virtual de almacenamiento (SVM) habilitada para CIFS en la que se añadirá la ruta de búsqueda.

   `-share-name %w` especifica el nombre del recurso compartido del directorio principal. ONTAP crea dinámicamente el nombre del recurso compartido a medida que cada usuario se conecta a su directorio inicial. El nombre del recurso compartido tendrá el formato *Windows_USER_NAME*.

   `-path %d/%w` especifica la ruta relativa al directorio raíz. La ruta relativa se crea dinámicamente a medida que cada usuario se conecta a su directorio principal y tendrá el formato *domain/Windows_user_name*.

   `-share-properties homedirectory[,…]+` especifica las propiedades de recurso compartido para ese recurso compartido. Debe especificar `homedirectory` el valor. Puede especificar propiedades de recursos compartidos adicionales mediante una lista delimitada por comas.

5. Compruebe que el recurso compartido tiene la configuración deseada con `vserver cifs share show` el comando.
6. Agregar una ruta de búsqueda del directorio inicial: `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver` *`vserver-name`* Especifica la SVM habilitada para CIFS en la que se añadirá la ruta de búsqueda.

   `-path` *`path`* especifica la ruta de acceso absoluta del directorio a la ruta de búsqueda.

7. Compruebe que ha agregado correctamente la ruta de búsqueda mediante el `vserver cifs home-directory search-path show` comando.
8. Para los usuarios que dispongan de un directorio inicial, cree un directorio correspondiente en el qtree o en el volumen designado para que contengan directorios iniciales.

   Por ejemplo, si creó un qtree con la ruta de `/vol/vol1/users` y el nombre de usuario cuyo directorio desea crear es mydomain\user1, debe crear un directorio con la ruta de acceso siguiente `/vol/vol1/users/mydomain/user1`: .

Si creaste un volumen llamado “home1” montado en `/home1`, crearías un directorio con la siguiente ruta: `/home1/mydomain/user1`.

9. Compruebe que un usuario puede conectarse correctamente al recurso compartido principal mediante la asignación de una unidad o la conexión mediante la ruta UNC.

   Por ejemplo, si el usuario mydomain\user1 desea conectarse al directorio creado en el Paso 8 que se encuentra en la SVM VS1, user1 se conectaría mediante la ruta UNC `\\vs1\user1` .

Ejemplo

Los comandos del siguiente ejemplo crean una configuración de directorio inicial con los siguientes ajustes:

- El nombre del recurso compartido es %w.
- La ruta de acceso relativa al directorio principal es %d/%w.
- La ruta de búsqueda que se utiliza para contener los directorios raíz `/home1` , es un volumen configurado con estilo de seguridad NTFS.
- La configuración se crea en SVM vs1.

Puede utilizar este tipo de configuración de directorio inicial cuando los usuarios acceden a sus directorios iniciales desde hosts de Windows. También puede utilizar este tipo de configuración cuando los usuarios acceden a sus directorios iniciales desde hosts Windows y UNIX y el administrador del sistema de archivos utiliza usuarios y grupos basados en Windows para controlar el acceso al sistema de archivos.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %w

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %d/%w
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                 Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

Información relacionada

- Configure directorios iniciales utilizando la variable %u
- Obtenga más información sobre configuraciones adicionales del directorio de inicio
- Mostrar información sobre las rutas del directorio de inicio del usuario

Configurar los directorios de inicio de ONTAP SMB utilizando la variable %u

Puede crear una configuración de directorio inicial donde se designe el nombre del recurso compartido mediante la `%w` variable, pero se utiliza la `%u` variable para designar la ruta relativa al recurso compartido del directorio inicial. A continuación, los usuarios pueden conectarse a su recurso compartido doméstico mediante recursos compartidos dinámicamente creados con su nombre de usuario de Windows sin tener en cuenta el nombre real o la ruta de acceso del directorio principal.

Pasos

1. Cree un qtree que contenga los directorios iniciales de usuario: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Compruebe que el qtree esté utilizando el estilo de seguridad correcto: `volume qtree show`
3. Si el qtree no está usando el estilo de seguridad deseado, cambie el estilo de seguridad con el `volume qtree security` comando.
4. Añadir un recurso compartido de directorio inicial: `vserver cifs share create -vserver vserver -share-name %w -path %u -share-properties homedirectory ,...]`

   `-vserver vserver` Especifica la máquina virtual de almacenamiento (SVM) habilitada para CIFS en la que se añadirá la ruta de búsqueda.

   `-share-name %w` especifica el nombre del recurso compartido del directorio principal. El nombre del recurso compartido se crea dinámicamente a medida que cada usuario se conecta a su directorio principal y tiene el formato *Windows_USER_NAME*.

   > También puede utilizar `%u` la variable para `-share-name` la opción. Esto crea una ruta de acceso de recursos compartidos relativa que utiliza el nombre de usuario UNIX asignado.

   `-path %u` especifica la ruta relativa al directorio raíz. La ruta relativa se crea dinámicamente a medida que cada usuario se conecta a su directorio principal y tiene el formato *corated_UNIX_user_name*.

   > El valor de esta opción también puede contener elementos estáticos. Por ejemplo, `eng/%u`.

   `-share-properties homedirectory\[,...\]` especifica las propiedades de recurso compartido para ese recurso compartido. Debe especificar `homedirectory` el valor. Puede especificar propiedades de recursos compartidos adicionales mediante una lista delimitada por comas.

5. Compruebe que el recurso compartido tiene la configuración deseada con `vserver cifs share show` el comando.
6. Agregar una ruta de búsqueda del directorio inicial: `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver vserver` Especifica la SVM habilitada para CIFS en la que se añadirá la ruta de búsqueda.

   `-path path` especifica la ruta de acceso absoluta del directorio a la ruta de búsqueda.

7. Compruebe que ha agregado correctamente la ruta de búsqueda mediante el `vserver cifs home-directory search-path show` comando.
8. Si el usuario UNIX no existe, cree el usuario UNIX con el `vserver services unix-user create` comando.

   > Debe existir el nombre de usuario UNIX al que se asigna el nombre de usuario de Windows antes de asignar el usuario.

9. Cree una asignación de nombres para el usuario Windows al usuario UNIX con el siguiente comando: `vserver name-mapping create -vserver vserver_name -direction win-unix -priority integer -pattern windows_user_name -replacement unix_user_name`

Si ya existen asignaciones de nombres que asignan usuarios de Windows a usuarios UNIX, no es necesario realizar el paso de asignación.

El nombre de usuario de Windows está asignado al nombre de usuario UNIX correspondiente. Cuando el usuario de Windows se conecta a su recurso compartido de directorio principal, se conectan a un directorio raíz creado dinámicamente con un nombre de recurso compartido que corresponde a su nombre de usuario de Windows sin tener en cuenta que el nombre de directorio corresponde al nombre de usuario UNIX.

10. Para los usuarios que dispongan de un directorio inicial, cree un directorio correspondiente en el qtree o en el volumen designado para que contengan directorios iniciales.

    Por ejemplo, si creaste un qtree con la ruta de acceso de `/vol/vol1/users` y el nombre de usuario UNIX asignado del usuario cuyo directorio quieres crear es 'unixuser1', crearías un directorio con la siguiente ruta de acceso `/vol/vol1/users/unixuser1`: .

    Si creaste un volumen llamado "home1" montado en `/home1`, crearías un directorio con la siguiente ruta: `/home1/unixuser1`.

11. Compruebe que un usuario puede conectarse correctamente al recurso compartido principal mediante la asignación de una unidad o la conexión mediante la ruta UNC.

    Por ejemplo, si el usuario mydomain\user1 se asigna al usuario UNIX unixuser1 y desea conectarse al directorio creado en el Paso 10 que se encuentra en SVM VS1, user1 se conectaría mediante la ruta UNC `\\vs1\user1` .

Ejemplo

Los comandos del siguiente ejemplo crean una configuración de directorio inicial con los siguientes ajustes:

- El nombre del recurso compartido es %w.
- La ruta de acceso relativa al directorio principal es %u.
- La ruta de búsqueda que se utiliza para contener los directorios raíz `/home1` , es un volumen configurado con estilo de seguridad UNIX.
- La configuración se crea en SVM vs1.

Puede utilizar este tipo de configuración de directorio inicial cuando los usuarios acceden a sus directorios iniciales desde hosts Windows o hosts Windows y UNIX y el administrador del sistema de archivos utiliza usuarios y grupos basados en UNIX para controlar el acceso al sistema de archivos.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %u

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %u
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show -vserver vs1
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1

cluster::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1

cluster::> vserver name-mapping show -pattern user1
Vserver        Direction Position
-------------- --------- --------
vs1            win-unix  5        Pattern: user1
                               Replacement: unixuser1
```

Información relacionada

- Cree configuraciones de directorio de inicio utilizando las variables %w y %d
- Obtenga más información sobre configuraciones adicionales del directorio de inicio
- Mostrar información sobre las rutas del directorio de inicio del usuario

Obtenga más información sobre configuraciones adicionales del directorio de inicio SMB de ONTAP

Puede crear configuraciones de directorio raíz adicionales mediante las `%w %d %u` variables , y, lo que permite personalizar la configuración del directorio raíz para satisfacer sus necesidades.

Puede crear una serie de configuraciones de directorios iniciales mediante una combinación de variables y cadenas estáticas en los nombres de recursos compartidos y las rutas de búsqueda. En la siguiente tabla se muestran algunos ejemplos que ilustran cómo crear distintas configuraciones de directorio principal:

Rutas creadas cuando `/vol1/user` contiene directorios iniciales…	**Compartir comando…**
Para crear una ruta de acceso compartida `\\vs1\~win_username` que dirija al usuario a. `/vol1/user/win_username`	`vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory`
Para crear una ruta de acceso compartida `\\vs1\win_username` que dirija al usuario a. `/vol1/user/domain/win_username`	`vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory`
Para crear una ruta de acceso compartida `\\vs1\win_username` que dirija al usuario a. `/vol1/user/unix_username`	`vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory`
Para crear una ruta de acceso compartida `\\vs1\unix_username` que dirija al usuario a. `/vol1/user/unix_username`	`vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory`

Comandos ONTAP para administrar rutas de búsqueda SMB

Hay comandos ONTAP específicos para gestionar las rutas de búsqueda de las configuraciones de directorios iniciales de SMB. Por ejemplo, hay comandos para agregar, quitar y mostrar información acerca de las rutas de búsqueda. También hay un comando para cambiar el orden de la ruta de búsqueda.

Si desea…	**Se usa este comando…**
Agregue una ruta de búsqueda	`vserver cifs home-directory search-path add`
Mostrar rutas de búsqueda	`vserver cifs home-directory search-path show`

Si desea…	Se usa este comando…
Cambie el orden de la ruta de búsqueda	`vserver cifs home-directory search-path reorder`
Quitar una ruta de búsqueda	`vserver cifs home-directory search-path remove`

Obtenga más información sobre `vserver cifs home-directory search-path` en el "Referencia de comandos del ONTAP".

Mostrar información sobre las rutas del directorio de inicio del usuario SMB de ONTAP

Puede mostrar la ruta de directorio inicial de un usuario SMB en la máquina virtual de almacenamiento (SVM), que puede utilizarse si tiene varias rutas de directorio raíz CIFS configuradas y desea ver qué ruta contiene el directorio raíz del usuario.

Paso

1. Visualice la ruta del directorio inicial con `vserver cifs home-directory show-user` el comando.

```
vserver cifs home-directory show-user -vserver vs1 -username user1
```

```
Vserver      User                 Home Dir Path
-----------  -------------------  ----------------------
vs1          user1                /home/user1
```

Información relacionada

Administrar la accesibilidad a los directorios personales de los usuarios

Administrar la accesibilidad a los directorios de inicio de los usuarios de ONTAP SMB

De forma predeterminada, sólo el usuario puede acceder al directorio principal de un usuario. Para los recursos compartidos donde el nombre dinámico del recurso compartido va precedido de una tilde (~), los administradores de Windows o cualquier otro usuario (acceso público) pueden habilitar o deshabilitar el acceso a los directorios principales de los usuarios.

Antes de empezar

Los recursos compartidos de directorio inicial en la máquina virtual de almacenamiento (SVM) deben configurarse con nombres de recursos compartidos dinámicos que van precedidos por una tilde (~). En los siguientes casos se ilustran los requisitos de nomenclatura de los recursos compartidos:

Nombre del recurso compartido del directorio inicial	Ejemplo de comando para conectarse al recurso compartido
~%d~%w	`net use * \\IPaddress\~domain~user/u:credentials`
~%w	`net use * \\IPaddress\~user/u:credentials`
~abc~%w	`net use * \\IPaddress\abc~user/u:credentials`

Paso

1. Ejecute la acción adecuada:

Si desea activar o desactivar el acceso a los directorios de inicio de los usuarios a…	Introduzca lo siguiente…
Administradores de Windows	`vserver cifs home-directory modify -vserver` *`vserver_name`* `-is-home-dirs -access-for-admin-enabled {true|false}` El valor predeterminado es `true`.
Cualquier usuario (acceso público)	a. Establezca el nivel de privilegio en AVANZADO: `set -privilege advanced` b. Activar o desactivar el acceso: `vserver cifs home-directory modify -vserver` *vserver_name* -is-home-dirs-access-for-public-enabled {true

El siguiente ejemplo habilita el acceso público a los directorios principales de los usuarios:

```
set -privilege advanced +
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public
-enabled true
set -privilege admin
```

Información relacionada

Mostrar información sobre las rutas del directorio de inicio del usuario

Configure el acceso del cliente SMB a los enlaces simbólicos de UNIX

Obtenga información sobre cómo proporcionar acceso de cliente SMB de ONTAP a enlaces simbólicos de UNIX

Un enlace simbólico es un archivo creado en un entorno UNIX que contiene una referencia a otro archivo o directorio. Si un cliente accede a un enlace simbólico, se redirige al cliente al archivo o directorio de destino al que hace referencia el enlace simbólico. ONTAP soporta enlaces simbólicos relativos y absolutos, incluyendo enlaces de widelinks (enlaces absolutos con destinos fuera del sistema de archivos local).

ONTAP proporciona a los clientes SMB la capacidad de seguir enlaces simbólicos UNIX configurados en la SVM. Esta función es opcional y puede configurarla por recurso compartido, utilizando la `-symlink -properties` opción del `vserver cifs share create` comando, con una de las siguientes opciones:

- Habilitada con acceso de lectura/escritura
- Habilitado con acceso de solo lectura
- Desactivado mediante la ocultación de enlaces simbólicos de clientes SMB
- Deshabilitado sin acceso a enlaces simbólicos de clientes SMB

Si habilita enlaces simbólicos en un recurso compartido, los enlaces simbólicos relativos funcionan sin más configuración.

Si activa enlaces simbólicos en un recurso compartido, los enlaces simbólicos absolutos no funcionan de inmediato. Primero debe crear una asignación entre la ruta UNIX del enlace simbólico a la ruta SMB de destino. Al crear asignaciones de vínculos simbólicos absolutos, puede especificar si se trata de un enlace local o de un *widelink*; las widelinks pueden ser enlaces a sistemas de archivos en otros dispositivos de almacenamiento o vínculos a sistemas de archivos alojados en SVM independientes en el mismo sistema ONTAP. Al crear un windelink, debe incluir la información que debe seguir el cliente; es decir, cree un punto de reanálisis para que el cliente detecte el punto de unión del directorio. Si crea un vínculo simbólico absoluto a un archivo o directorio fuera del recurso compartido local pero establece la localidad en local, ONTAP no permite el acceso al destino.

> Si un cliente intenta eliminar un enlace simbólico local (absoluto o relativo), sólo se eliminará el enlace simbólico, no el archivo o directorio de destino. Sin embargo, si un cliente intenta eliminar un widelink, podría eliminar el archivo de destino real o el directorio al que hace referencia el widelink. ONTAP no tiene control sobre esto, ya que el cliente puede abrir de forma explícita el archivo o directorio de destino fuera de la SVM y eliminarlo.

- **Puntos de análisis y servicios del sistema de archivos ONTAP**

  Un *reanálisis point* es un objeto del sistema de archivos NTFS que se puede almacenar opcionalmente en volúmenes junto con un archivo. Los puntos de análisis proporcionan a los clientes SMB la capacidad de recibir servicios del sistema de archivos mejorados o ampliados al trabajar con volúmenes de estilo NTFS. Los puntos de reanálisis constan de etiquetas estándar que identifican el tipo de punto de reanálisis y el contenido del punto de reanálisis que pueden recuperar los clientes SMB para un procesamiento posterior por parte del cliente. De los tipos de objeto disponibles para la funcionalidad ampliada del sistema de archivos, ONTAP implementa la compatibilidad con enlaces simbólicos NTFS y puntos de unión de directorios mediante etiquetas de punto de reanálisis. Los clientes SMB que no pueden comprender el contenido de un punto de análisis simplemente lo ignoran y no proporcionan el servicio de sistema de archivos ampliado que podría habilitar el punto de análisis.

- **Puntos de unión de directorios y soporte de ONTAP para enlaces simbólicos**

  Los puntos de unión de directorios son ubicaciones dentro de una estructura de directorios del sistema de archivos que pueden hacer referencia a ubicaciones alternativas en las que se almacenan los archivos, ya sea en una ruta de acceso diferente (enlaces simbólicos) o en un dispositivo de almacenamiento independiente (widelinks). Los servidores SMB de ONTAP exponen los puntos de unión de directorios a los clientes de Windows como puntos de análisis, lo que permite a los clientes con capacidad obtener contenidos de punto de análisis de ONTAP cuando se pasa un punto de unión de directorios. De este modo, pueden navegar y conectarse a diferentes rutas o dispositivos de almacenamiento, como si formaran parte del mismo sistema de archivos.

- **Activación de la compatibilidad con el uso de las opciones de punto de reanálisis**

`-is-use-junctions-as-reparse-points-enabled`La opción está habilitada de forma predeterminada en ONTAP 9. La opción para habilitar la información se puede configurar según la versión del protocolo, ya que no todos los clientes SMB admiten enlaces anchos. Esto permite a los administradores adaptar tanto a clientes SMB compatibles como a los no compatibles. Debe habilitar esta opción. `-widelink-as-reparse-point-versions` para cada protocolo de cliente que accede al recurso compartido mediante enlaces anchos; el valor predeterminado es SMB1.

Información relacionada

- "Aplicaciones de backup de Windows y symlinks de tipo Unix"
- "Documentación de Microsoft: Puntos de análisis"

Límites al configurar enlaces simbólicos de UNIX para el acceso SMB de ONTAP

Debe estar al tanto de determinados límites al configurar los enlaces simbólicos UNIX para el acceso a SMB.

Límite	Descripción
45	Longitud máxima del nombre del servidor CIFS que puede especificar al usar un FQDN para el nombre del servidor CIFS. También puede especificar el nombre del servidor CIFS como nombre NetBIOS, que está limitado a 15 caracteres.
80	La longitud máxima del nombre del recurso compartido.
256	Longitud máxima de la ruta de UNIX que puede especificar al crear un enlace simbólico o al modificar la ruta de UNIX de un enlace simbólico existente. La ruta de acceso de UNIX debe comenzar con un '/" (slash) and end with a "/'. Las barras diagonales iniciales y finales cuentan como parte del límite de 256 caracteres.
256	Longitud máxima de la ruta CIFS que puede especificar al crear un enlace simbólico o al modificar la ruta CIFS de un enlace simbólico existente. La ruta CIFS debe empezar por ' '/" (slash) and end with a " /'. Las barras diagonales iniciales y finales cuentan como parte del límite de 256 caracteres.

Información relacionada

Crear asignaciones de enlaces simbólicos para acciones

Controlar anuncios DFS automáticos en servidores SMB de ONTAP

Una opción de servidor CIFS controla cómo se anuncian las funcionalidades DFS a los clientes SMB al conectarse a recursos compartidos. Dado que ONTAP utiliza referencias DFS cuando los clientes acceden a enlaces simbólicos a través de SMB, debe ser consciente del impacto que tiene al deshabilitar o habilitar esta opción.

Una opción de servidor CIFS determina si los servidores CIFS se anuncian automáticamente que son DFS capaz de clientes SMB. De forma predeterminada, esta opción está habilitada y el servidor CIFS siempre anuncia que es DFS capaz de los clientes SMB (incluso cuando se conecta a recursos compartidos donde el acceso a enlaces simbólicos está deshabilitado). Si desea que el servidor CIFS anuncie que es compatible con DFS sólo cuando se conectan a recursos compartidos donde está habilitado el acceso a enlaces simbólicos, puede deshabilitar esta opción.

Debe tener en cuenta lo que ocurre cuando se deshabilita esta opción:

- La configuración de uso compartido de los enlaces simbólicos no cambia.
- Si el parámetro share se establece para permitir el acceso de enlace simbólico (ya sea de lectura y escritura o de sólo lectura), el servidor CIFS DFS anuncia capacidades a clientes que se conectan a ese recurso compartido.

  Las conexiones del cliente y el acceso a enlaces simbólicos se mantienen sin interrupción.

- Si el parámetro share se establece para no permitir el acceso de enlace simbólico (ya sea deshabilitando el acceso o si el valor del parámetro share es null), el servidor CIFS no anuncia capacidades DFS a clientes que se conectan a ese recurso compartido.

  Como los clientes tienen información en caché que el servidor CIFS es compatible con DFS y ya no anuncia que es, es posible que los clientes conectados a recursos compartidos donde se deshabilita el acceso a enlaces simbólicos no puedan acceder a estos recursos compartidos una vez que se deshabilita la opción de servidor CIFS. Después de deshabilitar la opción, es posible que deba reiniciar los clientes conectados a estos recursos compartidos, borrando de esta forma la información almacenada en caché.

Estos cambios no se aplican a conexiones SMB 1.0.

Configurar la compatibilidad con enlaces simbólicos de UNIX en recursos compartidos SMB de ONTAP

Puede configurar la compatibilidad de vínculos simbólicos de UNIX en recursos compartidos de SMB especificando una configuración de propiedad de recurso compartido de vínculo simbólico al crear recursos compartidos de SMB o en cualquier momento mediante la modificación de recursos compartidos de SMB existentes. La compatibilidad con el enlace simbólico de UNIX está habilitada de forma predeterminada. También puede deshabilitar la compatibilidad con enlaces simbólicos de UNIX en un recurso compartido.

Acerca de esta tarea

Al configurar la compatibilidad de enlaces simbólicos de UNIX para recursos compartidos de SMB, puede elegir una de las siguientes opciones de configuración:

Ajuste	Descripción
`enable` (ANTICUADO*)	Especifica que los enlaces simbólicos están habilitados para el acceso de lectura y escritura.
`read_only` (ANTICUADO*)	Especifica que los enlaces simbólicos están habilitados para el acceso de sólo lectura. Esta configuración no se aplica a las tintas widelinks. El acceso a Widelink siempre es de lectura y escritura.
`hide` (ANTICUADO*)	Especifica que los clientes SMB no pueden ver enlaces simbólicos.
`no-strict-security`	Especifica que los clientes siguen enlaces simbólicos fuera de los límites de recursos compartidos.
`symlinks`	Especifica que los enlaces simbólicos están habilitados localmente para el acceso de lectura y escritura. Los anuncios DFS no se generan incluso si la opción CIFS `is-advertise-dfs-enabled` está establecida en `true`. Esta es la configuración predeterminada.
`symlinks-and-widelinks`	Especifica que tanto los enlaces simbólicos locales como los widelinks para el acceso de lectura y escritura. Los anuncios DFS se generan tanto para enlaces simbólicos locales como widelinks incluso si la opción CIFS `is-advertise-dfs-enabled` está establecida en `false`.
`disable`	Especifica que los enlaces simbólicos y las tintas widelinks están desactivados. Los anuncios DFS no se generan incluso si la opción CIFS `is-advertise-dfs-enabled` está establecida en `true`.
`""` (nulo, no definido)	Deshabilita los enlaces simbólicos en el recurso compartido.
– (no configurado)	Deshabilita los enlaces simbólicos en el recurso compartido.

*Los parámetros *enable*, *ocultar* y *Read-only* están obsoletos y se pueden eliminar en una futura versión de ONTAP.

Pasos

1. Configure o deshabilite el soporte de enlaces simbólicos:

Si es…	Introduzca…
Un nuevo recurso compartido de SMB	`+vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink -properties {enable
hide	read-only
""	-
symlinks	symlinks-and-widelinks
disable},…]+`	Un recurso compartido de SMB existente
`+vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable	hide
read-only	""
-	symlinks
symlinks-and-widelinks	disable},…]+`

2. Compruebe que la configuración del recurso compartido de SMB sea correcta: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Ejemplo

El siguiente comando crea un recurso compartido SMB llamado «ata1» con la configuración de enlace simbólico de UNIX establecida en `enable`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                Share Properties: oplocks
                                  browsable
                                  changenotify
              Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: -
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Información relacionada

Crear asignaciones de enlaces simbólicos para acciones

Crear asignaciones de enlaces simbólicos para recursos compartidos SMB de ONTAP

Puede crear asignaciones de enlaces simbólicos UNIX para los recursos compartidos de SMB. Puede crear un vínculo simbólico relativo, que hace referencia al archivo o la carpeta relativa a su carpeta principal, o bien puede crear un vínculo simbólico absoluto, que hace referencia al archivo o la carpeta utilizando una ruta absoluta.

Acerca de esta tarea

Los usuarios de Mac OS X no pueden acceder a Widelinks si utilizan SMB 2.x. Cuando un usuario intenta conectarse a un recurso compartido mediante widelinks desde un cliente Mac OS X, el intento falla. Sin embargo, puede utilizar widelinks con clientes Mac OS X si utiliza SMB 1.

Pasos

1. Para crear asignaciones de enlaces simbólicos para recursos compartidos de SMB: `vserver cifs symlink create -vserver virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-directory {true|false}]`

   `-vserver virtual_server_name` Especifica el nombre de la máquina virtual de almacenamiento

(SVM).

`-unix-path path` Especifica la ruta UNIX. La ruta UNIX debe empezar por una barra diagonal (`/`) y debe terminar con una barra diagonal (`/`).

`-share-name share_name` Especifica el nombre del recurso compartido de SMB que se va a asignar.

`-cifs-path path` Especifica la ruta CIFS. La ruta CIFS debe comenzar con una barra diagonal (`/`) y debe terminar con una barra diagonal (`/`).

`-cifs-server server_name` Especifica el nombre del servidor CIFS. El nombre del servidor CIFS puede especificarse como un nombre DNS (por ejemplo, mynetwork.cifs.server.com), una dirección IP o un nombre NetBIOS. El nombre de NetBIOS se puede determinar mediante el `vserver cifs show` comando. Si no se especifica este parámetro opcional, el valor predeterminado es el nombre NetBIOS del servidor CIFS local.

`-locality local|free|widelink}` especifica si se debe crear un enlace local, un enlace libre o un enlace simbólico amplio. Un enlace simbólico local se asigna al recurso compartido local de SMB. Un enlace simbólico gratuito puede asignar en cualquier parte del servidor SMB local. Un amplio enlace simbólico se asigna a cualquier recurso compartido de SMB en la red. Si no se especifica este parámetro opcional, el valor por defecto es `local`.

`-home-directory true false}` especifica si el recurso compartido de destino es un directorio raíz. Aunque este parámetro sea opcional, debe definir este parámetro en `true` cuando el recurso compartido de destino esté configurado como directorio raíz. El valor predeterminado es `false`.

Ejemplo

El siguiente comando crea una asignación de enlaces simbólicos en la SVM llamada vs1. Tiene la ruta UNIX `/src/` , el nombre compartido SMB 'SOURCE', la ruta CIFS `/mycompany/source/` y la dirección IP del servidor CIFS 123.123.123.123, y es un enlace inalámbrico.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

Información relacionada

Configurar la compatibilidad de enlaces simbólicos de UNIX en recursos compartidos

Comandos ONTAP para administrar asignaciones de enlaces simbólicos SMB

Hay comandos ONTAP específicos para gestionar las asignaciones de enlaces simbólicos.

Si desea…	Se usa este comando…
Cree una asignación de vínculos simbólicos	`vserver cifs symlink create`
Mostrar información acerca de las asignaciones de enlaces simbólicos	`vserver cifs symlink show`

Si desea…	Se usa este comando…
Modificar una asignación de vínculos simbólicos	`vserver cifs symlink modify`
Eliminar una asignación de vínculos simbólicos	`vserver cifs symlink delete`

Obtenga más información sobre `vserver cifs symlink` en el "Referencia de comandos del ONTAP".

Aplicaciones de copia de seguridad de Windows y enlaces simbólicos de estilo Unix en servidores SMB de ONTAP

Cuando una aplicación de copia de seguridad que se ejecuta en Windows encuentra un enlace simbólico de estilo Unix (symlink), se sigue el enlace y se realiza una copia de seguridad de los datos. A partir de ONTAP 9.15.1, tiene la opción de realizar una copia de seguridad de los symlinks en lugar de los datos. Esta función es totalmente compatible con volúmenes de ONTAP FlexGroup y FlexVols.

Descripción general

Antes de cambiar la forma en que ONTAP maneja los enlaces simbólicos durante una operación de copia de seguridad de Windows, debería estar familiarizado con las ventajas, los conceptos clave y las opciones de configuración.

Beneficios

Cuando esta función está desactivada o no disponible, se recorre cada enlace simbólico y se realiza una copia de seguridad de los datos a los que enlaza. Debido a esto, a veces se puede hacer un backup de los datos innecesarios y en ciertas situaciones la aplicación podría terminar en un bucle. En su lugar, la copia de seguridad de los enlaces simbólicos evita estos problemas. Y como los archivos symlink son muy pequeños en comparación con los datos en la mayoría de los casos, las copias de seguridad tardan menos tiempo en completarse. El rendimiento general del clúster también puede mejorar debido a la reducción de las operaciones de I/O.

Entorno de servidor Windows

Esta función es compatible con aplicaciones de backup que se ejecutan en Windows. Debe comprender los aspectos técnicos relevantes del entorno antes de utilizarlo.

Atributos ampliados

Windows admite atributos extendidos (EA) que forman colectivamente metadatos adicionales asociados opcionalmente a los archivos. Estos atributos los utilizan varias aplicaciones, como el subsistema de Windows para Linux, como se describe en "Permisos de archivo para WSL". Las aplicaciones pueden solicitar atributos ampliados para cada archivo al leer datos de ONTAP.

Los enlaces simbólicos se devuelven en los atributos extendidos cuando la función está activada. Por lo tanto, una aplicación de copia de seguridad debe proporcionar compatibilidad de EA estándar que se utiliza para almacenar los metadatos. Algunas utilidades de Windows admiten y conservan los atributos extendidos. Sin embargo, si el software de copia de seguridad no admite la copia de seguridad y la restauración de los atributos extendidos, no conservará los metadatos asociados con cada archivo y no podrá procesar los enlaces simbólicos correctamente.

Configuración de Windows

Las aplicaciones de copia de seguridad que se ejecutan en un servidor de Microsoft Windows pueden tener un privilegio especial que les permite omitir la seguridad de archivos normal. Esto se realiza normalmente agregando las aplicaciones al grupo Operadores de copia de seguridad. A continuación, las aplicaciones pueden realizar copias de seguridad y restaurar archivos según sea necesario, así como realizar otras operaciones relacionadas con el sistema. Se producen sutiles cambios en el protocolo SMB que utilizan las aplicaciones de backup que ONTAP puede detectar a medida que se leen y escriben los datos.

Requisitos

La función de copia de seguridad Symlink tiene varios requisitos, entre los que se incluyen:

- El clúster ejecuta ONTAP 9.15.1 o una versión posterior.
- Aplicación de copia de seguridad de Windows a la que se han otorgado privilegios de copia de seguridad especiales.
- La aplicación de backup también debe admitir atributos ampliados y solicitarlos durante las operaciones de backup.
- La función de backup de symlink de ONTAP está habilitada para la SVM de datos correspondiente.

Opciones de configuración

Además de la interfaz de línea de comandos de ONTAP, también es posible gestionar esta función mediante la API de REST. Consulte "Novedades de la API de REST DE ONTAP y la automatización" para obtener más información. La configuración que determina cómo ONTAP procesa los enlaces simbólicos de estilo Unix se debe realizar por separado en cada SVM.

Habilite la función de backup de symlink en ONTAP

Se introdujo una opción de configuración en un comando de la CLI existente con ONTAP 9.15.1. Puede utilizar esta opción para activar o desactivar el procesamiento de enlaces simbólicos de estilo Unix.

Antes de empezar

Revise el básico Requisitos. Además:

- Sea capaz de elevar su privilegio de CLI al nivel avanzado.
- Determine la SVM de datos que desea modificar. La SVM `vs1` se usa en el comando de ejemplo.

Pasos

1. Establezca el nivel de privilegio avanzado.

```
set privilege advanced
```

2. Active la copia de seguridad de archivos symlink.

