Configuración de SMB para Microsoft Hyper-V y SQL Server

ONTAP 9

NetApp
April 20, 2024

This PDF was generated from https://docs.netapp.com/es-es/ontap/smb-hyper-v-sql/index.html on April 20, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Configuración de SMB para Microsoft Hyper-V y SQL Server . . . 1
Información general de la configuración de SMB para Microsoft Hyper-V y SQL Server . . . 1
Configurar ONTAP para soluciones Microsoft Hyper-V y SQL Server sobre SMB . . . 1
Operaciones no disruptivas para Hyper-V y SQL Server sobre SMB . . . 2
Backups basados en recursos compartidos con VSS remoto . . . 7
Cómo se utiliza la descarga de copias ODX con Hyper-V y SQL Server en recursos compartidos SMB . . . 11
Requisitos y consideraciones de configuración . . . 12
Recomendaciones para configuraciones de SQL Server y Hyper-V mediante SMB . . . 21
Planifique la configuración de Hyper-V o SQL Server con SMB . . . 21
Cree configuraciones de ONTAP para proporcionar operaciones no disruptivas con Hyper-V y SQL Server sobre SMB . . . 25
Gestione Hyper-V y SQL Server con las configuraciones de SMB . . . 39
Utilice estadísticas para supervisar la actividad de Hyper-V y SQL Server mediante SMB . . . 44
Compruebe que la configuración admite operaciones no disruptivas . . . 47

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 de ONTAP e interacción con servicios externos, consulte estos informes técnicos (TR): **"Informe técnico de NetApp 4172: Prácticas recomendadas de Microsoft Hyper-V mediante SMB 3.0 con ONTAP"** "Informe técnico de NetApp 4369: Prácticas recomendadas para Microsoft SQL Server y SnapManager 7.2 para SQL Server con Clustered Data 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 los servicios de backup rápidos basados en copias de Snapshot, diseñados para integrarse con configuraciones de Hyper-V mediante SMB.

  Para obtener información acerca del uso de SnapManager con configuraciones de Hyper-V mediante SMB, consulte *SnapManager para Hyper-V Guía de instalación y administración*.

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 copias de Snapshot, diseñados para integrarse con configuraciones de SQL Server en SMB.

  Para obtener información sobre cómo utilizar el plugin de SnapCenter para Microsoft SQL Server, consulte "Plugin de SnapCenter para Microsoft SQL Server" documentar.

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 Share y un tipo de manejador de archivo conocido como *persistent handle* que permite a los clientes SMB reclamar el estado de apertura de archivo y restablecer de forma transparente las conexiones SMB.

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.

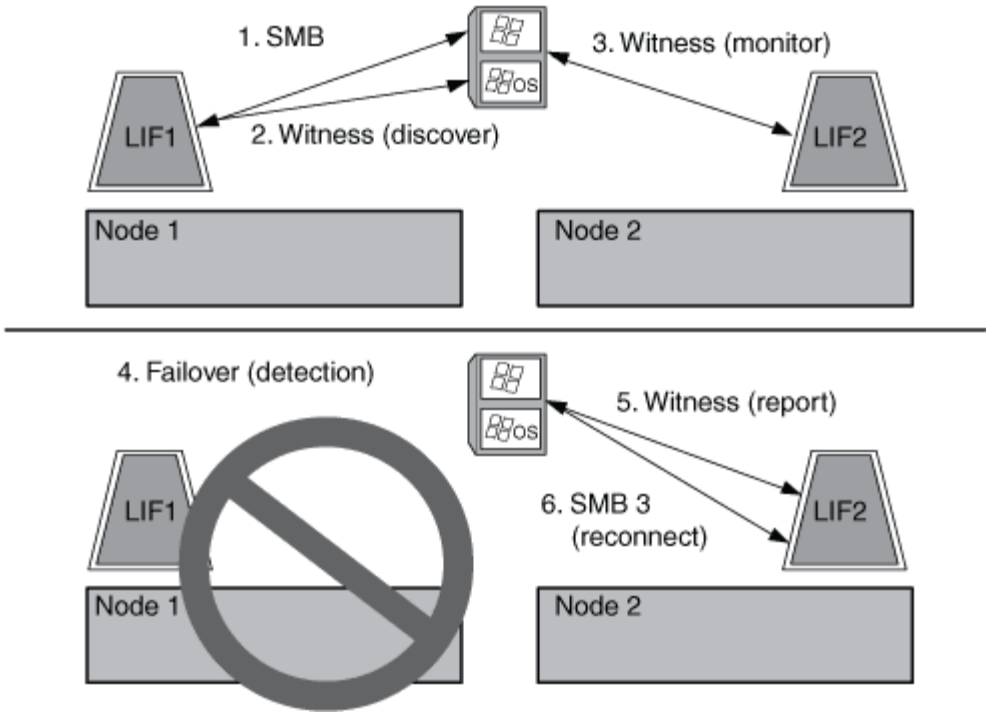
- Los servidores de aplicación deben conectarse al servidor CIFS mediante el nombre del servidor CIFS que se almacena en DNS en lugar de utilizar direcciones IP de LIF individuales.