```
vserver cifs options modify -vserver vs1 -is-backup-symlink-enabled true
```

Utilice BranchCache para almacenar en caché contenido compartido SMB en una sucursal

Obtenga información sobre el uso de BranchCache para almacenar en caché el contenido compartido de ONTAP SMB en una sucursal

BranchCache fue desarrollado por Microsoft para permitir el almacenamiento de contenido en la caché de los equipos locales de los clientes que lo soliciten. La implementación de BranchCache por parte de ONTAP puede reducir la utilización de la red de área amplia (WAN) y proporcionar un tiempo de respuesta de acceso mejorado cuando los usuarios de una sucursal acceden al contenido almacenado en máquinas virtuales de almacenamiento (SVM) mediante SMB.

Si configura BranchCache, los clientes de Windows BranchCache en primer lugar recuperan el contenido de la SVM y, a continuación, almacenan en caché el contenido de un equipo dentro de la sucursal. Si otro cliente con BranchCache habilitado en la sucursal solicita el mismo contenido, la SVM primero autentica y autoriza al usuario solicitante. A continuación, la SVM determina si el contenido en caché aún está actualizado y, si lo está, envía los metadatos del cliente sobre el contenido en caché. A continuación, el cliente utiliza los metadatos para recuperar contenido directamente desde la memoria caché basada en la ubicación local.

Información relacionada

Obtenga información sobre el uso de archivos sin conexión para permitir el almacenamiento en caché de archivos para su uso sin conexión

Requisitos y directrices

Obtenga información sobre la compatibilidad de versiones de ONTAP SMB BranchCache

Debe tener en cuenta qué versiones de BranchCache son compatibles con ONTAP.

ONTAP es compatible con BranchCache 1 y con BranchCache 2 mejorado:

- Cuando se configura BranchCache en el servidor SMB para la máquina virtual de almacenamiento (SVM), puede habilitar BranchCache 1, BranchCache 2 o todas las versiones.

  De forma predeterminada, todas las versiones están habilitadas.

- Si solo habilita BranchCache 2, los equipos cliente Windows de oficina remota deben admitir BranchCache 2.

  Solo los clientes SMB 3.0 o una versión posterior admiten BranchCache 2.

Para obtener más información sobre las versiones de BranchCache, consulte la biblioteca de Microsoft TechNet.

Información relacionada

"Biblioteca de Microsoft TechNet: technet.microsoft.com/en-us/library/"

Obtenga información sobre los requisitos de compatibilidad del protocolo de red SMB de ONTAP

Debe tener en cuenta los requisitos del protocolo de red para implementar BranchCache de ONTAP.

Puede implementar la función ONTAP BranchCache en redes IPv4 e IPv6 mediante SMB 2.1 o una versión posterior.

Todos los servidores CIFS y los equipos de oficinas remotas que participan en la implementación de BranchCache deben tener habilitado el protocolo SMB 2.1 o una versión posterior. SMB 2.1 tiene extensiones de protocolo que permiten que un cliente participe en un entorno de BranchCache. Esta es la versión mínima del protocolo SMB que ofrece compatibilidad con BranchCache. SMB 2.1 admite la versión de BranchCache, versión 1.

Si desea usar BranchCache versión 2, SMB 3.0 es la versión mínima admitida. Todos los servidores CIFS y los equipos de oficinas remotas que participan en una implementación de BranchCache 2 deben tener habilitado SMB 3.0 o una versión posterior.

Si tiene oficinas remotas en las que algunos clientes solo admiten SMB 2.1 y algunos de los clientes admiten SMB 3.0, puede implementar una configuración de BranchCache en el servidor CIFS que proporcione compatibilidad con el almacenamiento en caché tanto en BranchCache 1 como en BranchCache 2.

Aunque la función Microsoft BranchCache admite el uso de los protocolos HTTP/HTTPS y SMB como protocolos de acceso a archivos, ONTAP BranchCache solo admite el uso de SMB.

Obtenga información sobre los requisitos de las versiones de hosts de ONTAP SMB y Windows

Los hosts de ONTAP y de oficina remota deben cumplir determinados requisitos de versión para poder configurar BranchCache.

Antes de configurar BranchCache, debe asegurarse de que la versión de ONTAP en el clúster y los clientes de la sucursal participantes sean compatibles con SMB 2.1 o una versión posterior y con la función de BranchCache. Si configura el modo de caché alojada, también debe asegurarse de que utiliza un host compatible para el servidor de caché.

BranchCache 1 es compatible con las siguientes versiones de ONTAP y hosts de Windows:

- Servidor de contenido: Máquina virtual de almacenamiento (SVM) con ONTAP
- Servidor de caché: Windows Server 2008 R2 o Windows Server 2012 o posterior
- Igual o cliente: Windows 7 Enterprise, Windows 7 Ultimate, Windows 8, Windows Server 2008 R2 o Windows Server 2012 o posterior

BranchCache 2 es compatible con las siguientes versiones de ONTAP y hosts de Windows:

- Servidor de contenido: SVM con ONTAP
- Servidor de caché: Windows Server 2012 o posterior
- Igual o cliente: Windows 8 o Windows Server 2012 o posterior

Conozca las razones por las que ONTAP SMB invalida los hashes de BranchCache

Comprender los motivos por los que ONTAP invalida los hash puede ser útil a la hora de planificar la configuración de BranchCache. Puede ayudarle a decidir el modo operativo que debe configurar y a elegir en qué recursos compartidos desea habilitar BranchCache.

ONTAP debe gestionar los hash de BranchCache para garantizar que sean válidos. Si un hash no es válido, ONTAP invalida el hash y calcula un nuevo hash la próxima vez que se solicite el contenido, suponiendo que BranchCache siga estando habilitado.

ONTAP invalida los hash por los siguientes motivos:

- Se modifica la clave de servidor.

  Si se modifica la clave del servidor, ONTAP invalida todos los hash del almacén hash.

- Un hash se vacía de la caché porque se alcanzó el tamaño máximo del almacén hash de BranchCache.

  Se trata de un parámetro ajustable y puede modificarse para satisfacer sus requisitos empresariales.

- Un archivo se modifica mediante un acceso SMB o NFS.
- Un archivo para el que hay hash calculados se restaura con `snap restore` el comando.
- Un volumen que contiene recursos compartidos de SMB que tienen habilitada para BranchCache se restaura mediante `snap restore` el comando.

Obtenga información sobre cómo elegir la ubicación del almacén de hash de ONTAP SMB

Al configurar BranchCache, elija dónde almacenar los hash y qué tamaño debe tener el almacén hash. Las directrices a la hora de elegir la ubicación y el tamaño del almacén hash pueden ayudarle a planificar la configuración de BranchCache en una SVM habilitada para CIFS.

- Debe localizar el almacén hash en un volumen en el que se permitan las actualizaciones de atime.

  El tiempo de acceso de un archivo hash se utiliza para mantener los archivos a los que se accede con más frecuencia en el almacén hash. Si las actualizaciones de atime están deshabilitadas, se utiliza la hora de creación con este fin. Es preferible utilizar atime para realizar un seguimiento de los archivos utilizados con frecuencia.

- No puede almacenar hash en sistemas de archivos de solo lectura como los destinos de SnapMirror y los volúmenes SnapLock.
- Si se alcanza el tamaño máximo del almacén hash, los hash más antiguos se vacían para crear espacio para los hash nuevos.

  Es posible aumentar el tamaño máximo del almacén hash para reducir la cantidad de hash que se vacía de la caché.

- Si el volumen en el que almacena hash no está disponible o lleno, o si hay un problema con la comunicación dentro del clúster donde el servicio BranchCache no puede recuperar información hash, los servicios de BranchCache no estarán disponibles.

  El volumen puede no estar disponible porque está sin conexión o porque el administrador de almacenamiento especificó una nueva ubicación para el almacén de hash.

  Esto no provoca problemas con el acceso a archivos. Si se ve afectado el acceso al almacén hash, ONTAP devolverá un error definido por Microsoft al cliente, que hace que el cliente solicite el archivo con la solicitud de lectura SMB normal.

Información relacionada

- Configurar BranchCache en los servidores
- Modificar las configuraciones de BranchCache en los recursos compartidos

Conozca las recomendaciones de ONTAP SMB BranchCache

Antes de configurar BranchCache, hay ciertas recomendaciones que debe tener en cuenta a la hora de decidir qué recursos compartidos de SMB desea habilitar el almacenamiento en caché de BranchCache.

Debe tener en cuenta las siguientes recomendaciones a la hora de decidir qué modo operativo usar y en qué recursos compartidos de SMB para habilitar BranchCache:

- Las ventajas de BranchCache se reducen cuando los datos que se van a almacenar en caché de forma remota cambian con frecuencia.
- Los servicios de BranchCache son beneficiosos para los recursos compartidos que contienen contenido de archivos que se vuelve a utilizar por varios clientes de oficina remota o por contenido de archivo al que un único usuario remoto accede en repetidas ocasiones.
- Considere la posibilidad de habilitar el almacenamiento en caché para contenido de solo lectura, como datos en snapshots y destinos SnapMirror.

Configure BranchCache

Obtenga más información sobre la configuración de ONTAP SMB BranchCache

Puede configurar BranchCache en el servidor SMB con los comandos de la ONTAP. Para implementar BranchCache, también debe configurar los clientes y, opcionalmente, los servidores de caché alojados en las sucursales en las que desea almacenar en caché el contenido.

Si configura BranchCache para habilitar el almacenamiento en caché de recurso compartido por recurso, debe habilitar BranchCache en los recursos compartidos SMB para los que desea proporcionar servicios de almacenamiento en caché de BranchCache.

Requisitos para configurar ONTAP SMB BranchCache

Después de cumplir algunos requisitos previos, puede configurar BranchCache.

Debe cumplir los siguientes requisitos antes de configurar BranchCache en el servidor CIFS para la SVM:

- ONTAP debe instalarse en todos los nodos del clúster.
- CIFS debe tener una licencia y se debe configurar un servidor SMB. La licencia SMB se incluye con "ONTAP One". Si no tiene ONTAP One y la licencia no está instalada, póngase en contacto con su representante de ventas.
- Se debe configurar la conectividad de red IPv4 o IPv6.
- Para BranchCache 1, se debe habilitar SMB 2.1 o una versión posterior.
- Para BranchCache 2, se debe habilitar SMB 3.0 y los clientes de Windows remotos deben admitir BranchCache 2.

Configurar BranchCache en servidores SMB de ONTAP

Puede configurar BranchCache para proporcionar servicios de BranchCache por recurso compartido. Como alternativa, puede configurar BranchCache para habilitar automáticamente el almacenamiento en caché en todos los recursos compartidos de

SMB.

Acerca de esta tarea

Puede configurar BranchCache en las SVM.

- Puede crear una configuración de BranchCache para todos los recursos compartidos si desea ofrecer servicios de almacenamiento en caché para todo el contenido en todos los recursos compartidos SMB en el servidor CIFS.
- Puede crear una configuración de BranchCache por recurso compartido si desea ofrecer servicios de almacenamiento en caché para el contenido de ciertos recursos compartidos SMB en el servidor CIFS.

Debe especificar los siguientes parámetros al configurar BranchCache:

Parámetros necesarios	Descripción
SVM name	BranchCache se configura por SVM. Debe especificar en qué SVM con la función CIFS habilitada desea configurar el servicio BranchCache.
Path to hash store	Los hash de BranchCache se almacenan en archivos normales del volumen de SVM. Debe especificar la ruta a un directorio existente en el que desea que ONTAP almacene los datos de hash.la ruta hash de BranchCache debe ser de lectura y escritura. No se admiten rutas de solo lectura, como los directorios de snapshots. Es posible almacenar datos de hash en un volumen que contiene otros datos o se puede crear un volumen independiente para almacenar datos hash. Si la SVM es un origen de recuperación ante desastres de SVM, la ruta de hash no puede estar en el volumen raíz. Esto se debe a que el volumen raíz no se replica en el destino de recuperación ante desastres. La ruta de hash puede contener espacios en blanco y cualquier carácter válido de nombre de archivo.

Opcionalmente, puede especificar los siguientes parámetros:

Parámetros opcionales	Descripción
Versiones compatibles	ONTAP admite BranchCache 1 y 2. Puede habilitar la versión 1, la versión 2 o ambas versiones. El valor predeterminado es habilitar ambas versiones.

Parámetros opcionales	Descripción
Tamaño máximo del almacén hash	Puede especificar el tamaño que se usará para el almacén de datos hash. Si los datos de hash superan este valor, ONTAP eliminará los hash más antiguos para hacer sitio a los más recientes. El tamaño predeterminado del almacén hash es 1 GB. BranchCache funciona de manera más eficiente si no se descartan los hash de una forma excesivamente agresiva. Si determina que los hash se descartan con frecuencia porque el almacén hash está lleno, puede aumentar el tamaño del almacén hash modificando la configuración de BranchCache.
Clave de servidor	Puede especificar una clave de servidor que el servicio de BranchCache utilice para evitar que los clientes suplanten el servidor de BranchCache. Si no se especifica una clave de servidor, se genera de forma aleatoria al crear la configuración de BranchCache. Puede establecer la clave de servidor como un valor específico, de modo que, si hay varios servidores que proporcionan datos de BranchCache para los mismos archivos, los clientes puedan usar hash de cualquier servidor que utilice la misma clave de servidor. Si la clave de servidor contiene espacios, debe escribirla entre comillas.
Modo de funcionamiento	El valor predeterminado es habilitar BranchCache por recurso compartido. • Para crear una configuración de BranchCache donde se habilita BranchCache por recurso compartido, no se puede especificar este parámetro opcional o se puede especificar `per-share`. • Para habilitar automáticamente BranchCache en todos los recursos compartidos, debe establecer el modo operativo en `all-shares`.

Pasos

1. Habilite SMB 2.1 y 3.0 según sea necesario:
   a. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
   b. Compruebe la configuración de SMB de SVM configurada para determinar si todas las versiones necesarias de SMB están habilitadas: `vserver cifs options show -vserver` *`vserver_name`*
   c. Si es necesario, habilite SMB 2,1: `vserver cifs options modify -vserver` *`vserver_name`* `-smb2-enabled true`

      El comando habilita SMB 2.0 y SMB 2.1.

   d. Si es necesario, habilite SMB 3,0: `vserver cifs options modify -vserver` *`vserver_name`*

```
-smb3-enabled true
```

e. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

2. Configurar BranchCache: `vserver cifs branchcache create -vserver vserver_name -hash-store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all] [-server-key text] -operating-mode {per-share|all-shares}`

   La ruta de almacenamiento hash especificada debe existir y debe residir en un volumen gestionado por la SVM. La ruta también debe ubicarse en un volumen de lectura y escritura. El comando falla si la ruta es de solo lectura o no existe.

   Si desea usar la misma clave de servidor para configuraciones de BranchCache adicionales, registre el valor introducido para la clave de servidor. La clave de servidor no aparece cuando se muestra información sobre la configuración de BranchCache.

3. Compruebe que la configuración de BranchCache sea correcta: `vserver cifs branchcache show -vserver vserver_name`

Ejemplos

Los siguientes comandos verifican que tanto SMB 2.1 como 3.0 están habilitadas y configuran BranchCache para permitir automáticamente el almacenamiento en caché de todos los recursos compartidos de SMB en SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true


cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares
```

Los siguientes comandos verifican que tanto SMB 2.1 como 3.0 están habilitadas, configure BranchCache para permitir el almacenamiento en caché de acuerdo con un recurso compartido en SVM vs1 y verifique la configuración de BranchCache:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Información relacionada

- Obtenga más información sobre la compatibilidad de versiones de BranchCache
- Obtenga información sobre cómo configurar BranchCache en la oficina remota
- Cree un recurso compartido de SMB habilitado con BranchCache
- Habilitar BranchCache en recursos compartidos existentes
- Modificar las configuraciones de BranchCache en los recursos compartidos
- Obtenga información sobre cómo deshabilitar BranchCache en los recursos compartidos
- Eliminar la configuración de BranchCache en los recursos compartidos

Obtenga información sobre cómo configurar BranchCache en la oficina remota en ONTAP SMB

Después de configurar BranchCache en el servidor SMB, debe instalar y configurar BranchCache en los equipos cliente y, opcionalmente, en los servidores de almacenamiento en caché de la oficina remota. Microsoft proporciona instrucciones para la configuración de BranchCache en la oficina remota.

Las instrucciones para configurar clientes de sucursal y, de manera opcional, los servidores de almacenamiento en caché que usen BranchCache se encuentran en el sitio web de Microsoft BranchCache.

"Microsoft BranchCache Docs: Novedades"

Configure los recursos compartidos SMB habilitados para BranchCache

Obtenga información sobre cómo configurar recursos compartidos SMB de ONTAP habilitados para BranchCache

Una vez que configura BranchCache en el servidor SMB y en la sucursal, puede habilitar BranchCache en recursos compartidos SMB que contienen contenido que desea permitir que los clientes de las sucursales se almacenan en caché.

El almacenamiento en caché de BranchCache puede habilitarse en todos los recursos compartidos de SMB en el servidor SMB o de recurso compartido por recurso.

- Si habilita BranchCache por recurso compartido, puede habilitar BranchCache a medida que crea el recurso compartido o modifica los recursos compartidos existentes.

  Si habilita el almacenamiento en caché en un recurso compartido de SMB existente, ONTAP comienza a enviar hashes de computación y metadatos a clientes que soliciten contenido tan pronto como habilite BranchCache en ese recurso compartido.

- Todos los clientes que tengan una conexión SMB existente a un recurso compartido no obtienen compatibilidad con BranchCache si, a continuación, se habilita BranchCache en ese recurso compartido.

  ONTAP anuncia el soporte de BranchCache para un recurso compartido en el momento de la configuración de la sesión del bloque de mensajes del servidor. Los clientes que ya han establecido sesiones cuando se habilita BranchCache deben desconectar y volver a conectarse para usar el contenido en caché para este recurso compartido.

> Si BranchCache en un recurso compartido de SMB se encuentra deshabilitado posteriormente, ONTAP deja de enviar metadatos al cliente solicitante. Un cliente que necesita datos lo recupera directamente del servidor de contenido (servidor SMB).

Crear recursos compartidos SMB de ONTAP habilitados para BranchCache

Puede habilitar BranchCache en un recurso compartido de SMB cuando se crea el recurso compartido mediante la configuración `branchcache` de la propiedad de recurso compartido.

Acerca de esta tarea

- Si se habilita BranchCache en el recurso compartido de SMB, el recurso compartido debe tener la configuración de los archivos sin conexión establecida en el almacenamiento manual en caché.

  Esta es la configuración predeterminada cuando se crea un recurso compartido.

- También puede especificar parámetros de recurso compartido opcionales al crear el recurso compartido con BranchCache habilitado.
- Es posible establecer `branchcache` la propiedad en un recurso compartido aunque BranchCache no esté configurado y habilitado en la máquina virtual de almacenamiento (SVM).

  Sin embargo, si desea que el recurso compartido ofrezca contenido en caché, debe configurar y habilitar BranchCache en la SVM.

- Dado que no hay propiedades de recurso compartido predeterminadas aplicadas al recurso compartido al utilizar el `-share-properties` parámetro, debe especificar todas las demás propiedades de recurso compartido que desee aplicar al recurso compartido además de la `branchcache` propiedad de recurso compartido mediante una lista delimitada por comas.
- Obtenga más información sobre `vserver cifs share create` en el "Referencia de comandos del ONTAP".

Paso

1. Cree un recurso compartido de SMB habilitado para BranchCache:
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties branchcache[,…]`
2. Compruebe que la propiedad BranchCache Share esté configurada en el recurso compartido de SMB mediante `vserver cifs share show` el comando.

Ejemplo

El siguiente comando crea un recurso compartido SMB habilitado para BranchCache llamado «data» con una ruta de acceso `/data` de en SVM VS1. De forma predeterminada, la configuración de archivos fuera de línea se establece en `manual`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
                      Vserver: vs1
                        Share: data
     CIFS Server NetBIOS Name: VS1
                         Path: /data
             Share Properties: branchcache
                               oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: data
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Información relacionada

Deshabilitar BranchCache en un solo recurso compartido

Habilitar BranchCache en recursos compartidos SMB de ONTAP existentes

Puede habilitar BranchCache en un recurso compartido SMB existente agregando la `branchcache` propiedad de recurso compartido a la lista existente de propiedades de recurso compartido.

Acerca de esta tarea

- Si se habilita BranchCache en el recurso compartido de SMB, el recurso compartido debe tener la configuración de los archivos sin conexión establecida en el almacenamiento manual en caché.

  Si la opción de archivos sin conexión del recurso compartido existente no está establecida en almacenamiento en caché manual, debe configurarlo modificando el recurso compartido.

- Es posible establecer `branchcache` la propiedad en un recurso compartido aunque BranchCache no esté configurado y habilitado en la máquina virtual de almacenamiento (SVM).

  Sin embargo, si desea que el recurso compartido ofrezca contenido en caché, debe configurar y habilitar BranchCache en la SVM.

- Al agregar `branchcache` la propiedad Compartir al recurso compartido, se conservan la configuración de recurso compartido existente y las propiedades de recurso compartido.

  La propiedad share de BranchCache se agrega a la lista existente de propiedades compartidas. Obtenga más información sobre `vserver cifs share properties add` en el "Referencia de comandos del ONTAP".

Pasos

1. Si es necesario, configure el parámetro de recursos compartidos de archivos sin conexión para el almacenamiento en caché manual:
   a. Determine cuál es el valor del recurso compartido de archivos sin conexión mediante el `vserver cifs share show` comando.
   b. Si la configuración de archivos compartidos sin conexión no está establecida en manual, cámbiela al valor necesario: `vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual`
2. Habilitar BranchCache en un recurso compartido de SMB existente: `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. Compruebe que la propiedad de recurso compartido de BranchCache esté configurada en el recurso compartido de SMB: `vserver cifs share show -vserver vserver_name -share-name share_name`

Ejemplo

El siguiente comando habilita BranchCache en un recurso compartido SMB existente denominado «dATA2» con una ruta de acceso `/data2` de en SVM VS1:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              showsnapshot
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties add  -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              showsnapshot
                              changenotify
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Información relacionada

- Agregar o eliminar propiedades de recursos compartidos en recursos compartidos existentes
- Deshabilitar BranchCache en un solo recurso compartido

Modificar las configuraciones de BranchCache en los recursos compartidos SMB de ONTAP

Puede modificar la configuración del servicio BranchCache en las SVM, lo que incluye el cambio de la ruta de directorio del almacén hash, el tamaño máximo del directorio del almacén hash, el modo operativo y las versiones de BranchCache que son compatibles. También puede aumentar el tamaño del volumen que contiene el almacén hash.

Pasos

1. Ejecute la acción adecuada:

Si desea…	Introduzca lo siguiente…
Modifique el tamaño del directorio del almacén hash	`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB
MB	GB
TB	PB]}`
Aumente el tamaño del volumen que contiene el almacén hash	`volume size -vserver vserver_name -volume volume_name -new-size new_size[k
m	g
t]` Si el volumen que contiene el almacén hash se llena, es posible que pueda aumentar el tamaño del volumen. Puede especificar el nuevo tamaño del volumen como número, seguido de una designación de unidad. Más información acerca de "Gestión de volúmenes de FlexVol"	Modifique la ruta del directorio del almacén hash

Si desea…	Introduzca lo siguiente…
`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true	false}` Si la SVM es un origen de recuperación ante desastres de SVM, la ruta hash no puede estar en el volumen raíz. Esto se debe a que el volumen raíz no se replica en el destino de recuperación ante desastres. La ruta de hash de BranchCache puede contener espacios en blanco y cualquier carácter válido de nombre de archivo. Si modifica la ruta de hash, `-flush-hashes` es un parámetro requerido que especifica si desea que ONTAP vacíe los hash de la ubicación del almacén hash original. Puede definir los siguientes valores para el `-flush-hashes` parámetro: **Si especifica `true`, ONTAP eliminará los hash de la ubicación original y creará nuevos hash en la nueva ubicación a medida que los clientes habilitados para BranchCache realicen nuevas solicitudes.** Si especifica `false`, los hashes no se vacían. + En este caso, puede optar por reutilizar los hash existentes más adelante cambiando la ruta del almacén hash de vuelta a la ubicación original.
Cambie el modo de funcionamiento	`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share
all-shares	disable}` Debe tener en cuenta lo siguiente al modificar el modo de funcionamiento: **ONTAP anuncia el soporte de BranchCache para un recurso compartido cuando se configura la sesión SMB.** Los clientes que ya han establecido sesiones cuando se habilita BranchCache deben desconectar y volver a conectarse para usar el contenido en caché para este recurso compartido.
Cambie la compatibilidad de la versión de BranchCache	`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable
v2-enable	enable-all}`

2. Verifique los cambios de configuración con `vserver cifs branchcache show` el comando.

Mostrar información sobre las configuraciones de BranchCache en los recursos compartidos SMB de ONTAP

Puede mostrar información sobre las configuraciones de BranchCache en máquinas virtuales de almacenamiento (SVM), que se pueden utilizar al verificar una configuración o al determinar la configuración actual antes de modificar una configuración.

Paso

1. Ejecute una de las siguientes acciones:

Si desea mostrar…	Introduzca este comando…
Información resumida sobre las configuraciones de BranchCache en todas las SVM	`vserver cifs branchcache show`
Información detallada sobre la configuración de una SVM específica	`vserver cifs branchcache show -vserver` *`vserver_name`*

Ejemplo

En el siguiente ejemplo, se muestra información sobre la configuración de BranchCache en la SVM vs1:

```
cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
            Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
            Maximum Size of the Hash Store: 20GB
  Encryption Key Used to Secure the Hashes: -
          CIFS BranchCache Operating Modes: per_share
```

Cambiar la clave del servidor ONTAP SMB BranchCache

Puede cambiar la clave de servidor de BranchCache mediante la modificación de la configuración de BranchCache en la máquina virtual de almacenamiento (SVM) y la especificación de una clave de servidor diferente.

Acerca de esta tarea

Puede establecer la clave de servidor como un valor específico, de modo que, si hay varios servidores que proporcionan datos de BranchCache para los mismos archivos, los clientes puedan usar hash de cualquier servidor que utilice la misma clave de servidor.

Cuando cambia la clave de servidor, también debe vaciar la caché hash. Después de vaciar los hash, ONTAP crea nuevos hash a medida que los clientes habilitados para BranchCache crean nuevas solicitudes.

Pasos

1. Cambie la clave de servidor mediante el siguiente comando: `vserver cifs branchcache modify -vserver vserver_name -server-key text -flush-hashes true`

Al configurar una nueva clave de servidor, también debe especificar `-flush-hashes` y definir el valor en `true`.

2. Compruebe que la configuración de BranchCache sea correcta mediante `vserver cifs branchcache show` el comando.

Ejemplo

En el ejemplo siguiente se establece una nueva clave de servidor que contiene espacios y vacía la caché hash en la SVM vs1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Información relacionada

Conozca las razones por las que ONTAP invalida los hashes de BranchCache

Calcular previamente los hashes de BranchCache en rutas SMB de ONTAP específicas

Puede configurar el servicio BranchCache para que preajuste los valores hash de computación para un único archivo, para un directorio o para todos los archivos de una estructura de directorio. Esto puede resultar útil si desea calcular hash en datos de un recurso compartido habilitado con BranchCache durante las horas fuera de servicio y no en las horas punta.

Acerca de esta tarea

Si desea recoger una muestra de datos antes de mostrar estadísticas de hash, debe usar `statistics start` `statistics stop` los comandos opcionales y.

- Debe especificar la máquina virtual de almacenamiento (SVM) y la ruta en la que desea contar con los hash de tecnología previa.
- También debe especificar si desea calcular los valores hash de forma recursiva.
- Si desea calcular los hash de forma recursiva, el servicio BranchCache atraviesa todo el árbol de directorios bajo la ruta de acceso especificada y calcula los hash de cada objeto elegible.

  Obtenga más información sobre `statistics start` y `statistics stop` en el "Referencia de comandos del ONTAP" .

Pasos

1. Hash de precomputación como desee:

Si desea contar con hash de tecnología previa…	Introduzca el comando…
Un único archivo o directorio	`vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false`
Recursivamente en todos los archivos de una estructura de directorios	`vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true`

2. Verifique que los hash se están calculando mediante `statistics` el comando:

   a. Muestre estadísticas del `hashd` objeto en la instancia SVM deseada: `statistics show -object hashd -instance vserver_name`

   b. Compruebe que el número de hash creado aumenta repitiendo el comando.

   Obtenga más información sobre `statistics show` en el "Referencia de comandos del ONTAP".

Ejemplos

En el siguiente ejemplo se crean hash en la ruta `/data` y en todos los archivos y subdirectorios contenidos en SVM VS1:

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       85
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       92
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -
```

Información relacionada

- "Configuración de supervisión del rendimiento"

Limpiar hashes del almacén de hashes BranchCache de ONTAP SMB SVM

Puede vaciar todos los hash almacenados en caché del almacén hash de BranchCache en la máquina virtual de almacenamiento (SVM). Esto puede ser útil si ha cambiado la configuración de BranchCache de la sucursal. Por ejemplo, si recientemente reconfiguró el modo de almacenamiento en caché desde el almacenamiento en caché distribuido al modo de almacenamiento en caché alojado, debería vaciar el almacén hash.

Acerca de esta tarea

Después de vaciar los hash, ONTAP crea nuevos hash a medida que los clientes habilitados para BranchCache crean nuevas solicitudes.

Paso

1. Vacíe los hash del almacén hash de BranchCache: `vserver cifs branchcache hash-flush -vserver` *`vserver_name`*

   ```
   vserver cifs branchcache hash-flush -vserver vs1
   ```

Mostrar estadísticas de ONTAP SMB BranchCache

Puede mostrar las estadísticas de BranchCache para, entre otras cosas, identificar el nivel de rendimiento del almacenamiento en caché, determinar si su configuración proporciona contenido en caché a los clientes y determinar si los archivos hash se eliminaron para dar cabida a los datos hash más recientes.

Acerca de esta tarea

```
`hashd`El objeto de estadística contiene contadores que proporcionan
información estadística sobre los hashes de BranchCache.  `cifs`El objeto
estadístico contiene contadores que proporcionan información estadística
sobre la actividad relacionada con BranchCache. Puede recopilar y mostrar
información acerca de estos objetos en el nivel de privilegio avanzado.
```

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`

   ```
   cluster1::> set -privilege advanced

   Warning: These advanced commands are potentially dangerous; use them
   only when directed to do so by support personnel.
   Do you want to continue? {y|n}: y
   ```

2. Muestre los contadores relacionados con BranchCache mediante `statistics catalog counter show` el comando.

   ```
   cluster1::*> statistics catalog counter show -object hashd
   ```

```
Object: hashd
    Counter                       Description
    ---------------------------
-------------------------------------------
    branchcache_hash_created      Number of times a request to generate
                                  BranchCache hash for a file succeeded.
    branchcache_hash_files_replaced
                                  Number of times a BranchCache hash file
was
                                  deleted to make room for more recent
hash
                                  data. This happens if the hash store
size is
                                  exceeded.
    branchcache_hash_rejected     Number of times a request to generate
                                  BranchCache hash data failed.
    branchcache_hash_store_bytes
                                  Total number of bytes used to store hash
data.
    branchcache_hash_store_size Total space used to store BranchCache
hash
                                  data for the Vserver.
    instance_name                 Instance Name
    instance_uuid                 Instance UUID
    node_name                     System node name
    node_uuid                     System node id
9 entries were displayed.

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                       Description
    ---------------------------
-------------------------------------------
    active_searches               Number of active searches over SMB and
SMB2
    auth_reject_too_many          Authentication refused after too many
                                  requests were made in rapid succession
    avg_directory_depth           Average number of directories crossed by
SMB
                                  and SMB2 path-based commands
    avg_junction_depth            Average number of junctions crossed by
SMB
                                  and SMB2 path-based commands
    branchcache_hash_fetch_fail Total number of times a request to fetch
```

```
hash
                                 data failed. These are failures when
                                 attempting to read existing hash data.
It
                                 does not include attempts to fetch hash
data
                                 that has not yet been generated.
    branchcache_hash_fetch_ok    Total number of times a request to fetch
hash
                                 data succeeded.
    branchcache_hash_sent_bytes Total number of bytes sent to clients
                                 requesting hashes.
    branchcache_missing_hash_bytes
                                 Total number of bytes of data that had
to be
                                 read by the client because the hash for
that
                                 content was not available on the server.
   ....Output truncated....
```

Obtenga más información sobre `statistics catalog counter show` en el "Referencia de comandos del ONTAP".

3. Recopile estadísticas relacionadas con BranchCache mediante `statistics start` `statistics stop` los comandos y.