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 utiliza VSS remoto con recuperación automática para realizar backups de archivos de Hyper-V en 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.

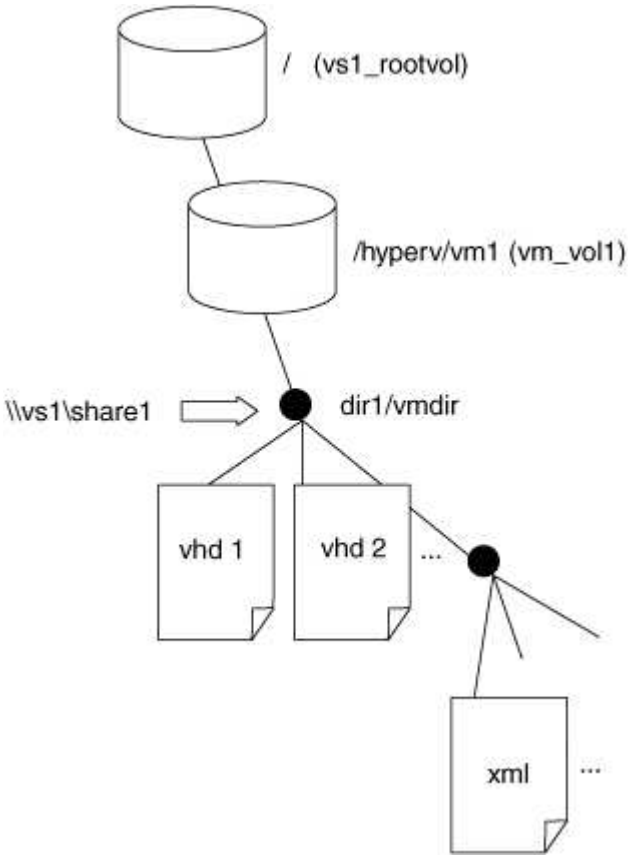
Una estructura de directorio compatible para la creación correcta de instantáneas cumple los siguientes requisitos:

- 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` En la máquina virtual de almacenamiento (SVM) vs1. Se crean subdirectorios para contener los archivos de la máquina virtual en el punto de unión. A los archivos de la máquina virtual del servidor de Hyper-V se accede a lo largo de compartia1 que tiene la ruta de acceso `/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:

- La integración de SnapDrive con ONTAP ofrece optimización del rendimiento al detectar la ubicación de los recursos compartidos de SMB.

  ONTAP proporciona a SnapDrive el nombre del volumen en el que reside el recurso compartido.

- 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 copias de Snapshot para SnapManager para Hyper-V y así poder utilizarlas para las restauraciones.

  No hay ninguna fase de backup. El backup es la copia Snapshot con una 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. Al usar SnapManager para Hyper-V para realizar un backup, los archivos de una copia snapshot se convierten en el backup. Por lo tanto, en la fase de backup se crea una copia snapshot para cada volumen que contenga recursos compartidos en el conjunto de backup. 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 la 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 de FlexClone se incluye en "ONTAP One". Si no tiene ONTAP One, debe hacerlo "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 debe configurar los servidores de aplicaciones para realizar conexiones mediante las 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 de 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 de SMB con el `continuously-availability` propiedad compartida establecida.

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. Compartido `.VHDX` No se admiten archivos para Hyper-V sobre 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 establecer la opción que determina la reserva de espacio de la copia Snapshot `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 Snapshot para la SVM no está deshabilitada y se configura para crear copias de Snapshot, debe especificar una política de Snapshot en el nivel de volumen y esa política debe deshabilitarse. Los backups habilitados para el servicio de copia de sombra y los backups de SQL Server gestionan la creación y eliminación de copias de Snapshot.