```
cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11
```

Obtenga más información sobre `statistics start` y `statistics stop` en el "Referencia de comandos del ONTAP" .

4. Muestre las estadísticas de BranchCache recogidas mediante `statistics show` el comando.

```
cluster1::*> statistics show -object cifs -counter
branchcache_hash_sent_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0

cluster1::*> statistics show -object cifs -counter
branchcache_missing_hash_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
```

Obtenga más información sobre `statistics show` en el "Referencia de comandos del ONTAP".

5. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

```
cluster1::*> set -privilege admin
```

Información relacionada

- Mostrar estadísticas
- "Configuración de supervisión del rendimiento"
- "Las estadísticas comienzan"
- "las estadísticas se detienen"

Obtenga información sobre la compatibilidad de ONTAP SMB con los objetos de política de grupo de BranchCache

BranchCache de ONTAP proporciona compatibilidad con objetos de directiva de grupo (GPO) de BranchCache, los cuales permiten una gestión centralizada para ciertos parámetros de configuración de BranchCache. Hay dos GPO utilizados para BranchCache, la publicación Hash para el GPO de BranchCache y la compatibilidad con versiones Hash para el GPO de BranchCache.

- **Publicación Hash para BranchCache GPO**

  La publicación hash para GPO de BranchCache corresponde al `-operating-mode` parámetro. Cuando se producen actualizaciones de GPO, este valor se aplica a los objetos de máquinas virtuales de almacenamiento (SVM) contenidos en la unidad organizativa (OU) a la que se aplica la directiva de grupo.

- **Compatibilidad con la versión Hash para el GPO de BranchCache**

  La compatibilidad de versiones hash para GPO de BranchCache corresponde al `-versions` parámetro. Cuando se producen actualizaciones de GPO, este valor se aplica a los objetos SVM incluidos en la unidad organizativa a la que se aplica la directiva de grupo.

Información relacionada

Obtenga información sobre cómo aplicar objetos de directiva de grupo a servidores SMB

Mostrar información sobre los objetos de directiva de grupo de ONTAP SMB BranchCache

Puede mostrar información acerca de la configuración de objeto de directiva de grupo (GPO) del servidor CIFS para determinar si se definen GPO de BranchCache para el dominio al que pertenece el servidor CIFS y, si es así, ¿cuáles son las configuraciones permitidas? También puede determinar si la configuración de GPO de BranchCache se aplica al servidor CIFS.

Acerca de esta tarea

Aunque se ha definido una configuración de GPO en el dominio al que pertenece el servidor CIFS, no se aplica necesariamente a la unidad organizativa (OU) que contiene la máquina virtual de almacenamiento (SVM) habilitada para CIFS. La configuración de GPO aplicada es el subconjunto de todos los GPO definidos que se aplican a la SVM habilitada para CIFS. La configuración de BranchCache que se aplica a través de los GPO anula la configuración aplicada a través de la CLI.

Pasos

1. Muestre la configuración de GPO de BranchCache definida para el dominio de Active Directory mediante `vserver cifs group-policy show-defined` el comando.

   Este ejemplo no muestra todos los campos de resultado disponibles para el comando. La salida está truncada.

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]
```

2. Muestre la configuración de GPO de BranchCache aplicada al servidor CIFS mediante `vserver cifs group-policy show-applied` el comando. "

> Este ejemplo no muestra todos los campos de resultado disponibles para el comando. La salida está truncada.

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
 [...]
```

Información relacionada

- Habilitar o deshabilitar la compatibilidad con GPO en los servidores
- "definido por la política de grupo cifs de vserver"
- "exposición de políticas de grupo cifs de vserver aplicada"

Deshabilite BranchCache en los recursos compartidos SMB

Obtenga información sobre cómo deshabilitar BranchCache en los recursos compartidos SMB de ONTAP

Si no desea proporcionar servicios de almacenamiento en caché de BranchCache en ciertos recursos compartidos de SMB, pero quizás desee proporcionar servicios de almacenamiento en caché en esos recursos compartidos más tarde, puede deshabilitar BranchCache en función de su recurso compartido. Si tiene BranchCache configurado para ofrecer almacenamiento en caché en todos los recursos compartidos pero desea deshabilitar temporalmente todos los servicios de almacenamiento en caché, puede

modificar la configuración de BranchCache para detener el almacenamiento en caché automático en todos los recursos compartidos.

Si BranchCache en un recurso compartido de SMB se deshabilita después de haber habilitado por primera vez, ONTAP deja de enviar metadatos al cliente que lo solicita. Un cliente que necesita datos los recupera directamente del servidor de contenido (servidor CIFS en la máquina virtual de almacenamiento (SVM)).

Información relacionada

Obtenga información sobre cómo configurar recursos compartidos habilitados para BranchCache

Deshabilitar BranchCache en un solo recurso compartido SMB de ONTAP

Si no desea ofrecer servicios de almacenamiento en caché en determinados recursos compartidos que anteriormente ofrecían contenido en caché, puede deshabilitar BranchCache en un recurso compartido de SMB existente.

Paso

1. Introduzca el siguiente comando: `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties branchcache`

   Se elimina la propiedad compartida de BranchCache. Otras propiedades de recursos compartidos aplicadas permanecen en vigor.

Ejemplo

El siguiente comando deshabilita BranchCache en un recurso compartido de SMB existente llamado «data2»:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Detener el almacenamiento en caché automático en todos los recursos compartidos SMB de ONTAP

Si la configuración de BranchCache habilita automáticamente el almacenamiento en caché en todos los recursos compartidos SMB en cada máquina virtual de almacenamiento (SVM), puede modificar la configuración de BranchCache para detener el almacenamiento en caché automático de contenido para todos los recursos compartidos SMB.

Acerca de esta tarea

Para detener el almacenamiento en caché automático en todos los recursos compartidos SMB, debe cambiar el modo operativo de BranchCache a almacenamiento en caché por recurso compartido.

Pasos

1. Configure BranchCache para detener el almacenamiento en caché automático en todos los recursos compartidos de SMB: `vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
2. Compruebe que la configuración de BranchCache sea correcta: `vserver cifs branchcache show -vserver vserver_name`

Ejemplo

El siguiente comando cambia la configuración de BranchCache en una máquina virtual de almacenamiento (SVM, antes conocida como Vserver) vs1 para detener el almacenamiento en caché automático en todos los recursos compartidos SMB:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Deshabilite o habilite BranchCache en la SVM

Descubra qué sucede cuando deshabilita o vuelve a habilitar BranchCache en servidores SMB de ONTAP

Si anteriormente configuró BranchCache pero no desea que los clientes de la sucursal utilicen contenido almacenado en caché, puede deshabilitar el almacenamiento en caché en el servidor CIFS. Debe tener en cuenta lo que sucede al deshabilitar BranchCache.

Cuando deshabilita BranchCache, ONTAP ya no calcula los hash ni envía los metadatos al cliente solicitante. Sin embargo, no se interrumpe el acceso a los archivos. A partir de entonces, cuando los clientes habilitados para BranchCache solicitan información de metadatos sobre el contenido al que desean acceder, ONTAP

responde con un error definido por Microsoft, lo que hace que el cliente envíe una segunda solicitud al contenido real. En respuesta a la solicitud de contenido, el servidor CIFS envía el contenido real almacenado en la máquina virtual de almacenamiento (SVM).

Una vez que se deshabilita BranchCache en el servidor CIFS, los recursos compartidos de SMB no anuncian las funcionalidades de BranchCache. Para acceder a los datos de nuevas conexiones SMB, los clientes realizan solicitudes de lectura SMB normales.

Puede volver a habilitar BranchCache en el servidor CIFS en cualquier momento.

- Dado que el almacén hash no se elimina cuando deshabilita BranchCache, ONTAP puede usar los hash almacenados al responder a las solicitudes hash una vez que vuelva a habilitar BranchCache, siempre y cuando el hash solicitado siga siendo válido.
- Todos los clientes que hayan establecido conexiones SMB a recursos compartidos habilitados con BranchCache durante el momento en el que se deshabilitó BranchCache no obtienen compatibilidad con BranchCache si se vuelve a habilitar BranchCache después.

  Esto se debe a que ONTAP anuncia el soporte de BranchCache para un recurso compartido en el momento de la configuración de la sesión del SMB. Los clientes que establecieron sesiones con recursos compartidos habilitados para BranchCache mientras BranchCache estaba deshabilitado necesitan desconectar y volver a conectarse para usar el contenido en caché para este recurso compartido.

Si no desea guardar el almacén hash después de deshabilitar BranchCache en un servidor CIFS, puede eliminarlo en forma manual. Si vuelve a habilitar BranchCache, debe asegurarse de que exista el directorio de almacén hash. Una vez que se vuelve a habilitar BranchCache, los recursos compartidos con BranchCache habilitados anuncian las funcionalidades de BranchCache. ONTAP crea nuevos hash a medida que las nuevas solicitudes las realizan los clientes habilitados para BranchCache.

Deshabilitar o habilitar BranchCache en recursos compartidos SMB de ONTAP

Es posible deshabilitar BranchCache en la máquina virtual de almacenamiento (SVM) si se cambia el modo operativo de BranchCache a `disabled`. Puede habilitar BranchCache en cualquier momento cambiando el modo operativo para ofrecer servicios de BranchCache por recurso compartido o automáticamente para todos los recursos compartidos.

Pasos

1. Ejecute el comando apropiado:

Si desea…	Introduzca lo siguiente…
Deshabilite BranchCache	`vserver cifs branchcache modify -vserver vserver_name -operating-mode disable`
Habilite BranchCache por recurso compartido	`vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`

Si desea…	Introduzca lo siguiente…
Habilite BranchCache para todos los recursos compartidos	`vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares`

2. Compruebe que el modo operativo BranchCache esté configurado con la configuración deseada: `vserver cifs branchcache show -vserver vserver_name`

Ejemplo

En el siguiente ejemplo, se deshabilita BranchCache en la SVM vs1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: disable
```

Elimine la configuración de BranchCache en las SVM

Descubra qué sucede cuando elimina la configuración de BranchCache en los recursos compartidos SMB de ONTAP

Si anteriormente configuró BranchCache, pero no desea que la máquina virtual de almacenamiento (SVM) continúe proporcionando contenido en caché, puede eliminar la configuración de BranchCache en el servidor CIFS. Debe saber lo que ocurre cuando se elimina la configuración.

Cuando se elimina la configuración, ONTAP quita la información de configuración de esa SVM del clúster y detiene el servicio BranchCache. Puede decidir si ONTAP debería eliminar el almacén hash de la SVM.

La eliminación de la configuración de BranchCache no interrumpe el acceso de los clientes habilitados para BranchCache. A partir de entonces, cuando los clientes habilitados para BranchCache solicitan información de metadatos sobre las conexiones SMB existentes para determinar el contenido que ya se ha almacenado en la caché, ONTAP responde con un error definido de Microsoft, lo que hace que el cliente envíe una segunda solicitud, solicitando el contenido real. En respuesta a la solicitud de contenido, el servidor CIFS envía el contenido real almacenado en la SVM

Una vez que se elimina la configuración de BranchCache, los recursos compartidos de SMB no anuncian las funcionalidades de BranchCache. Para acceder a contenido que no se ha almacenado previamente en la caché mediante nuevas conexiones SMB, los clientes realizan solicitudes de SMB de lectura normales.

Eliminar la configuración de BranchCache en los recursos compartidos SMB de ONTAP

El comando que se usa para eliminar el servicio BranchCache en la máquina virtual de almacenamiento (SVM) varía en función de si desea eliminar o conservar los hash existentes.

Paso

1. Ejecute el comando apropiado:

Si desea…	Introduzca lo siguiente…
Elimine la configuración de BranchCache y elimine los hash existentes	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes true`
Elimine la configuración de BranchCache, pero mantenga los hash existentes	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes false`

Ejemplo

En el siguiente ejemplo, se elimina la configuración de BranchCache en la SVM vs1 y se eliminan todos los hash existentes:

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes
true
```

Descubra qué sucede con ONTAP SMB BranchCache al revertir

Es importante comprender lo que sucede al revertir ONTAP a una versión que no admite BranchCache.

- Cuando revierte a una versión de ONTAP que no admite BranchCache, los recursos compartidos SMB no anuncian capacidades de BranchCache a los clientes habilitados para BranchCache; por lo tanto, los clientes no solicitan información hash.

  En su lugar, solicitan el contenido real mediante las solicitudes de lectura SMB normales. En respuesta a la solicitud de contenido, el servidor SMB envía el contenido real almacenado en la máquina virtual de almacenamiento (SVM).

- Cuando un nodo que aloja un almacén hash se revierte a una versión que no admite BranchCache, el administrador de almacenamiento debe revertir manualmente la configuración de BranchCache mediante un comando que se imprime durante la reversión.

  Este comando elimina la configuración y los hash de BranchCache.

  Una vez finalizada la reversión, el administrador de almacenamiento puede eliminar manualmente el directorio que contenía el almacén hash, si lo desea.

Información relacionada

Eliminar la configuración de BranchCache en los recursos compartidos

Mejorar el rendimiento de las copias remotas de Microsoft

Obtenga información sobre las mejoras de rendimiento de la copia remota de Microsoft en los servidores SMB de ONTAP

La transferencia de datos descargados (ODX) de Microsoft, también conocida como *copy fload*, permite transferir datos directamente dentro o entre dispositivos de almacenamiento compatibles sin transferir los datos a través del equipo host.

ONTAP admite ODX para los protocolos SMB Y SAN. El origen puede ser un servidor CIFS o una LUN; el destino puede ser un servidor CIFS o una LUN.

En las transferencias de archivos que no son ODX, los datos se leen del origen y se transfieren a través de la red al equipo cliente. El equipo cliente transfiere los datos a través de la red al destino. En resumen, el equipo cliente lee los datos del origen y los escribe en el destino. Con las transferencias de archivos ODX, los datos se copian directamente del origen al destino.

Dado que las copias descargados de ODX se realizan directamente entre el almacenamiento de origen y destino, se obtienen importantes ventajas en el rendimiento. Las ventajas en cuanto a rendimiento incluyen unos tiempos de copia más rápidos entre el origen y el destino, una menor utilización de recursos (CPU, memoria) en el cliente y una menor utilización de ancho de banda de I/o de la red.

En los entornos SMB, esta funcionalidad solo está disponible cuando el cliente y el servidor de almacenamiento admiten SMB 3.0 y la función ODX. En entornos SAN, esta funcionalidad solo está disponible cuando el cliente y el servidor de almacenamiento admiten la función ODX. Los equipos cliente compatibles con ODX y que tengan habilitada ODX automáticamente y de forma transparente utilizan la transferencia de archivos descargados cuando se mueven o copian archivos. ODX se utiliza independientemente de si arrastra y suelta archivos a través del Explorador de Windows, o si utiliza comandos de copia de archivos de la línea de comandos, o si una aplicación cliente inicia solicitudes de copia de archivos.

Información relacionada

- Aprenda a mejorar el tiempo de respuesta del cliente al proporcionar referencias automáticas de nodos con Ubicación automática
- "Configuración de SMB para Microsoft Hyper-V y SQL Server"

Obtenga más información sobre ODX en los servidores SMB de ONTAP

La descarga de copias ODX utiliza un mecanismo basado en tokens para leer y escribir datos dentro o entre servidores CIFS habilitados para ODX. En lugar de enrutar los datos a través del host, el servidor CIFS envía al cliente un pequeño token que representa los datos. El cliente ODX presenta ese token al servidor de destino, que posteriormente puede transferir los datos que representa ese token del origen al destino.

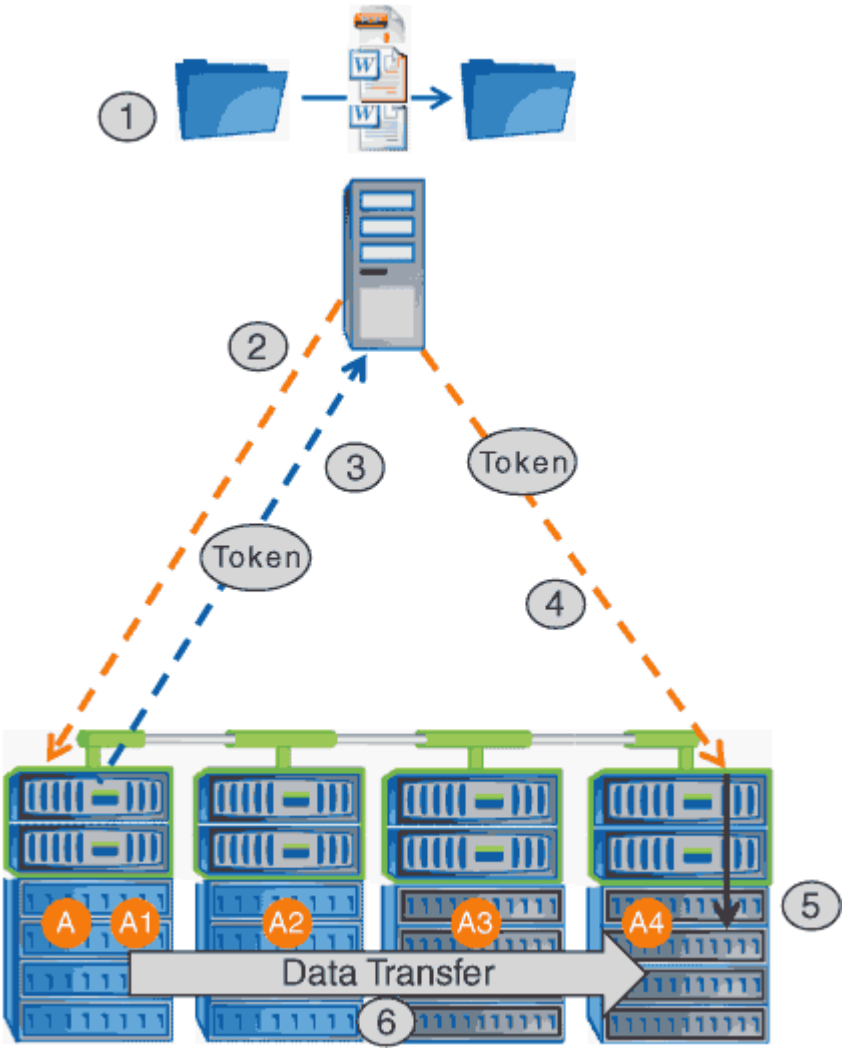
Cuando un cliente ODX descubre que el servidor CIFS es compatible con ODX, abre el archivo de origen y solicita un token del servidor CIFS. Después de abrir el archivo de destino, el cliente utiliza el token para indicar al servidor que copie los datos directamente del origen al destino.

El origen y el destino pueden estar en la misma máquina virtual de almacenamiento (SVM) o en distintas SVM, según el alcance de la operación de copia.

El token sirve como representación puntual de los datos. Por ejemplo, cuando copia datos entre ubicaciones de almacenamiento, se devuelve un token que representa un segmento de datos al cliente solicitante, que el cliente copia en el destino; de este modo, se elimina la necesidad de copiar los datos subyacentes a través del cliente.

ONTAP admite tokens que representan 8 MB de datos. Las copias ODX de más de 8 MB se realizan utilizando varios tokens, con cada token que representa 8 MB de datos.

En la siguiente figura, se explican los pasos involucrados en una operación de copia de ODX:



1. Un usuario copia o mueve un archivo mediante el Explorador de Windows, una interfaz de línea de comandos o como parte de la migración de un equipo virtual, o bien una aplicación inicia copias o traslados de archivos.
2. El cliente compatible con ODX convierte automáticamente esta solicitud de transferencia a una solicitud ODX.

   La solicitud ODX que se envía al servidor CIFS contiene una solicitud de token.
3. Si se habilita ODX en el servidor CIFS y la conexión a través de SMB 3.0, el servidor CIFS genera un token, que es una representación lógica de los datos en el origen.
4. El cliente recibe un token que representa los datos y se envía con la solicitud de escritura al servidor CIFS de destino.

Se trata de los únicos datos que se copian a través de la red desde el origen al cliente y, después, desde el cliente al destino.

5. El token se entrega al subsistema de almacenamiento.
6. La SVM realiza de forma interna la copia o el movimiento.

   Si el archivo que se copia o se mueve es de más de 8 MB, se necesitan varios tokens para realizar la copia. Pasos 2 a 6 según se requiera para completar la copia.

> Si se produce un error con la copia descargada de ODX, la operación de copia o movimiento se vuelve a leer y escribir tradicionales para la operación de copia o movimiento. Del mismo modo, si el servidor CIFS de destino no admite ODX ni ODX está deshabilitado, la operación de copia o movimiento se remonta a las lecturas y escrituras tradicionales para la operación de copia o movimiento.

Requisitos para usar ODX en servidores SMB de ONTAP

Antes de poder usar ODX para llevar a cabo descargas de copias con la máquina virtual de almacenamiento (SVM), debe conocer ciertos requisitos.

Requisitos de versión de ONTAP

ONTAP libera compatibilidad con ODX para realizar descargas de copias.

Requisitos de versión de SMB

- ONTAP es compatible con ODX mediante SMB 3.0 y versiones posteriores.
- Para poder habilitar ODX, es necesario habilitar SMB 3.0 en el servidor CIFS:
  - Si la función ODX no está habilitada, también habilita SMB 3.0.
  - Al deshabilitar SMB 3.0, también se deshabilita ODX.

Requisitos del servidor y del cliente de Windows

Antes de poder usar ODX para realizar descargas de copias, el cliente de Windows debe admitir la función.

El "Matriz de interoperabilidad de NetApp"contiene la información más reciente sobre los clientes de Windows compatibles.

Requisitos del volumen

- Los volúmenes de origen deben tener un mínimo de 1.25 GB.
- Si utiliza volúmenes comprimidos, el tipo de compresión debe ser adaptable y solo se admite el tamaño de grupo de compresión 8K.

  No se admite el tipo de compresión secundaria.

Pautas para el uso de ODX en servidores SMB de ONTAP

Antes de poder utilizar ODX para descarga de copias, debe conocer las directrices. Por ejemplo, debe saber en qué tipos de volúmenes se puede utilizar ODX y debe

comprender las consideraciones dentro del clúster y entre clústeres de ODX.

Directrices de volumen

- No se puede usar ODX para descargar la copia con las siguientes configuraciones de volumen:
  - El tamaño del volumen de origen es inferior a 1.25 GB

    El tamaño del volumen debe ser 1.25 GB o más para usar la función ODX.

  - Volúmenes de solo lectura

    ODX no se utiliza para archivos y carpetas que residen en reflejos de carga compartida o en volúmenes de destino de SnapMirror o SnapVault.

  - Si el volumen de origen no está deduplicado
- Las copias ODX solo son compatibles con las copias dentro del clúster.

  No se puede usar ODX para copiar archivos o carpetas en un volumen de otro clúster.

Otras directrices

- En los entornos SMB, para utilizar ODX para la descarga de copias, los archivos deben ser de 256 kb o más.

  Los archivos más pequeños se transfieren mediante una operación de copia tradicional.

- La descarga de copias ODX utiliza la deduplicación como parte del proceso de copia.

  Si no desea que la deduplicación se produzca en los volúmenes de SVM al copiar o mover datos, debe deshabilitar la descarga de la copia ODX en esa SVM.

- La aplicación que realiza la transferencia de datos debe escribirse para admitir ODX.

  Las operaciones de aplicaciones compatibles con ODX incluyen lo siguiente:

  - Las operaciones de gestión de Hyper-V, como la creación y conversión de discos duros virtuales (VHD), la gestión de snapshots y la copia de archivos entre máquinas virtuales
  - Operaciones del Explorador de Windows
  - Comandos de copia de Windows PowerShell
  - Comandos de copia en el símbolo del sistema de Windows

    Robocopy en el símbolo del sistema de Windows admite ODX.

    Las aplicaciones deben ejecutarse en servidores Windows o clientes que admitan ODX.

  +
  Para obtener más información acerca de las aplicaciones ODX admitidas en servidores y clientes Windows, consulte la biblioteca de Microsoft TechNet.

Información relacionada

"Biblioteca de Microsoft TechNet: technet.microsoft.com/en-us/library/"

Casos de uso de ODX en servidores SMB de ONTAP

Debe conocer los casos de uso de ODX en SVM para poder determinar en qué circunstancias le proporciona ventajas en rendimiento.

Los servidores y los clientes de Windows que admiten ODX utilizan la descarga de copias como forma predeterminada de copiar datos en servidores remotos. Si el cliente o el servidor Windows no son compatibles con ODX o se produce un error en cualquier momento, la operación de copia o movimiento vuelve a las lecturas y escrituras tradicionales para la operación de copia o movimiento.

Los siguientes casos de uso admiten el uso de copias y movimientos ODX:

- Volumen interno

  Los archivos o LUN de origen y destino están dentro del mismo volumen.

- Entre volúmenes, mismo nodo, misma SVM

  Los archivos de origen y de destino o las LUN se encuentran en distintos volúmenes ubicados en el mismo nodo. Los datos son propiedad de la misma SVM.

- Entre volúmenes, distintos nodos, misma SVM

  Los archivos de origen y de destino o las LUN se encuentran en volúmenes distintos que se encuentran en nodos diferentes. Los datos son propiedad de la misma SVM.

- Entre SVM, mismo nodo

  El archivo de origen y los LUN de destino se encuentran en distintos volúmenes ubicados en el mismo nodo. Los datos son propiedad de diferentes SVM.

- Entre SVM, diferentes nodos

  El archivo o las LUN de origen y destino se encuentran en distintos volúmenes ubicados en nodos diferentes. Los datos son propiedad de diferentes SVM.

- Entre clústeres

  Las LUN de origen y de destino se encuentran en distintos volúmenes ubicados en distintos nodos en varios clústeres. Solo se admite en SAN y no funciona para CIFS.

Existen algunos casos de uso especiales adicionales:

- Con la implementación de ODX de ONTAP, se puede utilizar ODX para copiar archivos entre recursos compartidos de SMB y unidades virtuales asociadas a FC o iSCSI.

  Puede utilizar el Explorador de Windows, la CLI de Windows o PowerShell, Hyper-V u otras aplicaciones que admiten ODX para copiar o mover archivos sin problemas mediante la descarga de la copia ODX entre recursos compartidos de SMB y LUN conectados, siempre y cuando los recursos compartidos y las LUN del SMB estén en el mismo clúster.

- Hyper-V proporciona algunos casos de uso adicionales para la descarga de copias ODX:

  - Se puede utilizar la transferencia de la copia ODX mediante Hyper-V para copiar datos dentro o a través de archivos de disco duro virtual (VHD), o bien copiar datos entre recursos compartidos de SMB

asignados y LUN iSCSI conectados dentro del mismo clúster.

Esto permite que las copias de sistemas operativos invitados pasen al almacenamiento subyacente.

- Al crear discos duros virtuales de tamaño fijo, ODX se utiliza para inicializar el disco con ceros, empleando un token de cero conocido.
- La descarga de copias ODX se utiliza para la migración de almacenamiento de máquinas virtuales si el almacenamiento de origen y destino está en el mismo clúster.

> Para aprovechar los casos de uso de un paso a través de la descarga de copias ODX mediante Hyper-V, el sistema operativo invitado debe ser compatible con ODX, mientras que los discos del sistema operativo invitado deben ser discos SCSI respaldados por almacenamiento (tanto SMB COMO SAN) que sean compatibles con ODX. Los discos IDE del sistema operativo invitado no admiten el paso a través de ODX.

Habilitar o deshabilitar ODX en servidores SMB de ONTAP

Es posible habilitar o deshabilitar ODX en máquinas virtuales de almacenamiento (SVM). El valor predeterminado es habilitar la compatibilidad con la descarga de copias ODX si también se habilita SMB 3.0.

Antes de empezar

Se debe habilitar SMB 3.0.

Acerca de esta tarea

Si deshabilita SMB 3.0, ONTAP también deshabilita SMB ODX. Si vuelve a habilitar SMB 3.0, debe volver a habilitar manualmente SMB ODX.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

Si desea que la descarga de copias de ODX sea…	Introduzca el comando…
Activado	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled true`
Deshabilitado	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled false`

3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Ejemplo

En el ejemplo siguiente se habilita la descarga de copias ODX en SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster1::*> set -privilege admin
```

Información relacionada

Opciones de servidor disponibles

Mejore el tiempo de respuesta del cliente al proporcionar referencias automáticas a nodos SMB con ubicación automática

Aprenda a mejorar el tiempo de respuesta del cliente al proporcionar referencias automáticas de nodos SMB de ONTAP con ubicación automática

Auto Location utiliza referencias de nodos automáticas de SMB para aumentar el rendimiento del cliente de SMB en máquinas virtuales de almacenamiento (SVM). Las referencias automáticas a nodos redirigen automáticamente el cliente solicitante a una LIF en la SVM de nodos que aloja el volumen en el que residen los datos, lo que puede mejorar los tiempos de respuesta del cliente.

Cuando un cliente SMB se conecta a un recurso compartido SMB alojado en la SVM, puede conectarse mediante una LIF que está en un nodo que no posee los datos solicitados. El nodo al que está conectado el cliente accede a los datos que pertenece a otro nodo mediante el uso de la red de clústeres. El cliente puede experimentar tiempos de respuesta más rápidos si la conexión SMB utiliza una LIF ubicada en el nodo que contiene los datos solicitados:

- ONTAP proporciona esta funcionalidad al utilizar referencias DFS de Microsoft para informar a los clientes SMB de que un archivo o carpeta solicitados en el espacio de nombres está alojado en otro lugar.

  Un nodo hace una referencia cuando determina que hay una LIF ANSVM en el nodo que contiene los datos.

- Las referencias automáticas de nodos son compatibles con las direcciones IP de LIF IPv4 e IPv6.
- Las referencias se realizan en función de la ubicación de la raíz del recurso compartido a través del cual está conectado el cliente.
- La referencia se produce durante la negociación SMB.

  La referencia se realiza antes de establecer la conexión. Una vez que ONTAP hace referencia al cliente SMB al nodo de destino, se establece la conexión y el cliente accede a los datos a través de la ruta LIF referida desde ese punto de encendido. Esto permite a los clientes acceder con más rapidez a los datos y evita la comunicación adicional del clúster.

Si un recurso compartido abarca varios puntos de unión y algunas uniones están en volúmenes contenidos en otros nodos, los datos del recurso compartido se distribuyen entre varios nodos. Dado que ONTAP proporciona las referencias que son locales a la raíz del recurso compartido, ONTAP debe usar la red de clúster para recuperar los datos contenidos en estos volúmenes no locales. Con este tipo de arquitectura de espacio de nombres, es posible que las referencias automáticas a nodos no ofrezcan importantes beneficios en el rendimiento.

Si el nodo que aloja los datos no tiene una LIF disponible, ONTAP establecerá la conexión mediante la LIF elegida por el cliente. Después de que un cliente SMB abre un archivo, éste continúa accediendo al archivo a través de la misma conexión referida.

Si, por algún motivo, el servidor CIFS no puede hacer una referencia, no se produce ninguna interrupción del servicio SMB. La conexión SMB se establece como si las referencias automáticas a nodos no estuvieran habilitadas.

Información relacionada

Mejora del rendimiento de las copias remotas de Microsoft

Requisitos y pautas para el uso de referencias automáticas de nodos en servidores SMB de ONTAP

Antes de poder utilizar las referencias automáticas de nodos SMB, también conocido como *autoubicación*, debe tener en cuenta ciertos requisitos, como las versiones de ONTAP que admiten esta función. También debe saber acerca de las versiones del protocolo SMB compatibles y otras directrices especiales.

Requisitos de versión y licencia de ONTAP

- Todos los nodos del clúster deben ejecutar una versión de ONTAP que admita las referencias automáticas al nodo.
- Los widgets deben estar habilitados en un recurso compartido SMB para utilizar la autolocalización.
- CIFS debe tener una licencia y el servidor SMB debe existir en las SVM. La licencia SMB se incluye con "ONTAP One". Si no tiene ONTAP One y la licencia no está instalada, póngase en contacto con su representante de ventas.

Requisitos de la versión del protocolo SMB

- Para SVM, ONTAP admite referencias de nodos automáticas en todas las versiones de SMB.

Requisitos del cliente SMB

Todos los clientes de Microsoft compatibles con ONTAP son compatibles con las referencias de nodo automáticas SMB.

La matriz de interoperabilidad contiene la información más reciente sobre los clientes Windows que admite ONTAP.

"Herramienta de matriz de interoperabilidad de NetApp"

Requisitos de LIF de datos

Si desea utilizar una LIF de datos como referencia potencial para los clientes de SMB, debe crear LIF de datos con NFS y CIFS habilitados.

Las referencias automáticas de nodos pueden fallar si el nodo de destino contiene LIF de datos que están habilitadas solo para el protocolo NFS o solo para el protocolo SMB.

Si no se cumple este requisito, el acceso a los datos no se verá afectado. El cliente de SMB asigna el recurso compartido mediante la LIF original que utilizó el cliente para conectarse a la SVM.

Requisitos de autenticación NTLM al realizar una conexión SMB a la que se hace referencia

Se debe permitir la autenticación NTLM en el dominio que contiene el servidor CIFS y en los dominios que contienen clientes que desean utilizar referencias automáticas a nodos.

Al realizar una referencia, el servidor SMB hace referencia a una dirección IP al cliente Windows. Dado que la autenticación NTLM se utiliza al realizar una conexión mediante una dirección IP, la autenticación Kerberos no se realiza para conexiones a las que se hace referencia.

Esto sucede porque el cliente Windows no puede crear el nombre principal de servicio utilizado por Kerberos (que es del formato `service/NetBIOS name` AND `service/FQDN`), lo que significa que el cliente no puede solicitar un ticket de Kerberos al servicio.

Instrucciones para el uso de referencias automáticas de nodos con la función de directorio inicial

Cuando los recursos compartidos se configuran con la propiedad del recurso compartido del directorio principal activada, puede haber una o varias rutas de búsqueda del directorio principal configuradas para una configuración de directorio principal. Las rutas de búsqueda pueden apuntar a los volúmenes contenidos en cada nodo que contiene volúmenes de SVM. Los clientes reciben una referencia y, si hay una LIF de datos local activa disponible, se conectan a través de una LIF de referencia que sea local al directorio raíz del usuario doméstico.

Existen directrices para que los clientes de SMB 1.0 accedan a directorios iniciales dinámicos con referencias de nodos automáticas habilitadas. Esto se debe a que los clientes de SMB 1.0 necesitan la referencia automática al nodo antes de que se hayan autenticado, lo que es antes de que el servidor SMB tenga el nombre del usuario. Sin embargo, el acceso al directorio raíz SMB funciona correctamente para los clientes SMB 1.0 si se cumplen las siguientes afirmaciones:

- Los directorios iniciales de SMB están configurados para usar nombres simples, como "'%w'" (nombre de usuario de Windows) o "'%u'" (nombre de usuario UNIX asignado), y no nombres de estilo de nombre de dominio, como "'%d\%w '" (nombre de dominio\nombre de usuario).
- Al crear recursos compartidos de directorios iniciales, los nombres de los recursos compartidos de directorios iniciales CIFS se configuran con variables ("'%w'" o "'%u'"), y no con nombres estáticos, como «'HOME».

Para los clientes SMB 2.x y SMB 3.0, no hay directrices especiales al acceder a directorios iniciales con referencias automáticas a nodos.

Directrices para deshabilitar las referencias automáticas de nodos en servidores CIFS con conexiones existentes referidas

Si deshabilita las referencias automáticas a nodos después de habilitar la opción, los clientes que están actualmente conectados a una LIF conocida mantienen la conexión referida. Dado que ONTAP utiliza referencias DFS como mecanismo para las referencias automáticas de nodo SMB, los clientes pueden incluso

volver a conectarse a la LIF mencionada después de deshabilitar la opción hasta que se agote el tiempo de espera de la referencia de DFS en caché del cliente para la conexión mencionada. Esto es cierto incluso si se revierte a una versión de ONTAP que no admite referencias automáticas a los nodos. Los clientes continúan utilizando referencias hasta que se agote el tiempo de espera de la referencia DFS desde la memoria caché del cliente.

La ubicación automática utiliza las referencias de nodos automáticos de SMB para aumentar el rendimiento del cliente de SMB al remitir a los clientes a la LIF en el nodo propietario del volumen de datos de una SVM. Cuando un cliente SMB se conecta a un recurso compartido SMB alojado en una SVM, puede conectarse mediante una LIF en un nodo que no posea los datos solicitados y utilice una red de interconexión de clúster para recuperar los datos. El cliente puede experimentar tiempos de respuesta más rápidos si la conexión SMB utiliza una LIF ubicada en el nodo que contiene los datos solicitados.

ONTAP proporciona esta funcionalidad al utilizar referencias del sistema de archivos distribuidos (DFS) de Microsoft para informar a los clientes SMB de que un archivo o una carpeta solicitados en el espacio de nombres se alojan en otro lugar. Un nodo hace una referencia cuando determina que hay una LIF de SVM en el nodo que contiene los datos. Las referencias se realizan en función de la ubicación de la raíz del recurso compartido a través del cual está conectado el cliente.

La referencia se produce durante la negociación SMB. La referencia se realiza antes de establecer la conexión. Una vez que ONTAP hace referencia al cliente SMB al nodo de destino, se establece la conexión y el cliente accede a los datos a través de la ruta LIF referida desde ese punto de encendido. Esto permite a los clientes acceder con más rapidez a los datos y evita la comunicación adicional del clúster.

Instrucciones para el uso de referencias automáticas a nodos con clientes Mac OS

Los clientes de Mac OS X no admiten referencias automáticas de nodos SMB, aunque Mac OS sea compatible con Microsoft Distributed File System (DFS). Los clientes de Windows realizan una solicitud de referencia DFS antes de conectarse a un recurso compartido SMB. ONTAP proporciona una referencia a una LIF de datos que se encuentra en el mismo nodo que aloja los datos solicitados, lo cual mejora los tiempos de respuesta de los clientes. Aunque Mac OS admite DFS, los clientes de Mac OS no se comportan exactamente igual que los clientes de Windows en esta área.

Información relacionada

- Obtenga información sobre cómo habilitar directorios de inicio dinámicos en servidores
- "Gestión de redes"
- "Herramienta de matriz de interoperabilidad de NetApp"

Compatibilidad con referencias automáticas de nodos SMB de ONTAP

Antes de habilitar las referencias automáticas al nodo SMB, tiene que tener en cuenta que ciertas funcionalidades de ONTAP no admiten referencias.

- Los siguientes tipos de volúmenes no son compatibles con las referencias de nodo automáticas del bloque de mensajes del servidor:
  - Miembros de solo lectura de un reflejo de carga compartida
  - Volumen de destino de un reflejo de protección de datos
- Las referencias de nodos no se mueven junto a un movimiento LIF.

  Si un cliente utiliza una conexión a la que se hace referencia a través de una conexión SMB 2.x o SMB 3.0 y una LIF de datos se mueve de forma no disruptiva, el cliente sigue usando la misma conexión a la que se hace referencia, aunque la LIF ya no sea local para los datos.

- Las referencias de los nodos no se mueven junto a un movimiento de volumen.

  Si un cliente está usando una conexión a través de cualquier conexión SMB y se produce un movimiento de volúmenes, el cliente sigue utilizando la misma conexión conocida, aunque el volumen ya no esté ubicado en el mismo nodo que la LIF de datos.

Habilitar o deshabilitar las referencias automáticas de nodos de ONTAP SMB

Puede habilitar las referencias de nodo automáticas para SMB para aumentar el rendimiento del acceso de los clientes SMB. Puede deshabilitar las referencias de nodo automáticas si no desea que ONTAP haga referencias a los clientes SMB.

Antes de empezar

Debe configurarse y ejecutarse un servidor CIFS en la máquina virtual de almacenamiento (SVM).

Acerca de esta tarea

La funcionalidad de referencias automáticas al nodo SMB está deshabilitada de manera predeterminada. Puede habilitar o deshabilitar esta funcionalidad en cada SVM, según sea necesario.

Esta opción está disponible en el nivel de privilegio avanzado.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Habilite o deshabilite las referencias de nodo automáticas para SMB según sea necesario:

Si desea que las referencias automáticas de nodo de SMB sean…	Introduzca el siguiente comando…
Activado	`vserver cifs options modify -vserver vserver_name -is-referral-enabled true`
Deshabilitado	`vserver cifs options modify -vserver vserver_name -is-referral-enabled false`

   La configuración de la opción surte efecto para nuevas sesiones SMB. Los clientes con conexión existente pueden utilizar la referencia de nodo sólo cuando caduque el tiempo de espera de caché existente.

3. Cambie al nivel de privilegio de administrador: `set -privilege admin`

Información relacionada

Opciones de servidor disponibles

Utilice estadísticas para supervisar la actividad de referencia automática de nodos de ONTAP SMB

Para determinar cuántas conexiones SMB se hace referencia, puede supervisar la actividad de referencia automática de nodos mediante `statistics` el comando. Al supervisar las referencias puede determinar en qué medida las referencias automáticas están ubicando conexiones en los nodos que alojan los recursos compartidos y si debe

redistribuir sus LIF de datos para proporcionar un mejor acceso local a los recursos compartidos en el servidor CIFS.

Acerca de esta tarea

`cifs`El objeto proporciona varios contadores en el nivel de privilegio avanzado que son útiles al supervisar referencias automáticas de nodos SMB:

- `node_referral_issued`

  Número de clientes a los que se ha emitido una referencia al nodo de la raíz compartida después de que el cliente se haya conectado mediante una LIF alojada por un nodo diferente al nodo de la raíz compartida.

- `node_referral_local`

  Número de clientes que se conectan mediante una LIF alojada por el mismo nodo que aloja la raíz compartida. El acceso local generalmente proporciona un rendimiento óptimo.

- `node_referral_not_possible`

  Número de clientes que no se han emitido una referencia al nodo que aloja el recurso compartido raíz tras la conexión mediante una LIF alojada por un nodo diferente al nodo raíz del recurso compartido. Esto se debe a que no se encontró una LIF de datos activa para el nodo raíz del recurso compartido.

- `node_referral_remote`

  Número de clientes que se conectan mediante una LIF alojada por un nodo diferente al nodo que aloja la raíz compartida. El acceso remoto puede provocar una degradación del rendimiento.

Es posible supervisar las estadísticas de referencia automática de nodos en la máquina virtual de almacenamiento (SVM) mediante la recopilación y la visualización de datos de un período de tiempo específico (una muestra). Puede ver los datos de la muestra si no detiene la recopilación de datos. Al detener la recopilación de datos, se proporciona una muestra fija. No detener la recopilación de datos le ofrece la posibilidad de obtener datos actualizados que puede utilizar para compararlos con consultas anteriores. La comparativa puede ayudarle a identificar las tendencias de rendimiento.

Para evaluar y utilizar la información que recopila del `statistics` comando, debe comprender la distribución de los clientes en sus entornos.

Pasos

1. Establezca el nivel de privilegio en avanzado: `set -privilege advanced`
2. Para ver estadísticas automáticas de referencia de nodo `statistics`, utilice el comando.

   En este ejemplo, se visualizan y recogen estadísticas de referencia automática de nodos:

   a. Inicie la colección: `statistics start -object cifs -instance vs1 -sample-id sample1`

```
Statistics collection is being started for Sample-id: sample1
```

b. Espere a que transcurra el tiempo de recogida deseado.

c. Detener la colección: `statistics stop -sample-id sample1`

```
Statistics collection is being stopped for Sample-id: sample1
```

Obtenga más información sobre `statistics start` y `statistics stop` en el "Referencia de comandos del ONTAP" .

d. Vea las estadísticas automáticas de referencia de nodo: `statistics show -sample-id sample1 -counter` **`node`**

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1

    Counter                                     Value
    --------------------------- ----------------------------
    node_name                                   node1
    node_referral_issued                            0
    node_referral_local                             1
    node_referral_not_possible                      2
    node_referral_remote                            2
    ...

    node_name                                   node2
    node_referral_issued                            2
    node_referral_local                             1
    node_referral_not_possible                      0
    node_referral_remote                            2
    ...
```

La salida muestra los contadores de todos los nodos que participan en SVM vs1. Para mayor claridad, en el ejemplo solo se proporcionan los campos de salida relacionados con las estadísticas automáticas de referencia de nodos.

Obtenga más información sobre `statistics show` en el "Referencia de comandos del ONTAP".

3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Información relacionada

- Mostrar estadísticas
- "Configuración de supervisión del rendimiento"

Supervisar la información de referencia automática de nodos de ONTAP SMB del lado del cliente mediante un cliente de Windows

Para determinar qué referencias se hacen desde la perspectiva del cliente, puede usar la `dfsutil.exe` utilidad de Windows.

El kit de herramientas de administración remota del servidor (RSAT) disponible con clientes de Windows 7 y posteriores contiene la `dfsutil.exe` utilidad. Con esta utilidad, puede mostrar información acerca del contenido de la caché de referencias así como ver información acerca de cada referencia que esté utilizando actualmente el cliente. También puede utilizar la utilidad para borrar la memoria caché de referencia del cliente. Para obtener más información, consulte la biblioteca de Microsoft TechNet.

Información relacionada

"Biblioteca de Microsoft TechNet: technet.microsoft.com/en-us/library/"

Proporcione seguridad de carpetas en recursos compartidos con enumeración basada en acceso

Proporcionar seguridad de carpetas SMB de ONTAP en recursos compartidos con enumeración basada en acceso

Cuando se habilita la enumeración basada en acceso (ABE) en un recurso compartido SMB, los usuarios que no tienen permiso para acceder a una carpeta o archivo contenido en el recurso compartido (ya sea mediante restricciones de permisos individuales o de grupo) no ven el recurso compartido que se muestra en su entorno, aunque el recurso compartido en sí sigue siendo visible.

Las propiedades de uso compartido convencionales permiten especificar qué usuarios (individualmente o en grupos) tienen permiso para ver o modificar archivos o carpetas contenidos en el recurso compartido. Sin embargo, no le permiten controlar si las carpetas o archivos dentro del recurso compartido son visibles para los usuarios que no tienen permiso para tener acceso a ellos. Esto podría plantear problemas si los nombres de estas carpetas o archivos del recurso compartido describen información confidencial, como los nombres de los clientes o los productos en desarrollo.

La enumeración basada en acceso (ABE) amplía las propiedades de recursos compartidos para incluir la enumeración de archivos y carpetas dentro del recurso compartido. POR tanto, ABE permite filtrar la visualización de archivos y carpetas dentro del recurso compartido en función de los derechos de acceso del usuario. Es decir, el recurso compartido en sí sería visible para todos los usuarios, pero los archivos y carpetas dentro del recurso compartido podrían mostrarse u ocultarse de los usuarios designados. Además de proteger la información confidencial en su lugar de trabajo, ABE le permite simplificar la presentación de grandes estructuras de directorio en beneficio de los usuarios que no necesitan acceso a su gama completa de contenido. Por ejemplo, el recurso compartido en sí sería visible para todos los usuarios, pero los archivos y carpetas dentro del recurso compartido podrían mostrarse u ocultarse.

Obtenga más información "Impacto sobre el rendimiento al utilizar la enumeración basada en SMB/CIFS Access"sobre .

Habilitar o deshabilitar la enumeración basada en acceso en recursos compartidos SMB de ONTAP

Puede habilitar o deshabilitar la enumeración basada en acceso (ABE) en recursos compartidos SMB para permitir o impedir que los usuarios vean recursos compartidos a

los que no tienen permiso para acceder.

Acerca de esta tarea

De forma predeterminada, ABE está desactivado.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el comando…
Habilite ABE en un nuevo recurso compartido	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration` Puede especificar configuraciones de recursos compartidos opcionales y propiedades de recursos compartidos adicionales al crear un recurso compartido de SMB. Obtenga más información sobre `vserver cifs share create` en el "Referencia de comandos del ONTAP".
Habilite ABE en un recurso compartido existente	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` Se conservan las propiedades de recurso compartido existentes. La propiedad ABE share se agrega a la lista existente de propiedades compartidas.
Deshabilite ABE en un recurso compartido existente	`vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` Se conservan otras propiedades de recurso compartido. Sólo la propiedad compartida ABE se elimina de la lista de propiedades de recursos compartidos.

2. Compruebe que la configuración del recurso compartido sea correcta mediante `vserver cifs share show` el comando.

Ejemplos

El siguiente ejemplo crea un recurso compartido SMB de ABE llamado “ventas” con una ruta de `/sales` en SVM VS1. El recurso compartido se crea con `access-based-enumeration` como propiedad de recurso compartido:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales  -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

                      Vserver: vs1
                        Share: sales
     CIFS Server NetBIOS Name: VS1
                         Path: /sales
            Share Properties: access-based-enumeration
                              oplocks
                              browsable
                              changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

El siguiente ejemplo agrega la `access-based-enumeration` propiedad de recurso compartido a un recurso compartido SMB llamado «ATA2»:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
------- ---------- ------------------------------------------------------
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration
```

Información relacionada

Agregar o eliminar propiedades de recursos compartidos en recursos compartidos existentes

Habilitar o deshabilitar la enumeración basada en acceso desde un cliente de Windows en recursos compartidos SMB de ONTAP

Puede habilitar o deshabilitar la enumeración basada en acceso (ABE) en recursos compartidos SMB desde un cliente Windows, que permite configurar esta configuración de recurso compartido sin tener que conectarse al servidor CIFS.

`abecmd`La utilidad no está disponible en nuevas versiones de Windows Server y clientes Windows. Se lanzó como parte de Windows Server 2008. El soporte finalizó para Windows Server 2008 el 14 de enero de 2020.

Pasos

1. Desde un cliente Windows compatible con ABE, introduzca el siguiente comando: `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

   Para obtener más información acerca `abecmd` del comando, consulte la documentación del cliente de Windows.

Dependencias de nomenclatura de archivos y directorios NFS y SMB

Obtenga información sobre las dependencias de nombres de archivos y directorios de ONTAP NFS y SMB

Las convenciones de nomenclatura de archivos y directorios dependen tanto de los sistemas operativos de los clientes de red como de los protocolos de uso compartido de archivos, además de la configuración de idioma del clúster ONTAP y de los clientes.

El sistema operativo y los protocolos de uso compartido de archivos determinan lo siguiente:

- Caracteres que puede utilizar un nombre de archivo
- Distinción entre mayúsculas y minúsculas de un nombre de archivo

ONTAP admite caracteres de varios bytes en nombres de archivos, directorios y qtrees, según la versión de ONTAP.

Obtenga información sobre los caracteres válidos para los nombres de archivos o directorios SMB de ONTAP

Si accede a un archivo o directorio desde clientes con sistemas operativos diferentes, debe utilizar caracteres válidos en ambos sistemas operativos.

Por ejemplo, si utiliza UNIX para crear un archivo o directorio, no utilice dos puntos (:) en el nombre porque no se permiten dos puntos en los nombres de archivos o directorios de MS-dos. Debido a que las restricciones de caracteres válidos varían de un sistema operativo a otro, consulte la documentación del sistema operativo cliente para obtener más información acerca de los caracteres prohibidos.

Distinción entre mayúsculas y minúsculas en los nombres de archivos y directorios SMB de ONTAP en un entorno multiprotocolo

Los nombres de archivo y directorio distinguen mayúsculas y minúsculas para los clientes NFS y no distinguen entre mayúsculas y minúsculas, pero sí lo hacen para los clientes SMB. Debe comprender las implicaciones que tiene en un entorno multiprotocolo y las acciones que podría tener que tomar al especificar la ruta al crear recursos compartidos de SMB y al acceder a datos dentro de los recursos compartidos.

Si un cliente SMB crea un directorio denominado `testdir`, los clientes SMB y NFS muestran el nombre del archivo como `testdir`. Sin embargo, si un usuario SMB intenta crear un nombre de directorio más adelante

`TESTDIR` , el nombre no está permitido porque, para el cliente SMB, ese nombre existe actualmente. Si un usuario NFS crea posteriormente un directorio denominado `TESTDIR`, los clientes NFS y SMB muestran el nombre del directorio de forma diferente, de la siguiente manera:

- En los clientes NFS, puede ver los nombres de directorio a medida que se crearon, por ejemplo `testdir` y `TESTDIR`, porque los nombres de directorio distinguen entre mayúsculas y minúsculas.
- Los clientes SMB utilizan los nombres 8.3 para distinguir entre los dos directorios. Un directorio tiene el nombre del archivo base. A directorios adicionales se les asigna un nombre de archivo 8.3.
  - En clientes SMB, puede ver `testdir` y `TESTDI~1`.
  - ONTAP crea el `TESTDI~1` nombre del directorio para diferenciar los dos directorios.

    En este caso, debe usar el nombre 8.3 al especificar una ruta de recurso compartido mientras crea o modifica un recurso compartido en una máquina virtual de almacenamiento (SVM).

Del mismo modo para los archivos, si un cliente SMB lo crea `test.txt`, los clientes SMB y NFS muestran el nombre del archivo como `text.txt`. Sin embargo, si un usuario SMB intenta crear `Test.txt`, el nombre no está permitido porque, para el cliente SMB, ese nombre existe actualmente. Si un usuario NFS crea posteriormente un archivo denominado `Test.txt`, los clientes NFS y SMB muestran el nombre del archivo de forma diferente, de la siguiente manera:

- En los clientes NFS, verá los nombres de archivo a medida que se crearon y `test.txt` `Test.txt` , porque los nombres de archivo distinguen entre mayúsculas y minúsculas.
- Los clientes SMB utilizan los nombres 8.3 para distinguir entre los dos archivos. Un archivo tiene el nombre del archivo base. Se asigna un nombre de archivo 8.3 a archivos adicionales.
  - En clientes SMB, puede ver `test.txt` y `TEST~1.TXT`.
  - ONTAP crea el `TEST~1.TXT` nombre de archivo para diferenciar los dos archivos.

> Si ha habilitado o modificado la asignación de caracteres mediante los comandos de asignación de caracteres CIFS del Vserver, una búsqueda de Windows normalmente no distingue mayúsculas y minúsculas se convierte en sensible a mayúsculas y minúsculas.

Aprenda a crear nombres de archivos y directorios SMB de ONTAP

ONTAP crea y mantiene dos nombres para archivos o directorios en cualquier directorio que tenga acceso desde un cliente SMB: El nombre largo original y un nombre en formato 8.3.

Para los nombres de archivos o directorios que excedan el nombre de ocho caracteres o el límite de extensión de tres caracteres (para archivos), ONTAP genera un nombre de formato de 8.3 de la siguiente manera:

- Trunca el nombre del archivo o directorio original a seis caracteres, si el nombre supera los seis.
- Agrega una tilde (~) y un número, de uno a cinco, a los nombres de archivo o directorio que ya no son únicos después de truncarse.

  Si se queda sin números porque hay más de cinco nombres similares, crea un nombre único que no tiene relación con el nombre original.

- En el caso de los archivos, trunca la extensión del nombre de archivo a tres caracteres.

Por ejemplo, si un cliente NFS crea un archivo llamado `specifications.html`, el nombre de archivo de formato 8,3 creado por ONTAP es `specif~1.htm`. Si este nombre ya existe, ONTAP utiliza un número diferente al final del nombre de archivo. Por ejemplo, si un cliente NFS crea otro archivo denominado `specifications_new.html`, el formato 8,3 de `specifications_new.html` es `specif~2.htm`.

Obtenga información sobre los nombres de archivos, directorios y qtree multibyte SMB de ONTAP

A partir de ONTAP 9.5, la compatibilidad con nombres codificados UTF-8 de 4 bytes permite la creación y visualización de nombres de archivos, directorios y árboles que incluyen caracteres complementarios Unicode fuera del plano multilingüe básico (BMP). En las versiones anteriores, estos caracteres complementarios no se mostraba correctamente en entornos multiprotocolo.

Para habilitar la compatibilidad con nombres codificados UTF-8 de 4 bytes, hay disponible un nuevo código de idioma *utf8mb4* para las `vserver volume` familias de comandos y.

Debe crear un nuevo volumen de una de las siguientes maneras:

- Configuración `-language` explícita de la opción volume: `volume create -language utf8mb4 {…}`
- Heredar `-language` la opción de volumen de una SVM que se haya creado o modificado para la opción: `vserver [create|modify] -language utf8mb4 {…}``volume create {…}`
- En ONTAP 9,6 y versiones anteriores, no puede modificar los volúmenes existentes para la compatibilidad con utf8mb4. Debe crear un volumen listo para utf8mb4 y después migrar los datos con las herramientas de copia basadas en cliente.

  Puede actualizar las SVM para que admitan utf8mb4, pero los volúmenes existentes conservan sus códigos de idioma originales.

  Si utiliza ONTAP 9.7P1 o una versión posterior, puede modificar los volúmenes existentes para utf8mb4 con una solicitud de soporte. Para obtener más información, consulte "¿Se puede cambiar el idioma del volumen después de crearlo en ONTAP?".

- A partir de ONTAP 9.8, puede usar `[-language <Language code>]` el parámetro para cambiar el idioma del volumen de *.utf-8 a utf8mb4. Para cambiar el idioma de un volumen, póngase en contacto con "Soporte de NetApp".

  Los nombres de las LUN con caracteres UTF-8 de 4 bytes no se admiten actualmente.

- Los datos de caracteres Unicode se suelen representar en aplicaciones de sistemas de archivos Windows que utilizan el formato de transformación Unicode de 16 bits (UTF-16) y en sistemas de archivos NFS que utilizan el formato de transformación Unicode de 8 bits (UTF-8).

  En las versiones anteriores a ONTAP 9.5, los nombres incluidos los caracteres complementarios UTF-16 creados por los clientes de Windows se mostraban correctamente a otros clientes de Windows pero no se tradujeron correctamente a UTF-8 para los clientes NFS. Del mismo modo, los nombres con caracteres complementarios UTF-8 de los clientes NFS creados no se tradujeron correctamente a UTF-16 para los clientes Windows.

- Cuando se crean nombres de archivo en sistemas que ejecutan ONTAP 9.4 o una versión anterior que contienen caracteres complementarios válidos o no válidos, ONTAP rechaza el nombre de archivo y devuelve un error de nombre de archivo no válido.

Para evitar este problema, utilice sólo los caracteres BMP en los nombres de archivo y evite utilizar caracteres complementarios, o actualice a ONTAP 9.5 o posterior.

A partir de ONTAP 9, se permiten caracteres Unicode en nombres de qtree.

- Puede usar `volume qtree` la familia de comandos o System Manager para configurar o modificar los nombres de qtree.
- Los nombres de qtree pueden incluir caracteres de varios bytes en formato Unicode, como los caracteres japoneses y chinos.
- En versiones anteriores a ONTAP 9.5, sólo se admiten los caracteres BMP (es decir, los que podrían representarse en 3 bytes).

> En las versiones anteriores a ONTAP 9.5, la ruta de unión del volumen principal del qtree puede contener nombres de qtree y directorio con caracteres Unicode. El `volume show` comando muestra estos nombres correctamente cuando el volumen primario tiene una configuración de idioma UTF-8. Sin embargo, si el idioma del volumen principal no es uno de los valores de idioma UTF-8, algunas partes de la ruta de unión se muestran utilizando un nombre NFS alternativo numérico.

- En las versiones 9.5 y posteriores, se admiten caracteres de 4 bytes en nombres de qtree, siempre y cuando el qtree se encuentre en un volumen habilitado para utf8mb4.

Configurar la asignación de caracteres para la traducción de nombres de archivos SMB de ONTAP en volúmenes

Los clientes NFS pueden crear nombres de archivo que contengan caracteres que no son válidos para los clientes SMB y ciertas aplicaciones Windows. Puede configurar la asignación de caracteres para la traducción de nombres de archivo en volúmenes para permitir que los clientes SMB accedan a archivos con nombres NFS que, de lo contrario, no serían válidos.

Acerca de esta tarea

Cuando los clientes SMB acceden a los archivos creados por los clientes NFS, ONTAP observa el nombre del archivo. Si el nombre no es un nombre de archivo SMB válido (por ejemplo, si tiene un carácter "':'" incrustado en dos puntos), ONTAP devuelve el nombre de archivo 8.3 que se mantiene para cada archivo. Sin embargo, esto causa problemas para las aplicaciones que codifican información importante en nombres de archivos largos.

Por lo tanto, si comparte un archivo entre clientes en diferentes sistemas operativos, debe utilizar caracteres en los nombres de archivo válidos en ambos sistemas operativos.

Sin embargo, si tiene clientes NFS que crean nombres de archivo que contienen caracteres que no son nombres de archivo válidos para clientes SMB, puede definir un mapa que convierte los caracteres NFS no válidos en caracteres Unicode que tanto SMB como determinadas aplicaciones Windows aceptan. Por ejemplo, esta funcionalidad admite las aplicaciones CATIA MCAD y Mathematica, así como otras aplicaciones que tienen este requisito.

Puede configurar la asignación de caracteres de volumen a volumen.

Debe tener en cuenta lo siguiente al configurar la asignación de caracteres en un volumen:

- La asignación de caracteres no se aplica a través de puntos de unión.

  Debe configurar explícitamente la asignación de caracteres para cada volumen de unión.

- Debe asegurarse de que los caracteres Unicode que se utilizan para representar caracteres no válidos o ilegales son caracteres que normalmente no aparecen en los nombres de archivo; de lo contrario, se producen asignaciones no deseadas.

  Por ejemplo, si intenta asignar dos puntos (:) a un guión (-) pero el guión (-) se utilizó correctamente en el nombre del archivo, un cliente de Windows que intente acceder a un archivo denominado «'a-b'» tendría su solicitud asignada al nombre NFS de «'a:b'» (no al resultado deseado).

- Después de aplicar la asignación de caracteres, si la asignación aún contiene un carácter de Windows no válido, ONTAP vuelve a los nombres de archivo de Windows 8.3.
- En las notificaciones de FPolicy, los registros de auditoría de NAS y los mensajes de seguimiento de seguridad, se muestran los nombres de archivos asignados.
- Cuando se crea una relación de SnapMirror del tipo DP, la asignación de caracteres del volumen de origen no se replica en el volumen de DP de destino.
- Distinción entre mayúsculas y minúsculas: Debido a que los nombres de Windows asignados se convierten en nombres NFS, la búsqueda de los nombres sigue a la semántica NFS. Esto incluye el hecho de que las búsquedas de NFS distinguen mayúsculas de minúsculas. Esto significa que las aplicaciones que acceden a recursos compartidos asignados no deben depender de un comportamiento que no distingue mayúsculas y minúsculas de Windows. Sin embargo, el nombre 8.3 está disponible y no distingue mayúsculas y minúsculas.
- Asignaciones parciales o no válidas: Tras asignar un nombre para devolver a los clientes que realizan enumeración de directorios ("dir"), se comprueba la validez de Windows en el nombre Unicode resultante. Si ese nombre sigue teniendo caracteres no válidos, o si no es válido para Windows (p. ej., finaliza en "". o en blanco) se devuelve el nombre 8.3 en lugar del nombre no válido.

Paso

1. Configurar asignación de caracteres: +

`vserver cifs character-mapping create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-mapping` *`mapping_text`*`, …` +

El mapeo consta de una lista de pares de caracteres fuente-objetivo separados por "':'". Los caracteres son caracteres Unicode introducidos mediante dígitos hexadecimales. Por ejemplo: 3C:E03C. +

El primer valor de cada `mapping_text` par que está separado por dos puntos es el valor hexadecimal del carácter NFS que desea traducir, y el segundo valor es el valor Unicode que utiliza SMB. Las parejas de asignación deben ser únicas (debe existir una asignación uno a uno).

- Asignación de fuentes +

La siguiente tabla muestra el conjunto de caracteres Unicode permisible para la asignación de origen:

+

Carácter Unicode	Carácter impreso	Descripción
0x01-0x19	No aplicable	Caracteres de control que no se imprimen

Carácter Unicode	Carácter impreso	Descripción
0x5C		Barra invertida
0x3A	:	Dos puntos
0x2A	*	Asterisco
0x3F	?	Signo de interrogación
0x22	"	Entre comillas
0x3C	<	Menor que
0x3E	>	Mayor que
0x7C		
Línea vertical	0xB1	±

- Asignación de objetivos

  Puede especificar caracteres de destino en el "'Área de uso privado'" de Unicode en el siguiente intervalo: U+E0000…U+F8FF.

Ejemplo

El siguiente comando crea una asignación de caracteres para un volumen denominado «data» en la máquina virtual de almacenamiento (SVM) vs1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  -----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

Información relacionada

Obtenga información sobre cómo crear y administrar volúmenes de datos en espacios de nombres

Comandos ONTAP para administrar asignaciones de caracteres para la traducción de nombres de archivos SMB

Puede gestionar la asignación de caracteres creando, modificando, mostrando información o eliminando asignaciones de caracteres de archivo utilizadas para la traducción del nombre del archivo SMB en volúmenes FlexVol.

Si desea…	Se usa este comando…
Cree nuevas asignaciones de caracteres de archivo	`vserver cifs character-mapping create`
Mostrar información acerca de las asignaciones de caracteres de archivo	`vserver cifs character-mapping show`
Modifique las asignaciones de caracteres de archivo existentes	`vserver cifs character-mapping modify`
Eliminar asignaciones de caracteres de archivo	`vserver cifs character-mapping delete`

Obtenga más información sobre `vserver cifs character-mapping` en el "Referencia de comandos del ONTAP".

Información relacionada

Configurar la asignación de caracteres para la traducción de nombres de archivos en volúmenes

Proporcione acceso del cliente S3 a los datos NAS

Obtenga más información sobre la compatibilidad multiprotocolo de ONTAP S3

A partir de ONTAP 9.12.1, puede permitir que los clientes que ejecutan el protocolo S3 accedan a los mismos datos que los clientes que utilizan los protocolos NFS y SMB sin necesidad de volver a formatear. Esta funcionalidad permite seguir proporcionando datos de NAS a los clientes NAS, a la vez que presenta datos de objetos a clientes S3 que ejecutan aplicaciones S3 (como la minería de datos y la inteligencia artificial).

La funcionalidad multiprotocolo de S3 aborda dos casos prácticos:

1. Acceso a los datos NAS existentes mediante clientes S3

   Si sus datos existentes se crearon utilizando clientes NAS tradicionales (NFS o SMB) y están ubicados en volúmenes NAS (volúmenes FlexVol o FlexGroup), puede usar herramientas analíticas en clientes S3 para acceder a estos datos.

2. Almacenamiento back-end para clientes modernos capaces de realizar I/o mediante protocolos NAS y S3

   Puede proporcionar acceso integrado para aplicaciones como Spark y Kafka que pueden leer y escribir los mismos datos utilizando los protocolos NAS y S3.

Funcionamiento del soporte multiprotocolo de S3

La compatibilidad con múltiples protocolos de ONTAP le permite presentar el mismo conjunto de datos como una jerarquía de archivos o como objetos en un depósito. Para ello, ONTAP crea "depósitos NAS S3" que permiten a los clientes S3 crear, leer, eliminar y enumerar archivos en el almacenamiento NAS mediante solicitudes de objetos S3. Esta asignación se ajusta a la configuración de seguridad del NAS, observando los permisos de acceso a archivos y directorios, y escribiendo en el registro de auditoría de seguridad según sea necesario.

Esta asignación se logra presentando una jerarquía de directorios NAS especificada como bloque de S3. Cada archivo de la jerarquía de directorio se representa como un objeto S3 cuyo nombre es relativo del directorio asignado hacia abajo, con límites de directorio representados por el carácter de barra diagonal ('/').

Los usuarios S3 definidos por ONTAP pueden acceder a este almacenamiento, según lo establecido por las políticas de buckets definidas para el bucket que se asigna al directorio NAS. Para que esto sea posible, deben definirse las asignaciones entre los usuarios de S3 y los usuarios SMB/NFS. Las credenciales del usuario SMB/NFS se utilizarán para la comprobación de permisos NAS y se incluirán en los registros de auditoría resultantes de estos accesos.

Cuando los clientes SMB o NFS lo crean, un archivo se coloca inmediatamente en un directorio y, por lo tanto, es visible para los clientes antes de escribir ningún dato en él. Los clientes S3 esperan una semántica diferente, en la que el nuevo objeto no esté visible en el espacio de nombres hasta que todos sus datos se hayan escrito. Esta asignación de S3 a almacenamiento NAS crea archivos mediante la semántica de S3, y mantiene los archivos invisibles de forma externa hasta que finaliza el comando de creación de S3.

Protección de datos para bloques NAS de S3

Los "buckets" NAS S3 son simplemente asignaciones de datos NAS para clientes S3, no son buckets S3 estándar. Por lo tanto, no es necesario proteger los buckets NAS S3 mediante la funcionalidad NetApp SnapMirror S3. En su lugar, puede proteger los volúmenes que contienen depósitos NAS S3 mediante la replicación de volumen asincrónica de SnapMirror . No se admiten la recuperación ante desastres sincrónica de SnapMirror ni SVM.

A partir de la versión 9.14.1 de ONTAP, los buckets NAS de S3 se admiten en agregados reflejados y no reflejados para las configuraciones de MetroCluster IP y FC.

Obtenga más información "SnapMirror asíncrono"sobre .

Auditoría de bloques NAS de S3

Dado que los bloques NAS de S3 no son bloques S3 convencionales, la auditoría de S3 no se puede configurar para auditar el acceso entre ellos. Más información sobre "Auditoría de S3".

No obstante, los archivos y directorios NAS que se asignan en bloques NAS de S3 pueden auditarse para eventos de acceso mediante procedimientos de auditoría ONTAP convencionales. Por lo tanto, las operaciones de S3 pueden activar eventos de auditoría de NAS, con las siguientes excepciones:

- Si la configuración de la política de S3 (grupo o política de bloques) deniega el acceso del cliente S3, no se inicia la auditoría de NAS para el evento. Esto se debe a que se comprueban los permisos de S3 antes de poder realizar comprobaciones de auditoría de SVM.
- Si el archivo de destino de una solicitud Get de S3 tiene un tamaño 0, se devuelve 0 contenido a la solicitud Get y el acceso de lectura no se registra.
- Si el archivo de destino de una solicitud Get de S3 se encuentra en una carpeta para la que el usuario no tiene permisos de recorrido, el intento de acceso falla y el evento no se registra.

Obtenga más información "Auditoría de eventos NAS en SVM"sobre .

Carga de varias partes de objeto

A partir de ONTAP 9.16.1, la carga de varias partes de objetos es compatible en bloques NAS de S3 cuando "equilibrado de capacidad avanzado" se habilita en el volumen FlexGroup subyacente.

La carga de varias partes de objetos en el almacenamiento de archivos NAS permite a un cliente de protocolo

S3 cargar un objeto grande como piezas más pequeñas. La carga de varias partes de objetos tiene las siguientes ventajas:

- Permite cargar objetos en paralelo.
- En caso de que se produzca un error de carga o una pausa, solo se deberán cargar las piezas que aún no se hayan cargado. No es necesario reiniciar la carga del objeto completo.
- Si el tamaño del objeto no se conoce por adelantado (por ejemplo, cuando todavía se escribe un objeto grande), los clientes pueden comenzar a cargar partes del objeto inmediatamente y completar la carga después de que se haya creado todo el objeto.

> Los objetos multiparte en los buckets NAS de S3 deben alinearse en tamaños enteros, no parciales. Por ejemplo, una parte puede ser de 4MB o 4GB o un tamaño similar. Una parte no puede usar tamaños parciales o menores a 1MB, como 4.5MB o 4000.5MB.

La carga de varias partes admite las siguientes S3 acciones:

- AbortMultipartUpload
- CompleteMultipartUpload
- CopyObject (a partir de ONTAP 9.17.1)
- CreateMultipartUpload

  A partir de ONTAP 9.17.1, CreateMultipartUpload admite el etiquetado y los pares clave/valor de metadatos de usuario.

- ListMultipartUpload
- UploadPart

> LA OBTENCIÓN por número de pieza («PARTNUMBER=xx») no es compatible con los bloques NAS S3. En su lugar, se devolverá el objeto completo.

Interoperabilidad con S3 y NAS

Los bloques NAS de ONTAP S3 admiten las funcionalidades estándar de NAS y S3, a excepción de las enumeradas aquí.

La funcionalidad NAS no es compatible actualmente con bloques NAS de S3

Nivel de capacidad de FabricPool

S3 Los bloques NAS no pueden configurarse como nivel de capacidad para FabricPool.

Acciones y funcionalidad de S3 no admitidas actualmente por buckets NAS de S3

Acciones

- ByPassGovernanceRetention
- DeleteBucketLifecycleConfiguration
- GetBucketLifecycleConfiguration
- GetBucketObjectLockConfiguration
- GetBucketVersioning

- GetObjectRetention
- Control de versiones de lista
- ListObjectVersions
- PutBucketLifecycleConfiguration
- PutBucketVersioning
- PutObjectLockConfiguration
- PutObjectRetention

Estas acciones de S3 no son compatibles específicamente cuando se utiliza S3 en bloques de NAS de S3. Cuando se utilizan cubos S3 nativos, estas acciones son "compatible con normalidad".

Metadatos de usuario de AWS

- A partir de ONTAP 9.17.1, compatibilidad con metadatos con objetos multiparte.
- A partir de ONTAP 9.16.1, soporte para metadatos con objetos de una sola parte.
- Para ONTAP 9.15.1 y versiones anteriores, los pares clave-valores recibidos como parte de los metadatos del usuario S3 no se almacenan en el disco junto con los datos de los objetos.
- Para ONTAP 9.15.1 y versiones anteriores, se ignoran los encabezados de solicitud con el prefijo “x-amz-meta”.

Etiquetas de AWS

- A partir de ONTAP 9.17.1, compatibilidad con etiquetas con objetos multiparte.
- A partir de ONTAP 9.16.1, compatibilidad con etiquetas con objetos de una sola parte.
- Para ONTAP 9.15.1 y versiones anteriores en las solicitudes PUT y Multipart Initiate, se ignoran las cabeceras con el prefijo «x-amz-tagging».
- Para ONTAP 9.15.1 y versiones anteriores, las solicitudes de actualización de etiquetas en un archivo existente (solicitudes PUT, GET y Delete con la cadena de consulta de etiquetado) se rechazan con un error.

Creación de versiones

No es posible especificar el control de versiones en la configuración de asignación de bloques.

- Las solicitudes que incluyen especificaciones de versión no nulas (el ID de versión=cadena de consulta xyz) reciben respuestas de error.
- Las solicitudes que afectan al estado de control de versiones de un bloque se rechazan con errores.

Obtenga información sobre los requisitos de datos NAS para el acceso del cliente ONTAP S3

Es importante comprender que hay algunas incompatibilidades inherentes a la asignación de archivos y directorios NAS para el acceso S3. Puede que sea necesario ajustar las jerarquías de archivos NAS antes de servirles mediante bloques NAS de S3.

Un bloque NAS de S3 proporciona acceso de S3 a un directorio NAS al asignar ese directorio mediante la sintaxis de bloque de S3, y los archivos del árbol de directorios se consideran objetos. Los nombres de objeto son los nombres de ruta delimitados por barras de los archivos en relación con el directorio especificado en la

configuración de bloque de S3.

Este mapa impone algunos requisitos cuando se sirven archivos y directorios mediante bloques NAS de S3:

- Los nombres de S3 están limitados a 1024 bytes, de modo que no se puede acceder a los archivos con nombres de ruta más largos mediante S3.
- Los nombres de archivo y directorio están limitados a 255 caracteres, por lo que el nombre de objeto no puede tener más de 255 caracteres consecutivos que no sean de barra (“b/”)
- En su lugar, un nombre de ruta SMB delimitado por caracteres de barra diagonal inversa ('\') aparecerá en s3 como nombre de objeto que contiene caracteres de barra diagonal ('/').
- Algunos pares de nombres de objetos S3 legales no pueden coexistir en el árbol de directorio NAS mapeado. Por ejemplo, los nombres de objetos S3 legales "part1/part2" y "part1/part2/part3" se asignan a archivos que no pueden existir simultáneamente en el árbol de directorios NAS, ya que "part1/part2" es un archivo en el primer nombre y un directorio en el otro.
  - Si "part1/part2" es un archivo existente, la creación de "part1/part2/part3" por parte de S3 fallará.
  - Si "part1/part2/part3" es un archivo existente, la creación o eliminación de "part1/part2" por parte de S3 fallará.
  - Una creación de objetos S3 que se ajuste al nombre de un objeto existente sustituye al objeto preexistente (en bloques sin versiones), que se conserva en NAS pero requiere una coincidencia exacta. Los ejemplos anteriores no provocarán la eliminación del objeto existente porque mientras los nombres chocan, no coinciden.

Si bien un almacén de objetos está diseñado para admitir una gran cantidad de nombres arbitrarios, una estructura de directorio NAS puede experimentar problemas de rendimiento si se coloca una gran cantidad de nombres en un directorio. En particular, los nombres que no tengan caracteres de barra ('/') se colocarán en el directorio raíz de la asignación de NAS. Las aplicaciones que hacen un uso extensivo de nombres que no son compatibles con NAS se alojarían mejor en un almacén de objetos real en lugar de en un mapeo NAS.

Habilitar el acceso del protocolo S3 a los datos NAS en un SVM de ONTAP

Habilitar el acceso al protocolo S3 consiste en garantizar que una SVM habilitada para NAS cumpla los mismos requisitos que un servidor habilitado para S3, incluyendo la adición de un servidor de almacén de objetos y la verificación de los requisitos de red y autenticación.

Para nuevas instalaciones de ONTAP, es recomendable habilitar el acceso del protocolo S3 a una SVM después de configurarlo para que sirva datos NAS a los clientes. Para obtener más información sobre la configuración del protocolo NAS, consulte:

- "Configuración de NFS"
- "Configuración de SMB"

Antes de empezar

Debe configurarse lo siguiente antes de habilitar el protocolo S3:

- Tiene licencia el protocolo S3 y los protocolos NAS deseados (NFS, SMB o ambos).
- Una SVM está configurada para los protocolos NAS deseados.
- Existen servidores NFS y/o SMB.
- DNS y cualquier otro servicio requerido están configurados.

- Los datos NAS se exportan o comparten a sistemas cliente.

Acerca de esta tarea

Se requiere un certificado de la entidad de certificación (CA) para habilitar el tráfico HTTPS desde clientes S3 a la SVM habilitada para S3. Se pueden utilizar certificados DE CA de tres orígenes:

- Un nuevo certificado autofirmado de ONTAP en la SVM.
- Un certificado autofirmado existente de ONTAP en la SVM.
- Un certificado de terceros.

Puede usar las mismas LIF de datos para el bloque de S3/NAS que utilizará para servir datos NAS. Si se requieren direcciones IP específicas, consulte "Cree LIF de datos". Es necesario aplicar una política de datos de servicio de S3 para habilitar el tráfico de datos S3 en las LIF; puede modificar la política de servicio existente de la SVM para incluir S3.

Cuando crea el servidor de objetos S3, debe estar preparado para introducir el nombre del servidor S3 como un nombre de dominio completo (FQDN), que los clientes utilizarán para el acceso S3. El FQDN del servidor S3 no debe comenzar por un nombre de bloque.

System Manager

1. Active S3 en una máquina virtual de almacenamiento con protocolos NAS configurados.
   a. Haga clic en **Almacenamiento > Storage VMs**, seleccione una VM de almacenamiento compatible con NAS, haga clic en Configuración y, a continuación, haga clic en ⚙ S3.
   b. Seleccione el tipo de certificado. Tanto si selecciona un certificado generado por el sistema como uno propio, será necesario para el acceso de los clientes.
   c. Introduzca las interfaces de red.
2. Si seleccionó el certificado generado por el sistema, la información del certificado se muestra cuando se confirma la creación de la máquina virtual de almacenamiento nueva. Haga clic en **Descargar** y guárdelo para acceder a los clientes.
   - La clave secreta no se volverá a mostrar.
   - Si necesita de nuevo la información del certificado: Haga clic en **almacenamiento > Storage VMs**, seleccione la VM de almacenamiento y haga clic en **Configuración**.

CLI

1. Compruebe que se permite el protocolo S3 en la SVM:
   `vserver show -fields allowed-protocols`
2. Registre el certificado de clave pública de esta SVM. + Si se necesita un nuevo certificado ONTAP autofirmado, consulte "Cree e instale un certificado de CA en la SVM".
3. Actualizar la política de datos de servicio
   a. Muestre la política de datos de servicio para la SVM
      `network interface service-policy show -vserver svm_name`

      Obtenga más información sobre `network interface service-policy show` en el "Referencia de comandos del ONTAP".

   b. Añada los `data-core` y `data-s3-server services` si no están presentes.
      `network interface service-policy add-service -vserver svm_name -policy policy_name -service data-core,data-s3-server`
4. Compruebe que las LIF de datos de la SVM cumplen sus requisitos:
   `network interface show -vserver svm_name`

   Obtenga más información sobre `network interface show` en el "Referencia de comandos del ONTAP".

5. Cree el servidor S3:
   `vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]`

Puede especificar opciones adicionales al crear el servidor S3 o en cualquier momento posterior.

- De forma predeterminada, HTTPS está habilitado en el puerto 443. Puede cambiar el número de puerto con la opción -secure-listener-Port. + cuando HTTPS está activado, se necesitan certificados de CA para una integración correcta con SSL/TLS. A partir de ONTAP 9.15.1, se admite TLS 1,3 con almacenamiento de objetos S3.
- HTTP está desactivado de forma predeterminada; cuando está habilitado, el servidor escucha en el

puerto 80. Puede activarlo con la opción -is-http-enabled o cambiar el número de puerto con la opción -listener-Port. + cuando HTTP está activado, todas las solicitudes y respuestas se envían a través de la red en texto no cifrado.

1. Compruebe que S3 está configurado como desee:
   `vserver object-store-server show`

Ejemplo + El siguiente comando verifica los valores de configuración de todos los servidores de almacenamiento de objetos:

```
cluster1::> vserver object-store-server show

Vserver: vs1

                     Object Store Server Name: s3.example.com
                         Administrative State: up
                       Listener Port For HTTP: 80
                 Secure Listener Port For HTTPS: 443
                                   HTTP Enabled: false
                                  HTTPS Enabled: true
             Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

Información relacionada

- "servicio adicional de política de servicio de interfaz de red"

Crear un depósito NAS de ONTAP S3

Un bucket NAS de S3 es una asignación entre el nombre de un bucket de S3 y una ruta NAS. Los buckets NAS de S3 permiten proporcionar acceso S3 a cualquier parte de un espacio de nombres SVM que tenga volúmenes y una estructura de directorios existentes.

Antes de empezar

- Un servidor de objetos S3 está configurado en una SVM que contiene datos NAS.
- Los datos del NAS se ajustan a la "Requisitos para el acceso de clientes S3".

Acerca de esta tarea

Puede configurar cubos NAS de S3 para especificar cualquier conjunto de archivos y directorios dentro del directorio raíz de la SVM.

También puede establecer políticas de bloques que permitan o inpermitan el acceso a datos NAS en función de cualquier combinación de estos parámetros:

- Archivos y directorios
- Permisos de usuario y grupo
- S3 operaciones

Por ejemplo, podrías querer configurar una política de bucket que otorgue acceso de solo lectura a los datos a

un gran grupo de usuarios y otra política de bucket que permita a un grupo limitado realizar operaciones en un subconjunto de esos datos.

A partir de ONTAP 9.18.1, puedes crear buckets NAS que permiten que las aplicaciones accedan a los datos en los volúmenes de FlexCache usando el protocolo S3. Todos los nodos del clúster deben estar ejecutando ONTAP 9.18.1 o una versión posterior. Antes de que puedas acceder a un volumen de FlexCache usando el protocolo S3, debes configurar la opción `-is-s3-enabled` en `true` "en el FlexCache volumen". El parámetro está configurado en `false` por defecto.

A partir de ONTAP 9.17.1, puede vincular directamente un bucket NAS de S3 a un volumen en lugar de a la ruta de unión. De forma predeterminada, un bucket S3 en un volumen NAS se asocia a una ruta de unión, que un administrador de ONTAP puede modificar en cualquier momento. Estos cambios pueden interrumpir las operaciones del bucket S3. A partir de ONTAP 9.17.1, puede usar `-is-nas-path-mutable false` opción con el `vserver object-store-server bucket create` Comando en la CLI de ONTAP para habilitar la vinculación del depósito NAS de S3 a un volumen. De forma predeterminada, `-is-nas-path-mutable` está configurado para `true` .

Dado que los "buckets" de S3 NAS son asignaciones y no buckets de S3, las siguientes propiedades de los buckets de S3 estándar no se aplican a los buckets de S3 NAS.

- **Aggr-list \ aggr-list-multiplicador \ Storage-service-level \ volume \ size \ exclude-aggr-list \ qos-policy-group** + no se crean volúmenes ni qtree al configurar cubos NAS S3.
- **role \ is -protected \ is -protected-on-ontap \ is -protected-on-cloud** + Los buckets NAS de S3 no están protegidos ni reflejados mediante SnapMirror S3, sino que utilizan la protección SnapMirror normal disponible en granularidad de volumen.
- **Versioning-state** + los volúmenes NAS suelen tener tecnología de instantáneas disponible para guardar diferentes versiones. Sin embargo, el control de versiones no está disponible actualmente en bloques NAS de S3.
- **Las estadísticas lógicas usadas \ object-count** + equivalentes están disponibles para los volúmenes NAS a través de los comandos de volumen.
- **objetos multiparte** + A partir de ONTAP 9.16.1, los objetos multiparte se admiten en los depósitos NAS de S3 cuando "equilibrado de capacidad avanzado" Está habilitado en el volumen FlexGroup subyacente. El balanceo de capacidad avanzado solo se puede habilitar en volúmenes FlexGroup . No se puede habilitar en volúmenes FlexVol .

Pasos

Puede utilizar el Administrador del sistema o la CLI de ONTAP para crear un depósito NAS.

System Manager

Agrega un nuevo bucket S3 NAS en una máquina virtual de almacenamiento habilitada para NAS.

1. Haga clic en **almacenamiento > Cuchos** y, a continuación, haga clic en **Agregar**.
2. Introduzca un nombre para el bloque NAS de S3 y seleccione la máquina virtual de almacenamiento, no introduzca un tamaño y, a continuación, haga clic en **más opciones**.
3. Introduzca un nombre de ruta válido o haga clic en examinar para seleccionar de una lista de nombres de ruta válidos. + cuando se introduce un nombre de ruta válido, las opciones que no son relevantes para la configuración de NAS S3 están ocultas.
4. Si ya ha asignado usuarios S3 a usuarios NAS y ha creado grupos, puede configurar sus permisos y, a continuación, hacer clic en **Guardar**. + antes de configurar permisos en este paso, debe haber asignado usuarios de S3 a usuarios NAS.

De lo contrario, haga clic en **Guardar** para completar la configuración de bloque NAS S3.

CLI

1. Cree un depósito NAS S3 en una SVM que contenga sistemas de archivos NAS.
   ```
   vserver object-store-server bucket create -vserver <svm_name> -bucket
   <bucket_name> -type nas -nas-path <junction_path> -is-nas-path-mutable
   true|false [-comment <text>]
   ```

   Ejemplo 1: Crear un depósito NAS S3

   ```
   cluster1::> vserver object-store-server bucket create -bucket testbucket
   -type nas -path /vol1
   ```

   Ejemplo 2: Crear un depósito NAS S3 y vincularlo a un volumen

   ```
   vserver object-store-server bucket create -vserver vs1 -bucket nasbucket1
   -type nas -nas-path /pathA/dir1 -is-nas-path-mutable false
   ```

Habilitar usuarios del cliente ONTAP S3

Para permitir que los usuarios del cliente S3 accedan a los datos NAS, debe asignar los nombres de usuario de S3 a los usuarios NAS correspondientes y luego otorgarles permiso para acceder a los datos NAS mediante políticas de servicio de bucket.

Antes de empezar

Los nombres de usuario para el acceso del cliente (usuarios de cliente LINUX/UNIX, Windows y S3) ya deben existir.

Debe tener en cuenta que algunas funciones S3 son "No compatible con buckets NAS de S3".

Acerca de esta tarea

La asignación de un nombre de usuario de S3 a un usuario de LINUX/UNIX o Windows correspondiente permite que las comprobaciones de autorización de los archivos NAS se honren cuando los clientes de S3 accedan a ellos. Las asignaciones de S3 a NAS se especifican proporcionando un nombre de usuario de S3 *Pattern*, que puede expresarse como un único nombre o una expresión regular POSIX, y un nombre de usuario de LINUX/UNIX o Windows *Replacement*.

En caso de que no exista ninguna asignación de nombres, se utilizará la asignación de nombres predeterminada, donde se utilizará el propio nombre de usuario de S3 como nombre de usuario UNIX y nombre de usuario de Windows. Puede modificar las asignaciones de nombre de usuario predeterminado de UNIX y Windows con el `vserver object-store-server modify` comando.

Solo se admite la configuración de asignación de nombres local; no se admite LDAP.

Después de asignar usuarios de S3 a usuarios NAS, puede conceder permisos a los usuarios especificando los recursos (directorios y archivos) a los que tienen acceso y las acciones a las que se les permiten o no ejecutar allí.

System Manager

1. Cree asignaciones de nombres locales para clientes UNIX o Windows (o ambos).
   a. Haga clic en **almacenamiento > Cuchos** y seleccione la VM de almacenamiento habilitada para S3/NAS.
   b. Seleccione **Configuración**, luego haga clic en → **Asignación de nombres** (en **Usuarios y grupos de host**).
   c. En los mosaicos de **S3 a Windows** o **S3 a UNIX** (o ambos), haga clic en **Agregar** y, a continuación, introduzca los nombres de usuario de **patrón** (S3) y **reemplazo** (NAS) que desee.
2. Cree una política de bloques para proporcionar acceso de cliente.
   a. Haga clic en **Almacenamiento > Buckets**, haga clic en ⋮ junto al cubo S3 deseado y luego haga clic en **Editar**.
   b. Haga clic en **Agregar** y proporcione los valores deseados.
      - **Principal**: Proporcione nombres de usuario S3 o utilice los valores predeterminados (todos los usuarios).
      - **Efecto**: Seleccione **permitir** o **Denegar**.
      - **Acciones**: Introduzca acciones para estos usuarios y recursos. El conjunto de operaciones de recursos que el servidor de almacén de objetos admite actualmente para los cubos NAS de S3 es: GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, GetObjectTagging, PutObjectTagging, DeleteObjectTagging, GetBucketLocation, GetBucketVersioning, PutBucketVersioning y ListBucketVersions. Se aceptan caracteres comodín para este parámetro.
      - **Recursos**: Introduzca las rutas de acceso a carpetas o archivos en las que se permiten o deniegan las acciones, o utilice los valores predeterminados (directorio raíz del bloque).

CLI

1. Cree asignaciones de nombres locales para clientes UNIX o Windows (o ambos).
   `vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix} -position` *`integer`* `-pattern` *`s3_user_name`* `-replacement` *`nas_user_name`*
   - `-position` - número de prioridad para la evaluación de mapas; introduzca 1 o 2.
   - `-pattern` - Un nombre de usuario S3 o una expresión regular
   - `-replacement` - un nombre de usuario de windows o unix

Ejemplos

```
vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1
-replacement win_user_1
vserver name-mapping create -direction s3-unix -position 2 -pattern s3_user_1
-replacement unix_user_1
```

1. Cree una política de bloques para proporcionar acceso de cliente.
   `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {deny|allow} -action list_of_actions -principal list_of_users_or_groups -resource [-sid alphanumeric_text]`
   - `-effect {deny|allow}` - especifica si el acceso es permitido o denegado cuando un usuario solicita una acción.

- `-action <Action>, …` - especifica las operaciones de recursos que se permiten o se deniegan. El conjunto de operaciones de recursos que el servidor de almacén de objetos soporta actualmente para los buckets S3 NAS son: GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl y GetBucketLocation. Se aceptan caracteres comodín para este parámetro.
- `-principal <Objectstore Principal>, …` - valida al usuario que solicita el acceso contra los usuarios o grupos del servidor del almacén de objetos especificados en este parámetro.
  - Un grupo de servidores de almacenes de objetos se especifica agregando un grupo de prefijos/ al nombre del grupo.
  - `-principal` - (el carácter de guion) otorga acceso a todos los usuarios.
- `-resource <text>, …` - especifica el cubo, carpeta, u objeto para el que se establecen permisos de permitir/denegar. Se aceptan caracteres comodín para este parámetro.
- `[-sid <SID>]` - especifica un comentario de texto opcional para la declaración de política de cubo del servidor de almacén de objetos.

Ejemplos

```
cluster1::> vserver object-store-server bucket policy add-statement -bucket
testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* sid "FullAccessForUser1"

cluster1::> vserver object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```

Configuración de SMB para Microsoft Hyper-V y SQL Server

Información general de la configuración de SMB para Microsoft Hyper-V y SQL Server

Las funciones de ONTAP le permiten habilitar las operaciones no disruptivas para dos aplicaciones de Microsoft a través del protocolo SMB: Microsoft Hyper-V y Microsoft SQL Server.

Debe utilizar estos procedimientos si desea implementar operaciones no disruptivas de SMB en las siguientes circunstancias:

- Se configuró el acceso básico a archivos del protocolo SMB.
- Quiere habilitar los recursos compartidos de archivos de SMB 3.0 o posteriores que residen en SVM para almacenar los siguientes objetos:
  - Archivos de equipos virtuales Hyper-V.
  - Bases de datos del sistema SQL Server

Información relacionada

Para obtener información adicional sobre la tecnología ONTAP y la interacción con servicios externos, consulta estos Technical Reports (TRs): ** "Informe técnico de NetApp 4172: Prácticas recomendadas de

Microsoft Hyper-V mediante SMB 3.0 con ONTAP"

Configurar ONTAP para soluciones Microsoft Hyper-V y SQL Server sobre SMB

Puede utilizar los recursos compartidos de archivos de SMB 3.0 y versiones posteriores disponibles de forma continua para almacenar archivos de máquinas virtuales de Hyper-V o bases de datos de sistemas de SQL Server y bases de datos de usuario en volúmenes que residen en SVM, al tiempo que ofrece operaciones no disruptivas (NDO) tanto para eventos planificados como no planificados.

Microsoft Hyper-V mediante SMB

Para crear una solución Hyper-V mediante SMB, primero debe configurar ONTAP para proporcionar servicios de almacenamiento para servidores de Microsoft Hyper-V. Además, también debe configurar clústeres de Microsoft (si se utiliza una configuración en clúster), servidores Hyper-V, conexiones SMB 3.0 disponibles de forma continua a los recursos compartidos alojados en el servidor CIFS y, opcionalmente, servicios de backup para proteger los archivos de máquina virtual almacenados en volúmenes de SVM.

Los servidores de Hyper-V deben estar configurados en Windows 2012 Server o una versión posterior. Se admiten tanto configuraciones independientes como de servidores de Hyper-V en cluster.

- Para obtener información sobre cómo crear clústeres de Microsoft y servidores Hyper-V, consulte el sitio web de Microsoft.
- SnapManager para Hyper-V es una aplicación basada en host que facilita servicios de backup rápidos basados en snapshots, diseñados para integrarse con configuraciones de Hyper-V mediante SMB.

  Para información sobre cómo usar SnapManager con configuraciones de Hyper-V sobre SMB, consulta la "Documentación de SnapManager for Hyper-V".

Microsoft SQL Server sobre SMB

Para crear una solución SQL Server con SMB, primero debe configurar ONTAP para proporcionar servicios de almacenamiento para la aplicación Microsoft SQL Server. Además, también debe configurar clústeres de Microsoft (si se utiliza una configuración en clúster). A continuación, debe instalar y configurar SQL Server en los servidores Windows y crear conexiones SMB 3.0 disponibles de forma continua con los recursos compartidos alojados en el servidor CIFS. De manera opcional, es posible configurar los servicios de backup para proteger los archivos de base de datos que están almacenados en volúmenes de SVM.

SQL Server debe estar instalado y configurado en Windows 2012 Server o posterior. Se admiten tanto configuraciones independientes como en cluster.

- Para obtener información acerca de cómo crear clústeres de Microsoft e instalar y configurar SQL Server, consulte el sitio Web de Microsoft.
- El plugin de SnapCenter para Microsoft SQL Server es una aplicación basada en host que facilita los servicios de backup rápidos basados en snapshots, diseñados para integrarse con configuraciones de SQL Server sobre SMB.

  Para obtener información sobre el uso del plugin de SnapCenter para Microsoft SQL Server, consulte "Plugin de SnapCenter para Microsoft SQL Server" el documento.

Operaciones no disruptivas para Hyper-V y SQL Server sobre SMB

¿Qué significan las operaciones no disruptivas para Hyper-V y SQL Server sobre SMB

Las operaciones no disruptivas para Hyper-V y SQL Server en SMB se refieren a la combinación de funcionalidades que permiten que los servidores de aplicaciones y las máquinas virtuales o bases de datos contenidos permanezcan en línea y proporcionen una disponibilidad continua durante muchas tareas administrativas. Esto incluye tanto los tiempos de inactividad previstos como imprevistos de la infraestructura de almacenamiento.

Las operaciones no disruptivas compatibles con servidores de aplicaciones en SMB incluyen lo siguiente:

- Toma de control y retorno al nodo primario planificados
- Respaldo no planificado
- Renovar
- Reubicación planificada de agregados (ARL)
- Migración LIF y recuperación tras fallos
- Movimiento de volumen planificado

Protocolos que permiten las operaciones no disruptivas en SMB

Junto con el lanzamiento de SMB 3.0, Microsoft ha lanzado nuevos protocolos para proporcionar las funcionalidades necesarias para admitir operaciones no disruptivas para Hyper-V y SQL Server sobre SMB.

ONTAP usa estos protocolos cuando proporciona operaciones no disruptivas a los servidores de aplicaciones a través de SMB:

- SMB 3,0
- Testigo

Conceptos clave sobre las operaciones no disruptivas de Hyper-V y SQL Server sobre SMB

Hay ciertos conceptos sobre las operaciones no disruptivas (NDO) que debe comprender antes de configurar la solución Hyper-V o SQL Server sobre SMB.

- **Cuota continuamente disponible**

  Un recurso compartido SMB 3.0 que tiene establecida la propiedad de recurso compartido disponible de forma continua. Los clientes que se conectan mediante recursos compartidos constantemente disponibles pueden sobrevivir a eventos disruptivos como la toma de control, la devolución y la reubicación de agregados.

- **Nodo**

  Una única controladora que forma parte de un clúster. Para distinguir entre los dos nodos de un par SFO, un nodo se denomina a veces el *local node* y el otro nodo se denomina a veces el *Partner node* o *remote node*. El propietario principal del almacenamiento es el nodo local. El propietario secundario, que toma el

control del almacenamiento cuando falla el propietario principal, es el nodo del partner. Cada nodo es el propietario principal de su almacenamiento y el propietario secundario para el almacenamiento de su partner.

- **Reubicación no disruptiva de agregados**

  La capacidad de mover un agregado entre nodos de partner dentro de un par SFO en un clúster sin interrumpir las aplicaciones del cliente.

- **Recuperación tras fallos no disruptiva**

  Consulte *takeover*.

- **Migración LIF no disruptiva**

  La capacidad de realizar una migración LIF sin interrumpir las aplicaciones cliente que están conectadas al clúster a través de esa LIF. En el caso de las conexiones SMB, esto solo es posible para clientes que se conectan mediante SMB 2.0 o una versión posterior.

- **Operaciones no disruptivas**

  La capacidad de realizar importantes operaciones de gestión y actualización de ONTAP, así como de resistir fallos de nodos sin interrumpir las aplicaciones cliente. Este término hace referencia a la colección de funciones de toma de control no disruptivas, actualización no disruptiva y migración en conjunto.

- **Actualización no disruptiva**

  Posibilidad de actualizar el hardware o el software de los nodos sin interrumpir las aplicaciones.

- **Movimiento de volumen no disruptivo**

  La capacidad de mover un volumen libremente por el clúster sin interrumpir las aplicaciones que estén utilizando el volumen. En el caso de las conexiones SMB, todas las versiones de SMB admiten movimientos de volúmenes no disruptivos.

- **Asas persistentes**

  Propiedad de SMB 3.0 que permite la conexión disponible de forma continua para volver a conectarse con total transparencia al servidor CIFS en caso de desconexión. Al igual que sucede con las asas duraderas, el servidor CIFS mantiene las asas persistentes durante un período de tiempo tras la pérdida de la comunicación con el cliente conectado. Sin embargo, las asas persistentes tienen más resiliencia que las asas duraderas. Además de dar al cliente la posibilidad de recuperar el controlador en una ventana de 60 segundos después de volver a conectarse, el servidor CIFS niega el acceso a los demás clientes que soliciten acceso al archivo durante esa ventana de 60 segundos.

  La información sobre las asas persistentes se refleja en el almacenamiento persistente del partner SFO, el cual permite a los clientes con asas persistentes desconectadas recuperar las asas duraderas tras un evento en el que el partner de SFO asume la propiedad del almacenamiento del nodo. Además de proporcionar operaciones no disruptivas en caso de movimiento de LIF (que gestiona mantenimiento duradero), las direcciones persistentes proporcionan operaciones no disruptivas para la toma de control, la devolución y la reubicación de agregados.

- **Retorno SFO**

  Devolver agregados a sus ubicaciones principales al recuperarse de un evento de toma de control.

- **Par SFO**

  Un par de nodos cuyas controladoras están configuradas para suministrar datos entre sí si uno de los dos nodos deja de funcionar. Según el modelo del sistema, ambas controladoras pueden estar en un solo chasis o las controladoras pueden estar en chasis separados. Conocido como par de alta disponibilidad en un clúster de dos nodos.

- **Adquisición**

  Proceso por el que el partner toma el control del almacenamiento cuando falla el propietario principal de ese almacenamiento. En el contexto de la OFS, la conmutación por error y la toma de control son sinónimos.

Cómo la funcionalidad SMB 3.0 admite operaciones no disruptivas en recursos compartidos de SMB

SMB 3.0 proporciona una funcionalidad crucial que permite admitir operaciones no disruptivas para Hyper-V y SQL Server en recursos compartidos SMB. Esto incluye la `continuously-available` propiedad de recurso compartido y un tipo de manejador de archivos conocido como *persistent handle* que permite a los clientes SMB recuperar el estado de apertura de archivos y restablecer las conexiones SMB de forma transparente.

Los identificadores persistentes se pueden otorgar a clientes compatibles con SMB 3.0 que se conectan a un recurso compartido con el conjunto de propiedades compartidas disponibles continuamente. Si la sesión SMB está desconectada, el servidor CIFS conserva información sobre el estado de gestión persistente. El servidor CIFS bloquea las solicitudes de otros clientes durante el periodo de 60 segundos en el que se permite al cliente reconectar, permitiendo al cliente con la gestión persistente recuperar el controlador tras una desconexión de red. Los clientes con controladores persistentes pueden volver a conectarse utilizando uno de los LIF de datos de la máquina virtual de almacenamiento (SVM), ya sea reconectando a través del mismo LIF o a través de un LIF diferente.

La reubicación, la toma de control y el retorno al nodo primario de los agregados se producen entre los pares de SFO. Para gestionar sin problemas la desconexión y reconexión de sesiones con archivos que tienen controladores persistentes, el nodo del partner mantiene una copia de toda la información del bloqueo del controlador persistente. Tanto si el evento está planificado como no planificado, el partner de SFO puede gestionar de forma no disruptiva el reconecta del controlador persistente. Con esta nueva funcionalidad, las conexiones SMB 3.0 al servidor CIFS pueden conmutar por error de forma transparente y sin interrupciones a otra LIF de datos asignada a la SVM en lo que tradicionalmente ha sido un evento disruptivo.

Aunque el uso de identificadores persistentes permite al servidor CIFS conmutar al respaldo de forma transparente en las conexiones de SMB 3.0, si un fallo provoca que la aplicación de Hyper-V conmute a otro nodo del clúster de Windows Server, el cliente no tiene forma de recuperar los controladores de archivos de estos controladores desconectados. En esta situación, los controladores de archivos en estado desconectado pueden bloquear potencialmente el acceso de la aplicación Hyper-V si se reinicia en un nodo diferente. "'clúster de conmutación por error'" es una parte de SMB 3.0 que aborda este escenario proporcionando un mecanismo para invalidar controladores obsoletos y en conflicto. Con este mecanismo, un clúster de Hyper-V se puede recuperar rápidamente cuando fallan los nodos del clúster de Hyper-V.

Lo que hace el protocolo de testigos para mejorar una conmutación por error transparente

El protocolo Witness proporciona funcionalidades mejoradas de recuperación tras fallos de clientes para recursos compartidos de SMB 3.0 continuamente disponibles (recursos

compartidos de CA). Witness facilita una conmutación al nodo de respaldo más rápida porque evita el período de recuperación tras fallos de LIF. Notifica a los servidores de aplicaciones cuando un nodo no está disponible sin tener que esperar a que se agote el tiempo de espera de la conexión SMB 3.0.

La conmutación por error es fluida, con aplicaciones que se ejecutan en el cliente no siendo consciente de que se ha producido una conmutación por error. Si no se dispone de un testigo, las operaciones de conmutación por error siguen teniendo éxito, pero la conmutación por error sin un testigo es menos eficiente.

Es posible realizar una conmutación por error mejorada con los siguientes requisitos:

- Solo se puede utilizar con servidores CIFS compatibles con SMB 3.0 que tengan habilitada SMB 3.0.
- Los recursos compartidos deben utilizar SMB 3.0 con la propiedad compartida de disponibilidad continua establecida.
- El partner SFO del nodo al que están conectados los servidores de aplicaciones debe tener al menos una LIF de datos operativos asignada a la máquina virtual de almacenamiento (SVM) que aloja datos de los servidores de aplicaciones.

> ⓘ El protocolo de testigos funciona entre pares de SFO. Dado que las LIF pueden migrar a cualquier nodo del clúster, es posible que cualquier nodo deba ser el testigo de su partner SFO. El protocolo de observación no puede proporcionar una rápida conmutación por error de las conexiones SMB en un nodo determinado si la SVM que aloja datos de los servidores de aplicaciones no tiene una LIF de datos activa en el nodo del partner. Por lo tanto, cada nodo del clúster debe tener al menos una LIF de datos para cada SVM que aloje una de estas configuraciones.

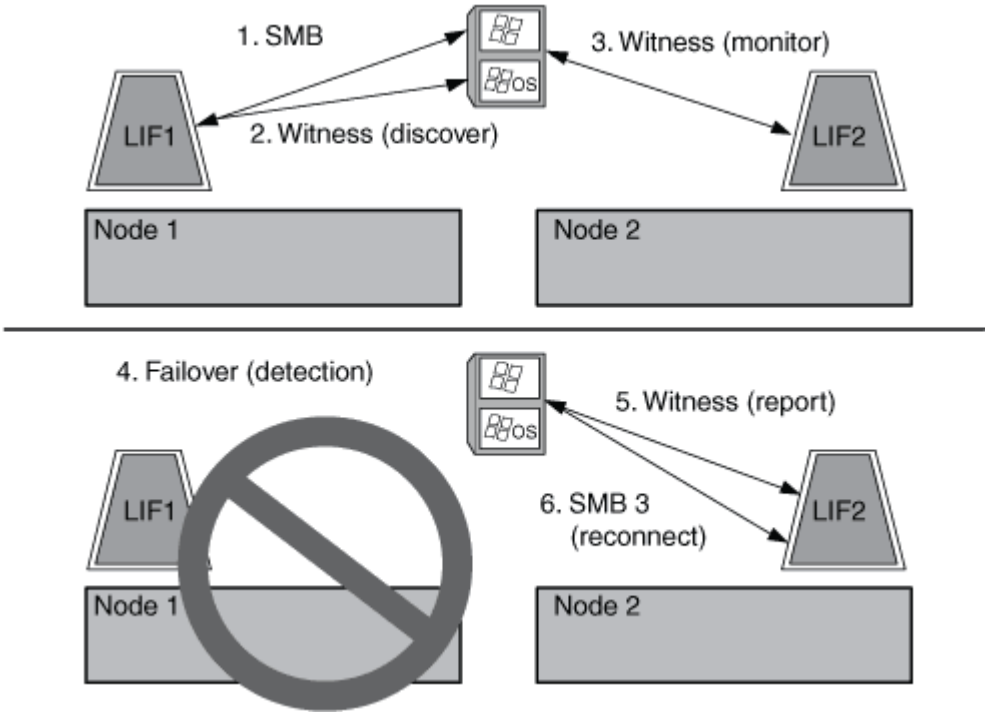
- Los servidores de aplicación deben conectarse al servidor CIFS mediante el nombre del servidor CIFS que se almacena en DNS en lugar de utilizar direcciones IP de LIF individuales.

Cómo funciona el protocolo de testigos

ONTAP implementa el protocolo Witness mediante el uso del partner SFO de un nodo como testigo. En caso de fallo, el partner detecta rápidamente el fallo y notifica al cliente SMB.

El protocolo Witness proporciona una recuperación tras fallos mejorada mediante el siguiente proceso:

1. Cuando el servidor de aplicaciones establece una conexión SMB de disponibilidad continua a Node1, el servidor CIFS informa al servidor de aplicaciones que el testigo está disponible.
2. El servidor de aplicaciones solicita las direcciones IP del servidor testigo de Node1 y recibe una lista de direcciones IP de LIF de datos Node2 (el partner SFO) asignadas a la máquina virtual de almacenamiento (SVM).
3. El servidor de aplicaciones elige una de las direcciones IP, crea una conexión de testigo a Node2 y se registra para recibir una notificación si la conexión disponible continuamente en Node1 se debe mover.
4. Si se produce un evento de conmutación por error en Node1, el testigo facilita los eventos de conmutación por error, pero no se ve involucrado en la devolución.
5. Witness detecta el evento de conmutación por error y notifica al servidor de aplicaciones a través de la conexión de testigos que la conexión SMB debe moverse a Node2.
6. El servidor de aplicaciones mueve la sesión SMB a Node2 y recupera la conexión sin interrupción del acceso del cliente.



Backups basados en recursos compartidos con VSS remoto

Información general sobre backups basados en recursos compartidos con VSS remoto

Puede utilizar VSS remoto para realizar backups basados en recursos compartidos de los archivos de máquinas virtuales Hyper-V almacenados en un servidor CIFS.

Microsoft Remote VSS (Volume Shadow Copy Services) es una extensión de la infraestructura de Microsoft VSS existente. Con VSS remoto, Microsoft ha ampliado la infraestructura VSS para dar soporte a las copias en la sombra de los recursos compartidos de SMB. Además, las aplicaciones de servidor como Hyper-V pueden almacenar archivos VHD en recursos compartidos de archivos SMB. Con estas extensiones, es posible tomar copias redundantes coherentes con las aplicaciones para máquinas virtuales que almacenan datos y archivos de configuración en recursos compartidos.

Conceptos de VSS remoto

Debe conocer ciertos conceptos que se requieren para comprender cómo los servicios de backup utilizan VSS remoto (Volume Shadow Copy Service, Servicio de instantáneas de volumen) con las configuraciones de Hyper-V en SMB.

- **VSS (Volume Shadow Copy Service, Servicio de instantáneas de volumen)**

  Tecnología de Microsoft que se usa para realizar copias de backup o copias Snapshot de datos en un volumen específico en un momento específico. VSS se coordina entre servidores de datos, aplicaciones de backup y software de gestión del almacenamiento para dar soporte a la creación y gestión de backups coherentes.

- **VSS remoto (Servicio de instantáneas de volumen remoto)**

  Tecnología de Microsoft que se utiliza para realizar copias de backup basadas en recursos compartidos de datos que están en un estado consistente con los datos en un momento específico en el que se accede a

los datos a través de recursos compartidos SMB 3.0. También se conoce como *Volume Shadow Copy Service*.

- **Copia de sombra**

  Un conjunto de datos duplicado que contiene el recurso compartido en un instante bien definido. Las copias de sombra se utilizan para crear backups coherentes de un momento específico de los datos, lo que permite al sistema o aplicaciones seguir actualizando los datos en los volúmenes originales.

- **Sistema de instantáneas**

  Colección de una o más instantáneas, con cada copia de sombra correspondiente a un recurso compartido. Las instantáneas de un conjunto de instantáneas representan todos los recursos compartidos de los que se debe realizar una copia de seguridad en la misma operación. El cliente VSS de la aplicación habilitada para VSS identifica las instantáneas que se incluirán en el conjunto.

- **Recuperación automática de conjuntos de instantáneas**

  La parte del proceso de backup de las aplicaciones de backup habilitadas para VSS remotas en las que el directorio de réplica que contiene las instantáneas es coherente en un momento específico. Al inicio del backup, el cliente VSS de la aplicación activa la aplicación para llevar a cabo puntos de control de software en los datos programados para la copia de seguridad (los ficheros de la máquina virtual en el caso de Hyper-V). A continuación, el cliente VSS permite que las aplicaciones continúen. Una vez creado el conjunto de instantáneas, VSS remoto hace que el conjunto de instantáneas sea modificable y expone la copia modificable a las aplicaciones. La aplicación prepara el conjunto de instantáneas para la copia de seguridad realizando una recuperación automática con el punto de control del software tomado anteriormente. La recuperación automática hace que las instantáneas se encuentren en un estado coherente, desenrolando los cambios realizados en los archivos y directorios desde que se creó el punto de comprobación. La recuperación automática es un paso opcional para los backups con VSS habilitado.

- **Id. De copia de sombra**

  GUID que identifica de forma exclusiva una copia oculta.

- **Id. De conjunto de copia de sombra**

  GUID que identifica de forma exclusiva una colección de Id. De copia oculta en el mismo servidor.

- **SnapManager para Hyper-V**

  El software que automatiza y simplifica las operaciones de backup y restauración para Microsoft Windows Server 2012 Hyper-V. SnapManager para Hyper-V usa VSS remoto con recuperación automática para realizar backups de archivos Hyper-V mediante recursos compartidos SMB.

Información relacionada

Conceptos clave sobre las operaciones no disruptivas de Hyper-V y SQL Server sobre SMB

Backups basados en recursos compartidos con VSS remoto

Ejemplo de estructura de directorio utilizada por VSS remoto

VSS remoto atraviesa la estructura de directorios que almacena archivos de máquina virtual Hyper-V a medida que crea instantáneas. Es importante entender qué es una estructura de directorio adecuada, para que pueda crear copias de seguridad de archivos

de equipos virtuales con éxito.

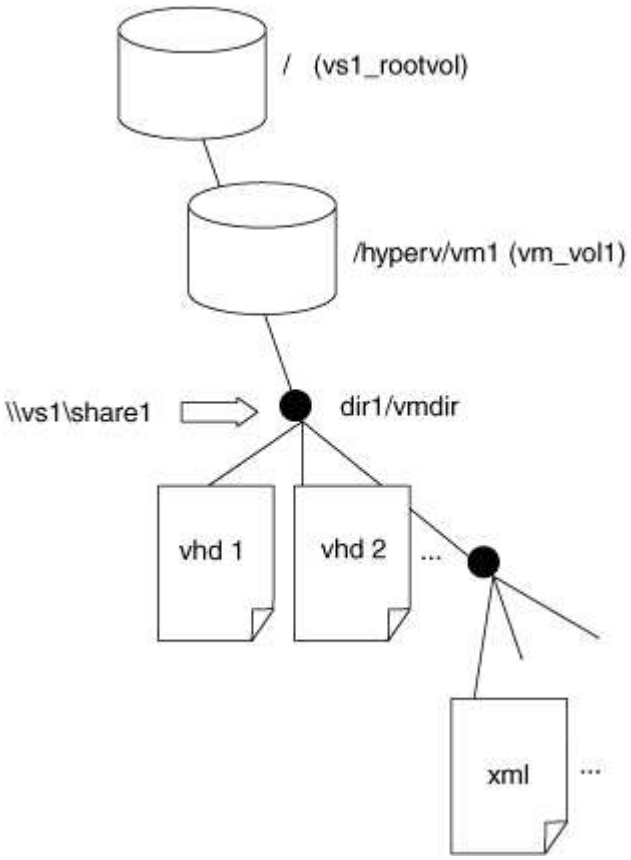
Una estructura de directorio compatible para la creación correcta de instantáneas cumple los siguientes requisitos:

- Sólo los directorios y los archivos normales están presentes en la estructura de directorios que se utiliza para almacenar archivos de máquinas virtuales.

  La estructura de directorios no contiene uniones, vínculos ni archivos no regulares.

- Todos los archivos de una máquina virtual residen dentro de un único recurso compartido.
- La estructura de directorio que se utiliza para almacenar archivos de equipos virtuales no excede la profundidad configurada del directorio de instantáneas.
- El directorio raíz del recurso compartido sólo contiene directorios o archivos de la máquina virtual.

En la siguiente ilustración, el volumen llamado vm_vol1 se crea con un punto de unión en `/hyperv/vm1` la máquina virtual de almacenamiento (SVM) VS1. Se crean subdirectorios para contener los archivos de la máquina virtual en el punto de unión. Se accede a los archivos de los equipos virtuales del servidor de Hyper-V a través de share1 que tiene la ruta `/hyperv/vm1/dir1/vmdir`. El servicio de instantáneas crea instantáneas de todos los archivos de la máquina virtual contenidos en la estructura de directorios bajo share1 (hasta la profundidad configurada del directorio de instantáneas).



Cómo gestiona SnapManager para Hyper-V los backups basados en VSS remotos para Hyper-V en SMB

Puede utilizar SnapManager para Hyper-V para gestionar los servicios de backup basados en VSS remoto. El servicio de backup gestionado de SnapManager para Hyper-

V ofrece ventajas con el fin de crear conjuntos de backup que utilizan el espacio de forma eficiente.

Entre las optimizaciones de SnapManager para backups gestionados por Hyper-V se incluyen las siguientes:

- SnapManager para Hyper-V especifica la lista de archivos de máquinas virtuales de los recursos compartidos de SMB que el servicio de copia en sombra necesita copiar.

  Al proporcionar una lista de destino de archivos de máquinas virtuales, el servicio de instantáneas no necesita crear instantáneas de todos los archivos del recurso compartido.

- La máquina virtual de almacenamiento (SVM) conserva las instantáneas para que SnapManager Hyper-V las utilice en las restauraciones.

  No hay ninguna fase de backup. El backup es la snapshot con gestión eficiente del espacio.

SnapManager para Hyper-V proporciona funcionalidades de backup y restauración para HyperV mediante SMB mediante el siguiente proceso:

1. Preparación para la operación de copia oculta

   El cliente VSS de la aplicación SnapManager para Hyper-V configura el conjunto de copias redundantes. El cliente VSS recopila información sobre los recursos compartidos que se incluirán en el conjunto de copias redundantes y proporciona esta información a ONTAP. Un conjunto puede contener una o más instantáneas y una copia de sombra corresponde a un recurso compartido.

2. Creación del conjunto de instantáneas (si se utiliza la recuperación automática)

   Por cada recurso compartido incluido en el conjunto de instantáneas, ONTAP crea una copia de sombra y hace que la copia de sombra sea editable.

3. Exponiendo el conjunto de instantáneas

   Una vez que ONTAP crea las copias instantáneas, éstas se exponen a SnapManager para Hyper-V para que los escritores de VSS de la aplicación puedan realizar una recuperación automática.

4. Recuperación automática del conjunto de instantáneas

   Durante la creación de conjuntos de instantáneas, hay un período de tiempo en el que se producen cambios activos en los archivos incluidos en el conjunto de copias de seguridad. Los escritores de VSS de la aplicación deben actualizar las instantáneas para asegurarse de que están en un estado completamente coherente antes de realizar la copia de seguridad.

   > La forma en que se realiza la recuperación automática es específica para cada aplicación. La fase de VSS remota no participa en esta.

5. Completar y limpiar el conjunto de instantáneas

   El cliente VSS notifica a ONTAP una vez que finaliza la recuperación automática. El conjunto de instantáneas es de sólo lectura y, a continuación, está listo para la copia de seguridad. Cuando se utiliza SnapManager para Hyper-V para la copia de seguridad, los archivos de una copia snapshot se convierten en la copia de seguridad; por lo tanto, para la fase de copia de seguridad, se crea una copia Snapshot para cada volumen que contenga acciones del conjunto de copia de seguridad. Una vez finalizada la copia de seguridad, el conjunto de instantáneas se elimina del servidor CIFS.

Cómo se utiliza la descarga de copias ODX con Hyper-V y SQL Server en recursos compartidos SMB

La transferencia de datos descargados (ODX), también conocida como *copy fload*, permite transferir datos directamente dentro o entre dispositivos de almacenamiento compatibles sin transferir los datos a través del equipo host. La descarga de copias ODX de ONTAP le ofrece ventajas en rendimiento al realizar operaciones de copia en su servidor de aplicaciones a través de la instalación de SMB.

En las transferencias de archivos que no son ODX, los datos se leen del servidor CIFS de origen y se transfieren a través de la red al equipo cliente. El equipo cliente transfiere los datos a través de la red al servidor CIFS de destino. En resumen, el equipo cliente lee los datos del origen y los escribe en el destino. Con las transferencias de archivos ODX, los datos se copian directamente del origen al destino.

Dado que las copias descargados de ODX se realizan directamente entre el almacenamiento de origen y destino, se obtienen importantes ventajas en el rendimiento. Las ventajas en cuanto a rendimiento incluyen unos tiempos de copia más rápidos entre el origen y el destino, una menor utilización de recursos (CPU, memoria) en el cliente y una menor utilización de ancho de banda de I/o de la red.

```
 ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0
continuously available connections.
Los siguientes casos de uso admiten el uso de copias y movimientos ODX:
```

- Volumen interno

  Los archivos o LUN de origen y destino están dentro del mismo volumen.

- Entre volúmenes, mismo nodo, misma máquina virtual de almacenamiento (SVM)

  Los archivos de origen y de destino o las LUN se encuentran en distintos volúmenes ubicados en el mismo nodo. Los datos son propiedad de la misma SVM.

- Entre volúmenes, distintos nodos, misma SVM

  Los archivos de origen y de destino o las LUN se encuentran en volúmenes distintos que se encuentran en nodos diferentes. Los datos son propiedad de la misma SVM.

- Entre SVM, mismo nodo

  El archivo de origen y los LUN de destino se encuentran en distintos volúmenes ubicados en el mismo nodo. Los datos son propiedad de diferentes SVM.

- Entre SVM, diferentes nodos

  El archivo o las LUN de origen y destino se encuentran en distintos volúmenes ubicados en nodos diferentes. Los datos son propiedad de diferentes SVM.

Algunos casos de uso específicos para la descarga de copias de ODX con soluciones Hyper-V son los siguientes:

- Se puede utilizar la transferencia de la copia ODX mediante Hyper-V para copiar datos dentro o a través de archivos de disco duro virtual (VHD), o bien copiar datos entre recursos compartidos de SMB

asignados y LUN iSCSI conectados dentro del mismo clúster.

Esto permite que las copias de sistemas operativos invitados pasen al almacenamiento subyacente.

- Al crear discos duros virtuales de tamaño fijo, ODX se utiliza para inicializar el disco con ceros, empleando un token de cero conocido.
- La descarga de copias ODX se utiliza para la migración de almacenamiento de máquinas virtuales si el almacenamiento de origen y destino está en el mismo clúster.

> Para aprovechar los casos de uso de un paso a través de la descarga de copias ODX mediante Hyper-V, el sistema operativo invitado debe ser compatible con ODX, mientras que los discos del sistema operativo invitado deben ser discos SCSI respaldados por almacenamiento (tanto SMB COMO SAN) que sean compatibles con ODX. Los discos IDE del sistema operativo invitado no admiten el paso a través de ODX.

Los casos de uso específicos para la descarga de copias ODX mediante soluciones SQL Server son los siguientes:

- Puede utilizar la descarga de copias de ODX para exportar e importar bases de datos de SQL Server entre recursos compartidos de SMB asignados o entre recursos compartidos de SMB y LUN iSCSI conectados dentro del mismo clúster.
- La descarga de copias ODX se utiliza para exportar e importar bases de datos si el almacenamiento de origen y destino se encuentran en el mismo clúster.

Requisitos y consideraciones de configuración

Requisitos de licencia y ONTAP

Debe estar al tanto de determinados requisitos de ONTAP y licencia cuando cree soluciones de SQL Server o Hyper-V mediante SMB para realizar operaciones no disruptivas en SVM.

Requisitos de versión de ONTAP

- Hyper-V mediante SMB

  ONTAP admite operaciones no disruptivas en recursos compartidos SMB para Hyper-V que se ejecutan en Windows 2012 o posterior.

- SQL Server sobre SMB

  ONTAP admite operaciones no disruptivas en recursos compartidos SMB para SQL Server 2012 o posterior que se ejecutan en Windows 2012 o posterior.

Para obtener la información más reciente sobre las versiones compatibles de ONTAP, Windows Server y SQL Server para realizar operaciones no disruptivas mediante recursos compartidos SMB, consulte la matriz de interoperabilidad.

"Herramienta de matriz de interoperabilidad de NetApp"

Requisitos de licencia

Se requieren las siguientes licencias:

- CIFS
- FlexClone (solo para Hyper-V mediante SMB)

  Esta licencia es necesaria si se usa VSS remoto para los backups. El servicio de copia de respaldo utiliza FlexClone para crear copias de un momento específico de los archivos que se usarán a la hora de crear un backup.

  Una licencia de FlexClone es opcional si se utiliza un método de backup que no utiliza Remote VSS.

La licencia FlexClone se incluye en "ONTAP One". Si no tiene ONTAP One, debe "verifique que las licencias necesarias estén instaladas", y, si es necesario, "instálelos".

Requisitos de LIF de datos y red

Debe estar al tanto de determinados requisitos de la red y de la LIF de datos al crear configuraciones de SQL Server o Hyper-V mediante SMB para lograr operaciones no disruptivas).

Requisitos de protocolos de red

- Las redes IPv4 e IPv6 son compatibles.
- Se requiere SMB 3.0 o una versión posterior.

  SMB 3.0 proporciona la funcionalidad necesaria para crear las conexiones SMB continuamente disponibles para ofrecer operaciones no disruptivas.

- Los servidores DNS deben contener entradas que asignan el nombre del servidor CIFS a las direcciones IP asignadas a las LIF de datos de la máquina virtual de almacenamiento (SVM).

  Los servidores de aplicaciones de Hyper-V o SQL Server suelen realizar varias conexiones a través de varias LIF de datos al acceder a archivos de equipos virtuales o bases de datos. Para obtener una funcionalidad adecuada, los servidores de aplicaciones deben efectuar estas varias conexiones SMB mediante el nombre del servidor CIFS en lugar de realizar varias conexiones a varias direcciones IP únicas.

  Para ello, también es necesario utilizar el nombre DNS del servidor CIFS en lugar de las direcciones IP de LIF individuales.

  A partir de ONTAP 9.4, puede mejorar el rendimiento y la tolerancia a fallos del servidor Hyper-V y SQL en configuraciones de SMB al habilitar multicanal de SMB. Para ello, debe tener varias NIC de 1 G, 10 G o más grandes implementadas en el clúster y los clientes.

Requisitos de LIF de datos

- La SVM que aloja la solución de servidor de aplicaciones a través de SMB debe tener al menos una LIF de datos operativos en cada nodo del clúster.

  Los LIF de datos de SVM pueden conmutar por error a otros puertos de datos del clúster, incluidos los nodos que actualmente no alojan datos a los que acceden los servidores de aplicaciones. Además, dado

que el nodo testigo siempre es el partner SFO de un nodo al que está conectado el servidor de aplicaciones, cada nodo del clúster es un nodo testigo potencial.

- Los LIF de datos no deben configurarse para que la reversión se restaure automáticamente.

  Tras un evento de toma de control o devolución, debe revertir manualmente las LIF de datos a sus puertos principales.

- Todas las direcciones IP de LIF de datos deben tener una entrada en DNS y todas las entradas se deben resolver en el nombre del servidor CIFS.

  Los servidores de aplicaciones deben conectarse a recursos compartidos SMB mediante el nombre del servidor CIFS. No configure los servidores de aplicaciones para realizar conexiones mediante direcciones IP de LIF.

- Si el nombre del servidor CIFS es diferente del nombre de la SVM, las entradas DNS se deben resolver en el nombre del servidor CIFS.

Requisitos de volumen y servidor de SMB para Hyper-V mediante SMB

Debe estar al tanto de determinados requisitos de volumen y servidor de SMB al crear configuraciones de Hyper-V mediante SMB para proporcionar operaciones no disruptivas.

Requisitos del servidor SMB

- Se debe habilitar SMB 3.0.

  Esta opción está habilitada de forma predeterminada.

- La opción de servidor CIFS del usuario UNIX predeterminado debe estar configurada con una cuenta de usuario UNIX válida.

  Los servidores de aplicaciones utilizan la cuenta del equipo al crear una conexión SMB. Dado que todos los accesos del bloque de mensajes del servidor requieren que el usuario de Windows se asigne correctamente a una cuenta de usuario de UNIX o a la cuenta de usuario de UNIX predeterminada, ONTAP debe poder asignar la cuenta de equipo del servidor de aplicaciones a la cuenta de usuario UNIX predeterminada.

- Las referencias automáticas al nodo deben estar deshabilitadas (esta funcionalidad está deshabilitada de forma predeterminada).

  Si desea utilizar referencias de nodo automáticas para acceder a datos que no sean archivos de máquina de Hyper-V, debe crear una SVM independiente para esos datos.

- Se debe permitir tanto la autenticación Kerberos como NTLM en el dominio al que pertenece el servidor SMB.

  ONTAP no anuncia el servicio Kerberos para VSS remoto; por lo tanto, el dominio debe configurarse para permitir NTLM.

- La función de copia de sombra debe estar activada.

  Esta funcionalidad está habilitada de forma predeterminada.

- La cuenta de dominio de Windows que utiliza el servicio de copia de sombra al crear instantáneas debe ser miembro del grupo local BUILTIN\Administrators o BUILTIN\Backup Operators del servidor SMB.

Requisitos del volumen

- Los volúmenes utilizados para almacenar archivos de máquinas virtuales se deben crear como volúmenes de estilo de seguridad NTFS.

  Para proporcionar NDOS a los servidores de aplicaciones mediante conexiones SMB disponibles de forma continua, el volumen que contiene el recurso compartido debe ser un volumen NTFS. Además, siempre debe haber sido un volumen NTFS. No se puede cambiar un volumen de estilo de seguridad mixto o un volumen de estilo de seguridad UNIX por un volumen de estilo de seguridad NTFS y utilizarlo directamente para NDOS en recursos compartidos SMB. Si cambia un volumen de estilo de seguridad mixto por un volumen de estilo de seguridad NTFS y piensa usarlo para NDO en recursos compartidos SMB, debe colocar manualmente una ACL en la parte superior del volumen y propagar esa ACL a todos los archivos y carpetas incluidos. De lo contrario, las migraciones de máquinas virtuales o exportaciones de archivos de base de datos e importaciones donde se mueven archivos a otro volumen pueden fallar si los volúmenes de origen o de destino se crearon inicialmente como volúmenes mixtos o de estilo de seguridad UNIX y posteriormente se cambiaron al estilo de seguridad NTFS.

- Para que las operaciones de copia de sombra se realicen correctamente, debe tener suficiente espacio disponible en el volumen.

  El espacio disponible debe ser al menos tan grande como el espacio combinado utilizado por todos los archivos, directorios y subdirectorios contenidos en los recursos compartidos incluidos en el conjunto de copia de seguridad de instantánea. Este requisito solo se aplica a copias instantáneas con recuperación automática.

Información relacionada

"Biblioteca de Microsoft TechNet: technet.microsoft.com/en-us/library/"

Requisitos de volumen y servidor de SMB para SQL Server sobre SMB

Debe estar al tanto de determinados requisitos de volumen y servidor SMB al crear SQL Server en configuraciones de SMB para proporcionar operaciones no disruptivas.

Requisitos del servidor SMB

- Se debe habilitar SMB 3.0.

  Esta opción está habilitada de forma predeterminada.

- La opción de servidor CIFS del usuario UNIX predeterminado debe estar configurada con una cuenta de usuario UNIX válida.

  Los servidores de aplicaciones utilizan la cuenta del equipo al crear una conexión SMB. Dado que todos los accesos del bloque de mensajes del servidor requieren que el usuario de Windows se asigne correctamente a una cuenta de usuario de UNIX o a la cuenta de usuario de UNIX predeterminada, ONTAP debe poder asignar la cuenta de equipo del servidor de aplicaciones a la cuenta de usuario UNIX predeterminada.

  Además, SQL Server utiliza un usuario de dominio como cuenta de servicio de SQL Server. La cuenta de servicio también debe tener asignado el usuario UNIX predeterminado.

- Las referencias automáticas al nodo deben estar deshabilitadas (esta funcionalidad está deshabilitada de forma predeterminada).

  Si desea utilizar referencias de nodo automáticas para acceder a datos que no sean archivos de base de datos de SQL Server, debe crear una SVM independiente para esos datos.

- La cuenta de usuario de Windows utilizada para instalar SQL Server en ONTAP debe tener asignado el privilegio SeSecurityPrivilege.

  Este privilegio se asigna al grupo BUILTIN\Administrators local del servidor SMB.

Requisitos del volumen

- Los volúmenes utilizados para almacenar archivos de máquinas virtuales se deben crear como volúmenes de estilo de seguridad NTFS.

  Para proporcionar NDOS a los servidores de aplicaciones mediante conexiones SMB disponibles de forma continua, el volumen que contiene el recurso compartido debe ser un volumen NTFS. Además, siempre debe haber sido un volumen NTFS. No se puede cambiar un volumen de estilo de seguridad mixto o un volumen de estilo de seguridad UNIX por un volumen de estilo de seguridad NTFS y utilizarlo directamente para NDOS en recursos compartidos SMB. Si cambia un volumen de estilo de seguridad mixto por un volumen de estilo de seguridad NTFS y piensa usarlo para NDO en recursos compartidos SMB, debe colocar manualmente una ACL en la parte superior del volumen y propagar esa ACL a todos los archivos y carpetas incluidos. De lo contrario, las migraciones de máquinas virtuales o exportaciones de archivos de base de datos e importaciones donde se mueven archivos a otro volumen pueden fallar si los volúmenes de origen o de destino se crearon inicialmente como volúmenes mixtos o de estilo de seguridad UNIX y posteriormente se cambiaron al estilo de seguridad NTFS.

- Aunque el volumen que contiene los archivos de la base de datos puede contener uniones, SQL Server no cruza las uniones al crear la estructura de directorio de la base de datos.
- Para que las operaciones de backup del plugin de SnapCenter para Microsoft SQL Server se realicen correctamente, es necesario contar con espacio disponible suficiente en el volumen.

  El volumen en el que residen los archivos de base de datos de SQL Server debe ser lo suficientemente grande como para contener la estructura de directorio de la base de datos y todos los archivos contenidos que residen en el recurso compartido.

Información relacionada

"Biblioteca de Microsoft TechNet: technet.microsoft.com/en-us/library/"

Disponibilidad continua de los requisitos de recursos compartidos y consideraciones para Hyper-V en SMB

Debe tener en cuenta ciertos requisitos y consideraciones a la hora de configurar recursos compartidos disponibles de forma continua para configuraciones de Hyper-V en SMB que admiten operaciones no disruptivas.

Comparta los requisitos

- Los recursos compartidos utilizados por los servidores de aplicaciones deben configurarse con el conjunto de propiedades continuamente disponibles.

  Los servidores de aplicaciones que se conectan a recursos compartidos disponibles de forma continua

reciben controladores persistentes que les permiten volver a conectarse de forma no disruptiva a recursos compartidos de SMB y reclamar bloqueos de archivos tras eventos disruptivos como la toma de control, el retorno al nodo primario y la reubicación de agregados.

- Si desea utilizar los servicios de backup habilitados para VSS remoto, no podrá colocar los archivos Hyper-V en los recursos compartidos que contienen uniones.

  En el caso de recuperación automática, se produce un error en la creación de instantáneas si se encuentra una unión mientras se pasa por el recurso compartido. En el caso no de recuperación automática, la creación de copias redundantes no falla, pero la unión no apunta a nada.

- Si desea utilizar servicios de backup habilitados para VSS remoto con recuperación automática, no puede colocar los archivos de Hyper-V en recursos compartidos que contengan lo siguiente:
  - Enlaces simbólicos, enlaces duros o enlaces con cables
  - Archivos no regulares

    La creación de instantáneas falla si hay vínculos o archivos no regulares en el recurso compartido a instantáneas. Este requisito solo se aplica a copias instantáneas con recuperación automática.

  - Para que las operaciones de copia oculta se realicen correctamente, debe tener suficiente espacio disponible en el volumen (solo para Hyper-V en SMB).

    El espacio disponible debe ser al menos tan grande como el espacio combinado utilizado por todos los archivos, directorios y subdirectorios contenidos en los recursos compartidos incluidos en el conjunto de copia de seguridad de instantánea. Este requisito solo se aplica a copias instantáneas con recuperación automática.

- Las siguientes propiedades compartidas no deben definirse en recursos compartidos disponibles continuamente que utilizan los servidores de aplicaciones:
  - Directorio inicial
  - Almacenamiento de atributos en caché
  - BranchCache

Consideraciones

- Las cuotas están soportadas por recursos compartidos constantemente disponibles.
- La siguiente funcionalidad no es compatible con las configuraciones de Hyper-V mediante SMB:
  - Auditoría
  - FPolicy
- La detección de virus no se realiza en recursos compartidos SMB con el `continuously-availability` parámetro establecido en `Yes`.

Requisitos de recursos compartidos y consideraciones continuamente disponibles para SQL Server en SMB

Debe tener en cuenta ciertos requisitos y consideraciones a la hora de configurar recursos compartidos disponibles de forma continua para configuraciones de SQL Server en SMB que admiten operaciones no disruptivas.

Comparta los requisitos

- Los volúmenes utilizados para almacenar archivos de máquinas virtuales se deben crear como volúmenes de estilo de seguridad NTFS.

  Para proporcionar operaciones no disruptivas para servidores de aplicaciones mediante conexiones SMB disponibles de forma continua, el volumen que contiene el recurso compartido debe ser un volumen NTFS. Además, siempre debe haber sido un volumen NTFS. No se puede cambiar un volumen de estilo de seguridad mixto o un volumen de estilo de seguridad UNIX por un volumen de estilo de seguridad NTFS y usarlo directamente para operaciones no disruptivas sobre recursos compartidos SMB. Si cambia un volumen de estilo de seguridad mixto por un volumen de estilo de seguridad NTFS y piensa usarlo para operaciones no disruptivas en recursos compartidos de SMB, debe colocar manualmente una ACL en la parte superior del volumen y propagar esa ACL a todos los archivos y carpetas incluidos. De lo contrario, las migraciones de máquinas virtuales o exportaciones de archivos de base de datos e importaciones donde se mueven archivos a otro volumen pueden fallar si los volúmenes de origen o de destino se crearon inicialmente como volúmenes mixtos o de estilo de seguridad UNIX y posteriormente se cambiaron al estilo de seguridad NTFS.

- Los recursos compartidos utilizados por los servidores de aplicaciones deben configurarse con el conjunto de propiedades continuamente disponibles.

  Los servidores de aplicaciones que se conectan a recursos compartidos disponibles de forma continua reciben controladores persistentes que les permiten volver a conectarse de forma no disruptiva a recursos compartidos de SMB y reclamar bloqueos de archivos tras eventos disruptivos como la toma de control, el retorno al nodo primario y la reubicación de agregados.

- Aunque el volumen que contiene los archivos de la base de datos puede contener uniones, SQL Server no cruza las uniones al crear la estructura de directorio de la base de datos.
- Para que las operaciones del plugin de SnapCenter para Microsoft SQL Server se realicen correctamente, es necesario contar con espacio disponible suficiente en el volumen.

  El volumen en el que residen los archivos de base de datos de SQL Server debe ser lo suficientemente grande como para contener la estructura de directorio de la base de datos y todos los archivos contenidos que residen en el recurso compartido.

- Las siguientes propiedades compartidas no deben definirse en recursos compartidos disponibles continuamente que utilizan los servidores de aplicaciones:
  - Directorio inicial
  - Almacenamiento de atributos en caché
  - BranchCache

Comparta consideraciones

- Las cuotas están soportadas por recursos compartidos constantemente disponibles.
- La siguiente funcionalidad no es compatible con configuraciones de SQL Server en SMB:
  - Auditoría
  - FPolicy
- La detección de virus no se realiza en recursos compartidos SMB con el `continuously-availability` conjunto de propiedades de recurso compartido.

Consideraciones de VSS remotas para configuraciones de Hyper-V mediante SMB

Al utilizar soluciones de backup habilitadas para VSS remoto para configuraciones de Hyper-V en SMB, debe tener en cuenta determinadas consideraciones.

Consideraciones generales sobre VSS remoto

- Se puede configurar un máximo de 64 recursos compartidos por servidor de aplicaciones de Microsoft.

  La operación de copia de sombra falla si hay más de 64 recursos compartidos en un conjunto de instantáneas. Este es un requisito de Microsoft.

- Solo se permite un conjunto de copias redundantes por servidor CIFS.

  Se producirá un error en las operaciones de copia de sombra si hay una operación de copia de sombra en curso en el mismo servidor CIFS. Este es un requisito de Microsoft.

- No se permiten uniones dentro de la estructura de directorios en la que VSS remoto crea una copia oculta.
  - En el caso de recuperación automática, se producirá un error en la creación de instantáneas si se encuentra una unión mientras se recorre el recurso compartido.
  - En el caso de recuperación no automática, la creación de instantáneas no falla, pero la unión no apunta a nada.

Consideraciones de VSS remotas que sólo son aplicables a las instantáneas con recuperación automática

Ciertos límites solo se aplican a las instantáneas con recuperación automática.

- Se permite una profundidad máxima de directorio de cinco subdirectorios para la creación de instantáneas.

  Esta es la profundidad de directorio sobre la que el servicio de instantáneas crea un conjunto de copia de seguridad de instantánea. La creación de instantáneas falla si los directorios que contienen archivos de máquina virtual están anidados más de cinco niveles. Con esto se pretende limitar el cruce de directorios al clonar el recurso compartido. La profundidad máxima de directorio puede cambiarse con una opción de servidor CIFS.

- La cantidad de espacio disponible en el volumen debe ser adecuada.

  El espacio disponible debe ser al menos tan grande como el espacio combinado utilizado por todos los archivos, directorios y subdirectorios contenidos en los recursos compartidos incluidos en el conjunto de copia de seguridad de instantánea.

- No se permiten vínculos ni archivos no regulares dentro de la estructura de directorios en la que Remote VSS crea una copia de sombra.

  La creación de instantáneas falla si hay vínculos o archivos no regulares en el recurso compartido a la instantánea. El proceso de clonación no es compatible con ellos.

- No se permiten ACL de NFSv4 en directorios.

  Aunque la creación de copias redundantes mantiene las ACL de NFSv4 en los archivos, se pierden las ACL de NFSv4 en los directorios.

- Se permite un máximo de 60 segundos para crear un conjunto de instantáneas.

Las especificaciones de Microsoft permiten un máximo de 60 segundos para crear el conjunto de instantáneas. Si el cliente VSS no puede crear el conjunto de instantáneas en este momento, la operación de copia oculta falla; por lo tanto, esto limita el número de archivos en un conjunto de instantáneas. El número real de archivos o máquinas virtuales que se pueden incluir en un conjunto de backups varía. Este número depende de muchos factores y se debe determinar en cada entorno del cliente.

Requisitos de copia ODX para SQL Server y Hyper-V mediante SMB

La descarga de copias de ODX debe habilitarse si desea migrar archivos de máquinas virtuales o exportar e importar archivos de base de datos directamente desde la ubicación de almacenamiento de origen a la de destino sin enviar datos a través de los servidores de aplicaciones. Hay ciertos requisitos que debe comprender sobre el uso de la descarga de copias ODX mediante soluciones de SQL Server y Hyper-V mediante SMB.

El uso de la descarga de copias ODX ofrece una importante ventaja en cuanto al rendimiento. Esta opción del servidor CIFS está habilitada de forma predeterminada.

- Debe habilitarse SMB 3.0 para utilizar la descarga de copias ODX.
- Los volúmenes de origen deben tener un mínimo de 1.25 GB.
- La deduplicación debe estar activada en los volúmenes utilizados para la descarga de copias.
- Si utiliza volúmenes comprimidos, el tipo de compresión debe ser adaptable y solo se admite el tamaño de grupo de compresión 8K.

  No se admite el tipo de compresión secundaria

- Para utilizar la descarga de copias ODX para migrar «guest» de Hyper-V dentro y entre discos, los servidores Hyper-V deben configurarse para usar discos SCSI.

  El valor predeterminado es configurar discos IDE, pero la descarga de copias ODX no funciona cuando se migran invitados si los discos se crean mediante discos IDE.

Recomendaciones para configuraciones de SQL Server y Hyper-V mediante SMB

Para estar seguro de que sus configuraciones de SQL Server y Hyper-V mediante SMB son sólidas y operativas, debe estar familiarizado con las mejores prácticas recomendadas al configurar las soluciones.

Recomendaciones generales

- Separe los archivos del servidor de aplicaciones de los datos generales del usuario.

  Si es posible, dedique una máquina virtual de almacenamiento (SVM) completa y su almacenamiento a los datos del servidor de aplicaciones.

- Para obtener el mejor rendimiento, no habilite la firma SMB en las SVM que se utilizan para almacenar los datos del servidor de aplicaciones.
- Para obtener el mejor rendimiento y una mejor tolerancia a fallos, permite que SMB MultiChannel proporcione múltiples conexiones entre ONTAP y clientes en una única sesión SMB.

- No cree recursos compartidos disponibles continuamente en ningún recurso compartido distinto a los que se utilizan en la configuración de Hyper-V o SQL Server sobre SMB.
- Deshabilite los notificaciones de cambio en los recursos compartidos utilizados para una disponibilidad continua.
- No mueva el volumen al mismo tiempo que la reubicación de agregados (ARL) porque la ARL tiene fases que pausan algunas operaciones.
- Para las soluciones Hyper-V en SMB, utilice unidades iSCSI de invitado al crear máquinas virtuales en clúster. `.VHDX`Los archivos compartidos no son compatibles con Hyper-V mediante SMB en los recursos compartidos de SMB de ONTAP.

Planifique la configuración de Hyper-V o SQL Server con SMB

Complete la hoja de datos de configuración de volumen

La hoja de trabajo proporciona una forma sencilla de registrar los valores que necesita al crear volúmenes para configuraciones de SQL Server y Hyper-V en SMB.

Para cada volumen, debe especificar la siguiente información:

- El nombre de la máquina virtual de almacenamiento (SVM)

  El nombre de SVM es el mismo para todos los volúmenes.

- Nombre del volumen
- Nombre del agregado

  Puede crear volúmenes en agregados ubicados en cualquier nodo del clúster.

- Tamaño
- Ruta de unión

Debe tener en cuenta lo siguiente al crear volúmenes que se utilizan para almacenar datos del servidor de aplicaciones:

- Si el volumen raíz no tiene estilo de seguridad NTFS, se debe especificar el estilo de seguridad como NTFS al crear el volumen.

  De forma predeterminada, los volúmenes heredan el estilo de seguridad del volumen raíz de la SVM.

- Los volúmenes se deben configurar con la garantía de espacio de volumen predeterminada.
- Opcionalmente, puede configurar la opción de gestión de espacio de autosize.
- Debe configurar la opción que determina la reserva de espacio de snapshot en `0`.
- Debe deshabilitarse la política de Snapshot aplicada al volumen.

  Si está deshabilitada la política de snapshot de SVM, no es necesario especificar una política de snapshot para los volúmenes. Los volúmenes heredan la política de Snapshot para la SVM. Si la política de snapshots para la SVM no está deshabilitada y está configurada para crear Snapshot, debe especificar una política de Snapshot en el nivel del volumen, y esa política debe deshabilitarse. Los backups habilitados para el servicio de copia en la sombra y los backups de SQL Server gestionan la creación y la eliminación de instantáneas.

- No se pueden configurar los reflejos con uso compartido de carga para los volúmenes.

Las rutas de unión en las que tiene previsto crear recursos compartidos que utilicen los servidores de aplicaciones deben seleccionarse de forma que no haya volúmenes con conexiones por debajo del punto de entrada de recurso compartido.

Por ejemplo, si desea almacenar archivos de máquinas virtuales en cuatro volúmenes denominados «'vol1'», «'vol2'», «'vol3'» y «'vol4'», puede crear el espacio de nombres que se muestra en el ejemplo. A continuación, puede crear recursos compartidos para los servidores de aplicaciones en las siguientes rutas de acceso `/data1/vol1:` , `/data1/vol2` `/data2/vol3` , Y `/data2/vol4`.

```
                    Junction                          Junction
Vserver Volume      Active   Junction Path            Path Source
------- ----------- -------- -------------------      -----------
vs1     data1        true     /data1                  RW_volume
vs1     vol1         true     /data1/vol1             RW_volume
vs1     vol2         true     /data1/vol2             RW_volume
vs1     data2        true     /data2                  RW_volume
vs1     vol3         true     /data2/vol3             RW_volume
vs1     vol4         true     /data2/vol4             RW_volume
```

Tipos de información	Valores
Volume 1: Nombre del volumen, agregado, tamaño, ruta de unión	
Volume 2: Nombre del volumen, agregado, tamaño, ruta de unión	
Volume 3: Nombre del volumen, agregado, tamaño, ruta de unión	
Volume 4: Nombre del volumen, agregado, tamaño, ruta de unión	
Volume 5: Nombre del volumen, agregado, tamaño, ruta de unión	
Volume 6: Nombre del volumen, agregado, tamaño, ruta de unión	
Volúmenes adicionales: Nombre del volumen, agregado, tamaño, ruta de unión	

Complete la hoja de datos de configuración de recursos compartidos de SMB

Utilice esta hoja de datos para registrar los valores necesarios cuando cree recursos

compartidos SMB disponibles de forma continua para configuraciones de SQL Server y Hyper-V en SMB.

Información acerca de las propiedades de los recursos compartidos de SMB y las opciones de configuración

Debe especificar la siguiente información para cada recurso compartido:

- El nombre de la máquina virtual de almacenamiento (SVM)

  El nombre de SVM es el mismo para todos los recursos compartidos

- Nombre del recurso compartido
- Ruta
- Comparta propiedades

  Debe configurar las siguientes dos propiedades compartidas:

  - `oplocks`
  - `continuously-available`

No deben configurarse las siguientes propiedades compartidas:

- `homedirectory attributecache`
- `branchcache`
- `access-based-enumeration`
  - Los enlaces simbólicos deben estar desactivados (el valor del `-symlink-properties` parámetro debe ser nulo [""]).

Información sobre las rutas de recursos compartidos

Si utiliza VSS remoto para realizar backups de archivos de Hyper-V, la opción de rutas de uso compartido a la hora de realizar conexiones SMB desde los servidores de Hyper-V a las ubicaciones de almacenamiento en las que están almacenados los archivos de la máquina virtual es importante. Aunque los recursos compartidos se pueden crear en cualquier punto del espacio de nombres, las rutas de los recursos compartidos que utilizan los servidores de Hyper-V no deben contener volúmenes que se han Unido. No se pueden realizar operaciones de copia de sombra en rutas de uso compartido que contienen puntos de unión.

SQL Server no puede cruzar uniones al crear la estructura de directorio de la base de datos. No debe crear rutas de acceso compartidas para SQL Server que contengan puntos de unión.

Por ejemplo, dado el espacio de nombre que se muestra, si desea almacenar archivos de máquina virtual o archivos de base de datos en los volúmenes «`vol1`», «`vol2`», «`vol3`» y «`VOL4`», debe crear recursos compartidos para los servidores de aplicaciones en las siguientes rutas: `/data1/vol1`, `/data1/vol2`, `/data2/vol3` Y `/data2/vol4`.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- -------------------    -----------
vs1     data1        true     /data1                RW_volume
vs1     vol1         true     /data1/vol1           RW_volume
vs1     vol2         true     /data1/vol2           RW_volume
vs1     data2        true     /data2                RW_volume
vs1     vol3         true     /data2/vol3           RW_volume
vs1     vol4         true     /data2/vol4           RW_volume
```

Aunque puede crear recursos compartidos en las `/data1` rutas y `/data2` para la gestión administrativa, no configure los servidores de aplicaciones para que utilicen esos recursos compartidos para almacenar datos.

Hoja de trabajo de planificación

Tipos de información	Valores
Volume 1: Nombre compartido SMB y ruta	
Volume 2: Nombre compartido SMB y ruta	
Volume 3: Nombre compartido SMB y ruta	
Volume 4: Nombre compartido SMB y ruta	
Volume 5: Nombre compartido SMB y ruta	
Volume 6: Nombre compartido SMB y ruta	
Volume 7: Nombre compartido SMB y ruta	
Volúmenes adicionales: Nombres de recursos compartidos SMB y rutas	

Cree configuraciones de ONTAP para proporcionar operaciones no disruptivas con Hyper-V y SQL Server sobre SMB

Cree configuraciones de ONTAP para proporcionar operaciones no disruptivas con Hyper-V y SQL Server sobre SMB

Hay varios pasos de configuración de ONTAP que debe realizar para preparar las instalaciones de Hyper-V y SQL Server que proporcionan operaciones no disruptivas a través de SMB.

Antes de crear la configuración de ONTAP para operaciones no disruptivas con Hyper-V y SQL Server sobre

SMB, deben completarse las siguientes tareas:

- Los servicios de hora deben configurarse en el clúster.
- Las redes deben configurarse para la SVM.
- Se debe crear la SVM.
- Las interfaces de LIF de datos deben configurarse en la SVM.
- DNS debe haberse configurado en la SVM.
- Los servicios de nombres deseados deben configurarse para la SVM.
- Debe crearse el servidor SMB.

Información relacionada

Planifique la configuración de Hyper-V o SQL Server con SMB

Requisitos y consideraciones de configuración

Verificar que la autenticación Kerberos y NTLMv2 están permitidas (Hyper-V en recursos compartidos SMB)

Las operaciones no disruptivas para Hyper-V a través de SMB requieren que el servidor CIFS en una SVM de datos y el servidor Hyper-V permita la autenticación Kerberos y NTLMv2. Debe verificar la configuración en el servidor CIFS y los servidores Hyper-V que controlan los métodos de autenticación permitidos.

Acerca de esta tarea

La autenticación Kerberos es necesaria cuando se hace una conexión compartida disponible continuamente. Parte del proceso de VSS remoto utiliza la autenticación NTLMv2. Por lo tanto, debe ser compatible con las conexiones que utilizan ambos métodos de autenticación en las configuraciones de Hyper-V mediante SMB.

Debe configurarse la siguiente configuración para permitir la autenticación Kerberos y NTLMv2:

- Debe deshabilitarse la política de exportación de SMB en la máquina virtual de almacenamiento (SVM).

La autenticación Kerberos y NTLMv2 siempre están habilitadas en las SVM, pero se pueden utilizar políticas de exportación para restringir el acceso en función del método de autenticación.

Las políticas de exportación de SMB son opcionales y están deshabilitadas de forma predeterminada. Si las directivas de exportación están deshabilitadas, la autenticación Kerberos y NTLMv2 se permite de forma predeterminada en un servidor CIFS.

- El dominio al que pertenecen el servidor CIFS y los servidores Hyper-V debe permitir la autenticación Kerberos y NTLMv2.

La autenticación Kerberos está habilitada de forma predeterminada en dominios de Active Directory. Sin embargo, la autenticación NTLMv2 puede estar permitida, ya sea mediante la configuración de la directiva de seguridad o las directivas de grupo.

Pasos

1. Realice lo siguiente para verificar que las políticas de exportación están deshabilitadas en la SVM:
   a. Configure el nivel de privilegio en Advanced:

set -privilege advanced

b. Compruebe que `-is-exportpolicy-enabled` la opción del servidor CIFS está establecida en `false`:

vserver cifs options show -vserver *vserver_name* -fields vserver,is-exportpolicy-enabled

c. Vuelva al nivel de privilegio de administrador:

set -privilege admin

2. Si no se deshabilitan las políticas de exportación de SMB, inhabilite estas opciones:

vserver cifs options modify -vserver *vserver_name* -is-exportpolicy-enabled false

3. Compruebe que tanto NTLMv2 como Kerberos están permitidos en el dominio.

Para obtener información acerca de cómo determinar qué métodos de autenticación se permiten en el dominio, consulte la biblioteca de Microsoft TechNet.

4. Si el dominio no permite la autenticación NTMLv2, habilite la autenticación NTLMv2 utilizando uno de los métodos descritos en la documentación de Microsoft.

Ejemplo

Los siguientes comandos verifican que las políticas de exportación de SMB se han deshabilitado en la SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-------- ------------------------
vs1      false

cluster1::*> set -privilege admin
```

Compruebe que las cuentas de dominio se asignan al usuario UNIX predeterminado en ONTAP

Hyper-V y SQL Server utilizan cuentas de dominio para crear conexiones SMB a recursos compartidos constantemente disponibles. Para crear correctamente la conexión, la cuenta de equipo debe asignar correctamente a un usuario de UNIX. La forma más cómoda de lograrlo es asignar la cuenta de equipo al usuario UNIX

predeterminado.

Acerca de esta tarea

Hyper-V y SQL Server utilizan las cuentas de equipo de dominio para crear conexiones SMB. Además, SQL Server utiliza una cuenta de usuario de dominio como cuenta de servicio que también realiza conexiones SMB.

Cuando crea una máquina virtual de almacenamiento (SVM), ONTAP crea automáticamente el usuario predeterminado llamado `pcuser` (con un UID de `65534`) y el grupo llamado `pcuser` (con un GID de `65534`) y agrega el usuario predeterminado a la `pcuser` grupo. Si configura una solución de Hyper-V mediante SMB en una SVM que existía antes de actualizar el clúster a Data ONTAP 8.2, es posible que el usuario y el grupo predeterminados no existan. Si no lo hacen, debe crearlos antes de configurar el usuario UNIX predeterminado del servidor CIFS.

Pasos

1. Determine si hay un usuario UNIX predeterminado:

```
vserver cifs options show -vserver <vserver_name>
```

2. Si la opción de usuario predeterminada no está establecida, determine si hay un usuario UNIX que se puede designar como usuario UNIX predeterminado:

```
vserver services unix-user show -vserver <vserver_name>
```

3. Si la opción de usuario predeterminado no está configurada y no hay un usuario UNIX que pueda designarse como usuario UNIX predeterminado, cree el grupo predeterminado y el usuario UNIX predeterminado, y agregue el usuario predeterminado al grupo.
4. El grupo predeterminado generalmente se llama "pcuser" El GID asignado al grupo debe ser `65534`.
   a. Cree el grupo predeterminado:

```
vserver services unix-group create -vserver <vserver_name> -name
pcuser -id 65534
```

   b. Cree el usuario predeterminado y agregue el usuario predeterminado al grupo predeterminado:

```
vserver services unix-user create -vserver <vserver_name> -user
pcuser -id 65534 -primary-gid 65534
```

   c. Compruebe que el usuario predeterminado y el grupo predeterminado están configurados correctamente:

```
vserver services unix-user show -vserver <vserver_name>
```

```
vserver services unix-group show -vserver <vserver_name> -members
```

5. Si el usuario predeterminado del servidor CIFS no está configurado, realice lo siguiente:
   a. Configure el usuario predeterminado:

```
vserver cifs options modify -vserver <vserver_name> -default-unix
-user pcuser
```

   b. Compruebe que el usuario UNIX predeterminado está configurado correctamente:

```
vserver cifs options show -vserver <vserver_name>
```

6. Para verificar que la cuenta de equipo del servidor de aplicaciones se asigna correctamente al usuario predeterminado, asigne una unidad a un recurso compartido que reside en la SVM y confirme la asignación del usuario Windows en la asignación de usuario UNIX con el `vserver cifs session show` comando.

   Obtenga más información sobre `vserver cifs options` en el "Referencia de comandos del ONTAP".

Ejemplo

Los siguientes comandos determinan que el usuario predeterminado del servidor CIFS no está configurado, pero determinan que el `pcuser` usuario y `pcuser` El grupo existe. El `pcuser` El usuario se asigna como usuario predeterminado del servidor CIFS en SVM vs1.

```
cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : -
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -



cluster1::> vserver services unix-user show
           User            User   Group  Full
Vserver    Name            ID     ID     Name
---------- --------------- ------ ------ ----------------
vs1        nobody          65535  65535  -
```

```
vs1       pcuser          65534  65534  -
vs1       root            0      1      -

cluster1::> vserver services unix-group show -members
Vserver        Name                ID
vs1            daemon              1
       Users: -
vs1            nobody              65535
       Users: -
vs1            pcuser              65534
       Users: -
vs1            root                0
       Users: -

cluster1::> vserver cifs options modify -vserver vs1 -default-unix-user
pcuser

cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

Compruebe que el estilo de seguridad del volumen raíz de SVM se haya establecido en NTFS

Para garantizar que las operaciones no disruptivas de Hyper-V y SQL Server sobre SMB se realicen correctamente, los volúmenes se deben crear con un estilo de seguridad NTFS. Dado que el estilo de seguridad del volumen raíz se aplica de manera predeterminada a los volúmenes creados en la máquina virtual de almacenamiento (SVM), el estilo de seguridad del volumen raíz se debe establecer en NTFS.

Acerca de esta tarea

- Puede especificar el estilo de seguridad del volumen raíz en el momento de crear la SVM.
- Si la SVM no se crea con el volumen raíz establecido en estilo de seguridad NTFS, puede cambiar el estilo de seguridad más adelante mediante `volume modify` el comando.

Pasos

1. Determine el estilo de seguridad actual del volumen raíz de la SVM:

   `volume show -vserver` *`vserver_name`* `-fields vserver,volume,security-style`

2. Si el volumen raíz no es un volumen con estilo de seguridad NTFS, cambie el estilo de seguridad a NTFS:

   volume modify -vserver *vserver_name* -volume root_volume_name -security-style ntfs

3. Compruebe que el volumen raíz de la SVM esté establecido en el estilo de seguridad NTFS:

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

Ejemplo

Los siguientes comandos verifican que el estilo de seguridad del volumen raíz es NTFS en la SVM vs1:

```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style
ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   ntfs
```

Comprobar que se han configurado las opciones necesarias del servidor CIFS

Debe verificar que las opciones del servidor CIFS necesarias se encuentran habilitadas y configuradas según los requisitos para las operaciones no disruptivas de Hyper-V y SQL Server sobre SMB.

Acerca de esta tarea

- Se deben habilitar SMB 2.x y SMB 3.0.
- La descarga de copias ODX debe estar habilitada para utilizar el rendimiento, lo que mejora la descarga de copias.
- Se deben habilitar los servicios de copia de volúmenes redundantes de VSS si la solución Hyper-V mediante SMB utiliza servicios de backup habilitados con VSS remoto (solo Hyper-V).

Pasos

1. Compruebe que las opciones necesarias del servidor CIFS estén habilitadas en la máquina virtual de almacenamiento (SVM):
   a. Configure el nivel de privilegio en Advanced:

      set -privilege advanced

   b. Introduzca el siguiente comando:

vserver cifs options show -vserver *vserver_name*

Las siguientes opciones se deben definir en `true`:

- `-smb2-enabled`
- `-smb3-enabled`
- `-copy-offload-enabled`
- `-shadowcopy-enabled` (Solo Hyper-V)

2. Si alguna de las opciones no está definida en `true`, realice lo siguiente:
   a. Establezca en `true` mediante `vserver cifs options modify` el comando.
   b. Compruebe que las opciones están definidas en `true` mediante `vserver cifs options show` el comando.
3. Vuelva al nivel de privilegio de administrador:

set -privilege admin

Ejemplo

Los siguientes comandos verifican que las opciones necesarias para la configuración de Hyper-V sobre SMB están habilitadas en SVM vs1. En el ejemplo, es necesario habilitar la descarga de copias ODX para satisfacer los requisitos de opciones.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
------- ------------ ------------ -------------------- ------------------
vs1     true         true         false                true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-------- --------------------
vs1      true

cluster1::*> set -privilege admin
```

Configure multicanal de SMB para un mayor rendimiento y 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, mejora el rendimiento y la tolerancia a fallos para Hyper-V y SQL Server en configuraciones SMB.

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: -
```

Crear volúmenes de datos NTFS

Debe crear volúmenes de datos NTFS en la máquina virtual de almacenamiento (SVM) antes de poder configurar recursos compartidos disponibles de forma continua para usarlos con Hyper-V o SQL Server en servidores de aplicaciones SMB. Use la hoja de cálculo de configuración de volúmenes para crear los volúmenes de datos.

Acerca de esta tarea

Existen parámetros opcionales que se pueden usar para personalizar un volumen de datos. Para obtener más información sobre la personalización de los volúmenes, consulte "Gestión de almacenamiento lógico".

A medida que cree los volúmenes de datos, no debe crear puntos de unión en un volumen que contenga los siguientes:

- Archivos de Hyper-V para los que ONTAP realiza instantáneas
- Archivos de base de datos de SQL Server de los que se realiza un backup mediante SQL Server

Si crea de forma accidental un volumen que utiliza un estilo de seguridad mixto o UNIX, no se puede cambiar el volumen a un volumen de estilo de seguridad NTFS y, a continuación, usarlo directamente para crear recursos compartidos disponibles de forma continua para operaciones no disruptivas. Las operaciones no disruptivas para Hyper-V y SQL Server sobre SMB no funcionan correctamente a menos que los volúmenes utilizados en la configuración se creen como volúmenes de estilo de seguridad NTFS. Debe eliminar el volumen y volver a crear el volumen con estilo de seguridad NTFS. También es posible asignar el volumen en un host de Windows y aplicar una ACL en la parte superior del volumen y propagar la ACL a todos los archivos y carpetas del volumen.

Pasos

1. Cree el volumen de datos introduciendo el comando correspondiente:

Si desea crear un volumen en una SVM donde el estilo de seguridad del volumen raíz es…	Introduzca el comando…
NTFS	`volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size integer[KB|MB|GB|TB|PB] -junction-path path`
No NTFS	`volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size integer[KB|MB|GB|TB|PB]- security-style ntfs -junction-path path`

2. Compruebe que la configuración del volumen sea correcta:

```
volume show -vserver vserver_name -volume volume_name
```

Crear recursos compartidos de SMB disponibles de forma continua

Después de crear los volúmenes de datos, puede crear los recursos compartidos disponibles de forma continua que los servidores de aplicaciones utilizan para acceder a los archivos de configuración y de la máquina virtual Hyper-V y los archivos de la base de datos de SQL Server. Debe utilizar la hoja de datos de configuración del recurso compartido a medida que crea los recursos compartidos de SMB.

Pasos

1. Muestre información sobre los volúmenes de datos existentes y sus rutas de unión:

```
volume show -vserver vserver_name -junction
```

2. Crear un recurso compartido de SMB disponible de forma continua:

```
vserver cifs share create -vserver vserver_name -share-name share_name -path
path -share-properties oplocks,continuously-available -symlink "" [-comment
text]
```

- Opcionalmente, puede añadir un comentario a la configuración del recurso compartido.
- De forma predeterminada, la propiedad offline files share se configura en el recurso compartido y se establece en `manual`.
- ONTAP crea el recurso compartido con el permiso de recurso compartido predeterminado de Windows de `Everyone` / `Full Control`.

3. Repita el paso anterior para todos los recursos compartidos de la hoja de datos de configuración del recurso compartido.
4. Compruebe que la configuración es correcta mediante `vserver cifs share show` el comando.
5. Configure los permisos de archivo NTFS en los recursos compartidos disponibles continuamente asignando una unidad a cada recurso compartido y configurando los permisos de archivo mediante la ventana **Propiedades de Windows**.

Ejemplo

Los siguientes comandos crean un recurso compartido disponible de forma continua llamado «data2» en la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1. Los vínculos simbólicos están deshabilitados estableciendo `-symlink` el parámetro en `""`:

```
cluster1::> volume show -vserver vs1 -junction
                      Junction                  Junction
Vserver   Volume      Active   Junction Path    Path Source
--------- ----------- -------- ---------------- ------------
vs1       data        true     /data            RW_volume
vs1       data1       true     /data/data1      RW_volume
vs1       data2       true     /data/data2      RW_volume
vs1       vs1_root    -        /                -

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data/data2
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Agregue el privilegio SeSecurityPrivilege a la cuenta de usuario (para recursos compartidos SMB de SQL Server).

La cuenta de usuario de dominio utilizada para instalar el servidor SQL debe tener asignado el privilegio "SeSecurityPrivilege" para realizar determinadas acciones en el servidor CIFS que requieren privilegios no asignados de forma predeterminada a los usuarios de dominio.

Antes de empezar

La cuenta de dominio utilizada para instalar SQL Server ya debe existir.

Acerca de esta tarea

Al agregar el privilegio a la cuenta del instalador de SQL Server, ONTAP podría validar la cuenta poniéndose en contacto con el controlador de dominio. Es posible que se produzca un error en el comando si ONTAP no puede comunicarse con la controladora de dominio.

Pasos

1. Añada el privilegio "SeSecurityPrivilege":

   vserver cifs users-and-groups privilege add-privilege -vserver *vserver_name* -user-or-group-name *account_name* -privileges SeSecurityPrivilege

   El valor del `-user-or-group-name` parámetro es el nombre de la cuenta de usuario de dominio utilizada para instalar SQL Server.

2. Compruebe que el privilegio se aplica a la cuenta:

   vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *account_name*

Ejemplo

El siguiente comando agrega el privilegio "SeSecurityPrivilege" a la cuenta del instalador de SQL Server en el dominio DE EJEMPLO de la máquina virtual de almacenamiento (SVM) vs1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\SQLinstaller -privileges
SeSecurityPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name          Privileges
--------- --------------------       ---------------
vs1       EXAMPLE\SQLinstaller       SeSecurityPrivilege
```

Configurar la profundidad del directorio de copia de sombra de VSS (para Hyper-V mediante recursos compartidos de SMB)

Opcionalmente, puede configurar la profundidad máxima de directorios dentro de recursos compartidos SMB en los que crear copias de sombra. Este parámetro resulta útil si desea controlar manualmente el nivel máximo de subdirectorios en los que ONTAP debe crear instantáneas.

Antes de empezar

La función de copia de sombra VSS debe estar activada.

Acerca de esta tarea

El valor predeterminado es crear instantáneas para un máximo de cinco subdirectorios. Si el valor está definido en `0`, ONTAP crea copias shadow para todos los subdirectorios.

> Aunque puede especificar que la profundidad del directorio del conjunto de instantáneas incluya más de cinco subdirectorios o todos los subdirectorios, existe el requisito de Microsoft de que la creación del conjunto de instantáneas se lleve a cabo en 60 segundos. La creación del conjunto de instantáneas falla si no se puede completar en este momento. La profundidad del directorio de instantáneas que elija no debe hacer que el tiempo de creación supere el límite de tiempo.

Pasos

1. Configure el nivel de privilegio en Advanced:

   set -privilege advanced

2. Establezca la profundidad del directorio de copia de sombra VSS en el nivel deseado:

   vserver cifs options modify -vserver *vserver_name* -shadowcopy-dir-depth integer

   vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6

3. Vuelva al nivel de privilegio de administrador:

   set -privilege admin

Gestione Hyper-V y SQL Server con las configuraciones de SMB

Configure los recursos compartidos existentes para una disponibilidad continua

Puede modificar los recursos compartidos existentes para que estén siempre disponibles y que los servidores de aplicaciones de Hyper-V y SQL Server utilicen para acceder de forma no disruptiva a los archivos de configuración y de máquinas virtuales de Hyper-V, así como a los archivos de bases de datos de SQL Server.

Acerca de esta tarea

No puede utilizar un recurso compartido existente como un recurso compartido disponible de forma continua para las operaciones no disruptivas con servidores de aplicaciones a través de SMB si el recurso compartido tiene las siguientes características:

- Si la `homedirectory` propiedad Compartir está establecida en ese recurso compartido
- Si el recurso compartido contiene enlaces simbólicos activados o enlaces con cables
- Si el recurso compartido contiene volúmenes juntados por debajo de la raíz del recurso compartido

Debe verificar que los dos parámetros de recursos compartidos siguientes estén configurados correctamente:

- `-offline-files`El parámetro se establece en `manual` (el valor por defecto) o `none`.
- Los enlaces simbólicos deben estar desactivados.

Deben configurarse las siguientes propiedades compartidas:

- `continuously-available`
- `oplocks`

No se deben establecer las siguientes propiedades compartidas. Si están presentes en la lista de propiedades de recursos compartidos actuales, deben eliminarse del recurso compartido continuamente disponible:

- `attributecache`
- `branchcache`

Pasos

1. Mostrar la configuración actual de los parámetros de recursos compartidos y la lista actual de propiedades de recursos compartidos configuradas:

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
```

2. Si es necesario, modifique los parámetros de uso compartido para deshabilitar los enlaces simbólicos y establezca los archivos sin conexión en manual mediante `vserver cifs share modify` el comando.
   - Puede desactivar los enlaces simbólicos definiendo el valor del `-symlink` parámetro en `""`.
   - Puede establecer el `-offline-files` parámetro en el valor correcto especificando `manual`.
3. Agregue `continuously-available` la propiedad Compartir y, si es necesario, la `oplocks` propiedad Compartir:

```
vserver cifs share properties add -vserver <vserver_name> -share-name
<share_name> -share-properties continuously-available[,oplock]
```

   Si la `oplocks` propiedad Compartir no está establecida, debe agregarla junto con la `continuously-available` propiedad Compartir.

4. Quite todas las propiedades de recursos compartidos que no sean compatibles con recursos compartidos disponibles de forma continua:

```
vserver cifs share properties remove -vserver <vserver_name> -share-name
<share_name> -share-properties properties[,...]
```

   Puede quitar una o varias propiedades de recursos compartidos si especifica las propiedades de recursos compartidos con una lista delimitada por comas.

5. Compruebe que los `-symlink` `-offline-files` parámetros y se han definido correctamente:

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
-fields symlink-properties,offline-files
```

6. Compruebe que la lista de propiedades de recursos compartidos configuradas es correcta:

```
vserver cifs share properties show -vserver <vserver_name> -share-name
<share_name>
```

Ejemplos

El siguiente ejemplo muestra cómo configurar un recurso compartido existente denominado «share1» en la máquina virtual de almacenamiento (SVM) «VS1» para NDOS con un servidor de aplicaciones mediante SMB:

- Los vínculos simbólicos se desactivan en el recurso compartido definiendo `-symlink` el parámetro en `""`.

- El `-offline-file` parámetro se modifica y se establece en `manual`.
- `continuously-available`La propiedad Compartir se agrega al recurso compartido.
- `oplocks`La propiedad de recurso compartido ya está en la lista de propiedades de recurso compartido; por lo tanto, no es necesario agregarla.
- La `attributecache` propiedad Compartir se elimina del recurso compartido.
- `browsable`La propiedad de recurso compartido es opcional para un recurso compartido de disponibilidad continua utilizado para NDOS con servidores de aplicaciones a través de SMB y se conserva como una de las propiedades de recurso compartido.

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1

                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: vs1
                         Path: /data
             Share Properties: oplocks
                               browsable
                               attributecache
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: data
                Offline Files: documents
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share modify -vserver vs1 -share-name share1
-offline-file manual -symlink ""

cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties continuously-available

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share1 -share-properties attributecache

cluster1::> vserver cifs share show -vserver vs1 -share-name share1
-fields symlink-properties,offline-files
vserver  share-name symlink-properties offline-files
-------- ---------- ------------------ -------------
vs1      share1    -                  manual

cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1

         Vserver: vs1
           Share: share1
Share Properties: oplocks
                  browsable
                  continuously-available
```

Habilite o deshabilite las copias de sombra de VSS para backups de Hyper-V mediante SMB

Si utiliza una aplicación de backup compatible con VSS para realizar backups de los archivos de máquina virtual de Hyper-V almacenados en recursos compartidos SMB, debe habilitarse la copia de sombra de VSS. Puede deshabilitar la copia de sombra de VSS si no utiliza aplicaciones de backup compatibles con VSS. El valor predeterminado es activar la copia de sombra VSS.

Acerca de esta tarea

Puede activar o desactivar las instantáneas VSS en cualquier momento.

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Ejecute una de las siguientes acciones:

Si desea que las copias redundantes de VSS sean…	Introduzca el comando…
Activado	`vserver cifs options modify -vserver vserver_name -shadowcopy-enabled true`
Deshabilitado	`vserver cifs options modify -vserver vserver_name -shadowcopy-enabled false`

3. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Ejemplo

Los siguientes comandos habilitan las copias de sombra de VSS en la SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -shadowcopy-enabled
true

cluster1::*> set -privilege admin
```

Utilice estadísticas para supervisar la actividad de Hyper-V y SQL Server mediante SMB

Determine qué objetos y contadores de estadísticas están disponibles en ONTAP

Para poder obtener información acerca de las estadísticas de CIFS, SMB, auditoría y BranchCache hash, y supervisar el rendimiento, debe conocer los objetos y contadores disponibles desde los cuales puede obtener datos.

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Ejecute una de las siguientes acciones:

Si desea determinar…	Introduzca…
Qué objetos están disponibles	`statistics catalog object show`
Objetos específicos disponibles	`statistics catalog object show -object` *`object_name`*
Qué contadores están disponibles	`statistics catalog counter show -object` *`object_name`*

   Obtenga más información sobre `statistics catalog object show` y `statistics catalog counter show` en el "Referencia de comandos del ONTAP" .

3. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Ejemplos

El siguiente comando muestra descripciones de los objetos de estadísticas seleccionados relacionados con CIFS y acceso SMB en el clúster tal y como se ve en el nivel de privilegio avanzado:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

El siguiente comando muestra información acerca de algunos de los contadores del `cifs` objeto como se ve en el nivel de privilegio avanzado:

> En este ejemplo no se muestran todos los contadores disponibles para `cifs` el objeto; la salida se trunca.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
--------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                                vserver_1:10.72.205.179
    instance_uuid                                       2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

Obtenga más información sobre `statistics start` en el "Referencia de comandos del ONTAP".

Mostrar estadísticas de SMB en ONTAP

Puede mostrar varias estadísticas de SMB para supervisar el rendimiento y diagnosticar problemas.

Pasos

1. Utilice `statistics start` `statistics stop` los comandos y opcionales para recopilar una muestra de datos.
2. Ejecute una de las siguientes acciones:

Si desea mostrar estadísticas de…	Introduzca el siguiente comando…
Todas las versiones de SMB	**`statistics show -object cifs`**
SMB 1,0	**`statistics show -object smb1`**
SMB 2.x y SMB 3.0	**`statistics show -object smb2`**
Subsistema SMB del nodo	**`statistics show -object nblade_cifs`**

Información relacionada

- "Las estadísticas muestran"
- "Las estadísticas comienzan"
- "las estadísticas se detienen"

Compruebe que la configuración admite operaciones no disruptivas

Utilice la supervisión del estado para determinar si el estado de las operaciones no disruptivas es correcto

La supervisión del estado proporciona información sobre el estado del sistema en todo el clúster. El monitor de estado supervisa la configuración de Hyper-V y SQL Server en SMB para garantizar las operaciones no disruptivas (NDO) de los servidores de aplicaciones. Si el estado es degradado, puede ver detalles del problema, incluidas la causa probable y las acciones de recuperación recomendadas.

Hay varios monitores de estado. ONTAP supervisa el estado general del sistema y el de los monitores de estado individuales. El monitor de estado de conectividad del nodo contiene el subsistema CIFS-NDO. El monitor tiene un conjunto de políticas de estado que activan alertas si ciertas condiciones físicas pueden producir interrupciones y, si se produce una condición disruptiva, genera alertas y proporciona información sobre acciones correctivas. Para OPERACIONES NO DISRUPTIVAS en configuraciones de SMB, se generan alertas de las dos condiciones siguientes:

ID de alerta	Gravedad	Condición
HaNotReadyCifsNdo_Alert	Importante	Se han abierto uno o varios archivos alojados por un volumen de un agregado del nodo a través de un recurso compartido de SMB disponible de forma continua con la promesa de persistencia en caso de fallo; sin embargo, la relación de alta disponibilidad con el partner no está configurada o no es correcta.
NoStandbyLifCifsNdo_Alert	Menor	La máquina virtual de almacenamiento (SVM) está sirviendo datos activamente en SMB a través de un nodo. Además, hay archivos SMB abiertos de forma persistente en recursos compartidos disponibles de forma continua; sin embargo, su nodo de partner no está exponiendo ningún LIF de datos activo para la SVM.

Muestre el estado de funcionamiento no disruptivo mediante la supervisión del estado del sistema

Puede usar `system health` los comandos para mostrar información sobre el estado general del sistema del clúster y el estado del subsistema CIFS-NDO, para responder a alertas, configurar futuras alertas y mostrar información sobre la configuración de la supervisión del estado.

Pasos

1. Supervise el estado realizando la acción correspondiente:

Si desea mostrar…	Introduzca el comando…
El estado del sistema, que refleja el estado general de los monitores de estado individuales	**system health status show**
Información sobre el estado del subsistema CIFS-NDO	**system health subsystem show -subsystem CIFS-NDO -instance**

2. Muestre información acerca de cómo se configura la supervisión de alertas CIFS-NDO mediante las acciones adecuadas:

Si desea mostrar información acerca de…	Introduzca el comando…
La configuración y el estado del monitor de estado del subsistema CIFS-NDO, como nodos supervisados, estado de inicialización y estado	**system health config show -subsystem CIFS-NDO**

Si desea mostrar información acerca de…	Introduzca el comando…
Las alertas CIFS-NDO que un monitor de estado puede generar potencialmente	**system health alert definition show -subsystem CIFS-NDO**
Las políticas de supervisión del estado de CIFS-NDO, que determinan cuándo se generan las alertas	**system health policy definition show -monitor node-connect**

Utilice `-instance` el parámetro para mostrar información detallada.

Ejemplos

En el siguiente resultado se muestra información acerca del estado general del clúster y del subsistema CIFS-NDO:

```
cluster1::> system health status show
Status
---------------
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                  Subsystem: CIFS-NDO
                     Health: ok
        Initialization State: initialized
Number of Outstanding Alerts: 0
 Number of Suppressed Alerts: 0
                       Node: node2
  Subsystem Refresh Interval: 5m
```

En el siguiente resultado, se muestra información detallada sobre la configuración y el estado del monitor de estado del subsistema CIFS-NDO:

```
cluster1::> system health config show -subsystem CIFS-NDO -instance

                          Node: node1
                       Monitor: node-connect
                     Subsystem: SAS-connect, HA-health, CIFS-NDO
                        Health: ok
               Monitor Version: 2.0
            Policy File Version: 1.0
                       Context: node_context
                    Aggregator: system-connect
                      Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

                          Node: node2
                       Monitor: node-connect
                     Subsystem: SAS-connect, HA-health, CIFS-NDO
                        Health: ok
               Monitor Version: 2.0
            Policy File Version: 1.0
                       Context: node_context
                    Aggregator: system-connect
                      Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0
```

Compruebe la configuración de recursos compartidos de SMB continuamente disponible

Para admitir operaciones no disruptivas, los recursos compartidos de Hyper-V y SQL Server SMB deben configurarse como recursos compartidos constantemente disponibles. Además, hay otros ajustes de recursos compartidos que debe comprobar. Debe verificar que los recursos compartidos están correctamente configurados para proporcionar operaciones sin interrupciones para los servidores de aplicaciones, en caso de que se produzcan eventos de interrupción planificados o no planificados.

Acerca de esta tarea

Debe verificar que los dos parámetros de recursos compartidos siguientes estén configurados correctamente:

- `-offline-files`El parámetro se establece en `manual` (el valor por defecto) o `none`.
- Los enlaces simbólicos deben estar desactivados.

Para que las operaciones sean correctas no disruptivas, debe configurarse las siguientes propiedades compartidas:

- `continuously-available`
- `oplocks`

No deben configurarse las siguientes propiedades compartidas:

- `homedirectory`
- `attributecache`
- `branchcache`
- `access-based-enumeration`

Pasos

1. Compruebe que los archivos fuera de línea están definidos en `manual` o `disabled` y que los enlaces simbólicos están desactivados:

   vserver cifs shares show -vserver *vserver_name*

2. Compruebe que los recursos compartidos de SMB están configurados para una disponibilidad continua:

   vserver cifs shares properties show -vserver *vserver_name*

Ejemplos

En el siguiente ejemplo, se muestra la configuración de recurso compartido para un recurso compartido llamado «shara1» en la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1. Los archivos fuera de línea se establecen en `manual` y los enlaces simbólicos se desactivan (designados por un guión en `Symlink Properties` la salida del campo):

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: VS1
                         Path: /data/share1
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

En el siguiente ejemplo, se muestran las propiedades de uso compartido de un recurso compartido denominado «shara1» en la SVM vs1:

```
cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1
Vserver    Share   Properties
---------  ------  ----------
vs1        share1  oplocks
                   continuously-available
```

Comprobar el estado de la LIF

Aunque configure máquinas virtuales de almacenamiento (SVM) con Hyper-V y SQL Server en configuraciones de SMB para tener LIF en cada nodo de un clúster, durante las operaciones diarias, algunas LIF se pueden mover a puertos de otro nodo. Debe verificar el estado de LIF y realizar las acciones correctivas que sean necesarias.

Acerca de esta tarea

Para proporcionar soporte de operaciones no disruptivas y fluido, cada nodo de un clúster debe tener al menos un LIF para la SVM y todos los LIF deben estar asociados a un puerto de inicio. Si algunos de los LIF configurados actualmente no están asociados a su puerto de inicio, debe solucionar cualquier problema de los puertos y, a continuación, revertir los LIF a su puerto de inicio.

Pasos

1. Muestra información acerca de las LIF configuradas para la SVM:

   network interface show -vserver *vserver_name*

   En este ejemplo, "'lif1'" no se encuentra en el puerto de origen.

`network interface show -vserver vs1`

```
            Logical    Status     Network          Current    Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node       Port
Home
----------- ---------- ---------- ---------------- ---------- -------
----
vs1
            lif1         up/up    10.0.0.128/24    node2      e0d
false
            lif2         up/up    10.0.0.129/24    node2      e0d
true
```

Obtenga más información sobre `network interface show` en el "Referencia de comandos del ONTAP".

2. Si algunas de las LIF no están en sus puertos raíz, realice los pasos siguientes:

   a. Para cada LIF, determine en qué puerto de inicio de la LIF se encuentra:

   network interface show -vserver *vserver_name* -lif *lif_name* -fields home-node,home-port

   network interface show -vserver vs1 -lif lif1 -fields home-node,home-port

   ```
   vserver lif  home-node  home-port
   ------- ---- ---------- ---------
   vs1     lif1 node1      e0d
   ```

   b. Para cada LIF, determine si el puerto de inicio del LIF está activo:

   network port show -node *node_name* -port *port* -fields port,link

   `network port show -node node1 -port e0d -fields port,link`

   ```
   node       port link
   ---------- ---- ----
   node1      e0d  up
   ```

   En este ejemplo, "`lif1`" debe ser migrado de vuelta a su puerto de origen, `node1:e0d`.

   Obtenga más información sobre `network port show` en el "Referencia de comandos del ONTAP".

3. Si alguna de las interfaces de red del puerto principal a las que deben estar asociadas las LIF no tiene `up` estado, resuelva el problema para que estas interfaces estén activas. Obtenga más información sobre `up` en el "Referencia de comandos del ONTAP".

4. Si es necesario, revierte las LIF a sus puertos de inicio:

   network interface revert -vserver *vserver_name* -lif *lif_name*

   network interface revert -vserver vs1 -lif lif1

   Obtenga más información sobre `network interface revert` en el "Referencia de comandos del ONTAP".

5. Compruebe que cada nodo del clúster tiene un LIF activo para la SVM:

   network interface show -vserver *vserver_name*

   network interface show -vserver vs1

```
            Logical    Status     Network          Current    Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node       Port
Home
----------- ---------- ---------- ---------------- ---------- -------
----
vs1
            lif1         up/up    10.0.0.128/24    node1      e0d
true
            lif2         up/up    10.0.0.129/24    node2      e0d
true
```

Determinar si las sesiones SMB están disponibles continuamente

Muestra información de la sesión SMB

Puede mostrar información acerca de las sesiones SMB establecidas, incluidos la conexión SMB y el ID de sesión y la dirección IP de la estación de trabajo mediante la sesión. Es posible mostrar información sobre la versión del protocolo SMB de la sesión y el nivel de protección disponible continuamente, lo que ayuda a identificar si la sesión admite operaciones no disruptivas.

Acerca de esta tarea

Puede mostrar información de todas las sesiones de la SVM en formato de resumen. Sin embargo, en muchos casos, la cantidad de producción que se devuelve es grande. Puede personalizar la información que se muestra en el resultado especificando parámetros opcionales:

- Puede utilizar el parámetro opcional `-fields` para mostrar resultados sobre los campos seleccionados.

  Puede introducir `-fields ?` para determinar qué campos puede utilizar.

- Puede usar el `-instance` parámetro para mostrar información detallada acerca de las sesiones SMB establecidas.
- Puede usar `-fields` el parámetro o el `-instance` parámetro solo o en combinación con otros

parámetros opcionales.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea mostrar información de la sesión SMB…	Introduzca el siguiente comando…
Para todas las sesiones del SVM en formato de resumen	**vserver cifs session show -vserver *vserver_name***
En un ID de conexión especificado	**vserver cifs session show -vserver *vserver_name* -connection-id integer**
Desde una dirección IP de estación de trabajo especificada	**vserver cifs session show -vserver *vserver_name* -address *workstation_IP_address***
En una dirección IP de LIF especificada	**vserver cifs session show -vserver *vserver_name* -lif -address *LIF_IP_address***
En un nodo especificado	`*vserver cifs session show -vserver *vserver_name* -node {node_name
local}*`	Desde un usuario de Windows especificado
vserver cifs session show -vserver *vserver_name* -windows-user *user_name* El formato para `user_name` es `[domain]\user`.	Con un mecanismo de autenticación especificado

Si desea mostrar información de la sesión SMB…	Introduzca el siguiente comando…
vserver cifs session show -vserver *vserver_name* -auth -mechanism authentication_mechanism El valor de `-auth -mechanism` puede ser uno de los siguientes: • `NTLMv1` • `NTLMv2` • `Kerberos` • `Anonymous`	Con una versión de protocolo especificada

Si desea mostrar información de la sesión SMB…	Introduzca el siguiente comando…
`vserver cifs session show -vserver vserver_name -protocol-version protocol_version` El valor de `-protocol-version` puede ser uno de los siguientes: • `SMB1` • `SMB2` • `SMB2_1` • `SMB3` • `SMB3_1`	Con un nivel especificado de protección continua disponible

Si desea mostrar información de la sesión SMB…	Introduzca el siguiente comando…
`vserver cifs session show -vserver` ***`vserver_name`*** **`-continuously -available`** ***`continuously_available_protection_level`*** El valor de `-continuously -available` puede ser uno de los siguientes: • `No` • `Yes` • `Partial`	Con un estado de sesión de firma SMB especificado

Ejemplos

El siguiente comando muestra información de sesión para las sesiones en SVM vs1 establecidas desde una estación de trabajo con dirección IP 10.1.1.1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files         Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

un archivo abierto continuam ente

El siguiente comando muestra información detallada de la sesión para las sesiones con protección continuamente disponible en SVM vs1. La conexión se realizó mediante la cuenta de dominio.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                      Node: node1
                   Vserver: vs1
                Session ID: 1
              Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
             Windows User: DOMAIN\SERVER1$
                UNIX User: pcuser
              Open Shares: 1
               Open Files: 1
               Open Other: 0
            Connected Time: 10m 43s
                 Idle Time: 1m 19s
          Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

a no están abiertos con la protección disponible continuam ente.

El siguiente comando muestra información de sesión en una sesión mediante SMB 3.0 y SMB MultiChannel en SVM vs1. En el ejemplo, el usuario se conectó a este recurso compartido desde un cliente con capacidad para SMB 3.0 mediante la dirección IP de LIF; por lo tanto, el mecanismo de autenticación se estableció de forma predeterminada en NTLMv2. La conexión se debe realizar mediante la autenticación Kerberos para

conectarse con la protección disponible continuamente.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
             **Connection IDs: 3151272607,31512726078,3151272609
           Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
               Connected Time: 6m 22s
                    Idle Time: 5m 42s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Muestra información sobre los archivos SMB abiertos en ONTAP

Es posible ver información sobre los archivos SMB abiertos, incluidos la conexión de SMB y el ID de sesión, el volumen de host, el nombre del recurso compartido y la ruta del recurso compartido. También es posible ver información acerca del nivel de protección continuamente disponible de un archivo, lo cual es útil para determinar si un archivo abierto está en un estado que admite operaciones no disruptivas.

Acerca de esta tarea

Puede ver información sobre los archivos abiertos en una sesión de SMB establecida. La información que se muestra es útil cuando necesita determinar la información de la sesión SMB para determinados archivos dentro de una sesión SMB.

Por ejemplo, si tiene una sesión SMB en la que algunos de los archivos abiertos están abiertos con protección disponible continuamente y otros no están abiertos con protección disponible continuamente (el valor `-continuously-available` del campo en `vserver cifs session show` la salida del comando es `Partial`), puede determinar qué archivos no están disponibles continuamente mediante este comando.

Puede mostrar información de todos los archivos abiertos en sesiones SMB establecidas en máquinas virtuales de almacenamiento (SVM) de forma resumida, mediante `vserver cifs session file show` el comando sin ningún parámetro opcional.

Sin embargo, en muchos casos, la cantidad de producción devuelta es grande. Puede personalizar la información que se muestra en el resultado especificando parámetros opcionales. Esto puede resultar útil si desea ver información sólo de un pequeño subconjunto de archivos abiertos.

- Puede utilizar el parámetro opcional `-fields` para mostrar la salida en los campos seleccionados.

  Es posible usar este parámetro de forma independiente o combinada con otros parámetros opcionales.

- Puede utilizar el `-instance` parámetro para mostrar información detallada sobre los archivos SMB abiertos.

  Es posible usar este parámetro de forma independiente o combinada con otros parámetros opcionales.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea mostrar archivos SMB abiertos…	Introduzca el siguiente comando…
En la SVM de forma resumida	**vserver cifs session file show -vserver *vserver_name***
En un nodo especificado	`*vserver cifs session file show -vserver *vserver_name* -node {node_name
local}*`	En un ID de archivo especificado
vserver cifs session file show -vserver *vserver_name* -file-id integer	En un ID de conexión de SMB especificado
vserver cifs session file show -vserver *vserver_name* -connection-id integer	En un ID de sesión de SMB especificado
vserver cifs session file show -vserver *vserver_name* -session-id integer	En el agregado de host especificado
vserver cifs session file show -vserver *vserver_name* -hosting -aggregate *aggregate_name*	En el volumen especificado
vserver cifs session file show -vserver *vserver_name* -hosting-volume *volume_name*	En el recurso compartido de SMB especificado
vserver cifs session file show -vserver *vserver_name* -share *share_name*	En la ruta del bloque de mensajes del servidor especificada

Si desea mostrar archivos SMB abiertos…	Introduzca el siguiente comando…
vserver cifs session file show -vserver *vserver_name* -path *path*	Con el nivel especificado de protección continua disponible
vserver cifs session file show -vserver *vserver_name* -continuously -available *continuously_available_status* El valor de `-continuously-available` puede ser uno de los siguientes: • `No` • `Yes` Si el estado de disponibilidad continua es `No`, esto significa que estos archivos abiertos no pueden recuperarse sin interrupciones de la toma de control y la devolución. Tampoco pueden recuperarse de la reubicación general de agregados entre partners en una relación de alta disponibilidad.	Con el estado reconectado especificado

Existen parámetros opcionales adicionales que se pueden utilizar para refinar los resultados de la salida. Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

Ejemplos

En el siguiente ejemplo, se muestra información sobre los archivos abiertos en la SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

En el siguiente ejemplo, se muestra información detallada sobre los archivos SMB abiertos con el ID de archivo 82 en la SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.