- 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 rutas siguientes: `/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	

Tipos de información	Valores
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 de `-symlink-properties` el 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, en el espacio de nombres que se muestra, si desea almacenar archivos de máquina virtual o archivos de base de datos en los volúmenes «'vol1'», «'vol2'», «'vol3'» y «'vol4'», deberá crear recursos compartidos para los servidores de aplicaciones en las rutas siguientes: `/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 la `/data1` y.. `/data2` rutas de acceso para la administración administrativa, no debe configurar 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 y ruta del recurso compartido del SMB	
Volume 2: Nombre compartido SMB y ruta	
Volume 3: Nombre compartido SMB y ruta	
Volume 4: Nombre compartido SMB y ruta	

Tipos de información	Valores
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 el `-is-exportpolicy-enabled` La opción del servidor CIFS se establece 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

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 se crea una máquina virtual de almacenamiento (SVM), ONTAP crea automáticamente el usuario predeterminado llamado "'pcuser'" (con un UID de `65534`) Y el grupo denominado «'pcuser'» (con una GID de `65534`), y agrega el usuario predeterminado al grupo «'pcuser'». 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 predeterminada no está establecida y no hay ningún usuario UNIX que pueda designarse como usuario UNIX predeterminado, cree el usuario UNIX predeterminado y el grupo predeterminado y agregue el usuario predeterminado al grupo.

   Por lo general, al usuario predeterminado se le asigna el nombre de usuario «'pcuser'» y debe asignarse el UID de `65534`. Por lo general, al grupo por defecto se le da el nombre de grupo «'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

4. 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*

5. Para comprobar 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 de usuario de Windows a UNIX mediante el `vserver cifs session show` comando.

   Para obtener más información acerca de cómo utilizar este comando, consulte las páginas man.

Ejemplo

Los siguientes comandos determinan que el usuario predeterminado del servidor CIFS no está establecido, pero determinan que existen el usuario «'pcaduser'» y el grupo «'pcaduser'». Al usuario «'pcuser'» se le asigna como usuario predeterminado del servidor CIFS en la 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 el `volume modify` 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 deben configurarse en `true`:

      - `-smb2-enabled`
      - `-smb3-enabled`
      - `-copy-offload-enabled`
      - `-shadowcopy-enabled` (Solo Hyper-V)
2. Si alguna de las opciones no se ha establecido en `true`, lleve a cabo lo siguiente:
   a. Configúrelas como `true` mediante el uso de `vserver cifs options modify` comando.
   b. Compruebe que las opciones están definidas en `true` mediante el uso de `vserver cifs options show` 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.

Lo que necesitará

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 options 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 acerca de cómo personalizar volúmenes, consulte xref:./smb-hyper-v-sql/"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 de recurso compartido de archivos sin conexión está configurada en el recurso compartido y se establece en `manual`.
   - ONTAP crea el recurso compartido con el permiso de recurso compartido predeterminado de Windows `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 el `vserver cifs share show` 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 enlaces simbólicos se desactivan mediante la configuración de `-symlink` parámetro a. `""`:

```
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.

Lo que necesitará

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 de `-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.

Lo que necesitará

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 se establece en `0`, ONTAP crea instantáneas 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` la propiedad share se establece 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:

- La `-offline-files` el parámetro está establecido en cualquiera de los dos `manual` (el valor predeterminado) 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 del recurso compartido para desactivar los enlaces simbólicos y establezca los archivos offline en manual mediante el `vserver cifs share properties modify` comando.

   Puede deshabilitar los enlaces simbólicos estableciendo el valor de `-symlink` parámetro a. `""`.

   - Puede deshabilitar los enlaces simbólicos estableciendo el valor de `-symlink` parámetro a. `""`.
   - Puede ajustar la `-offline-files` especifique el parámetro en el ajuste correcto `manual`.

3. Añada el `continuously-available` compartir la propiedad y, si es necesario, la `oplocks` compartir propiedad:

   vserver cifs share properties add -vserver *vserver_name* -share-name *share_name* -share-properties continuously-available[,oplock]

   Si la `oplocks` la propiedad share no está establecida, debe añadirla junto con la `continuously-available` compartir propiedad.

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 el `-symlink` y.. `-offline-files` los parámetros se ajustan 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 shares properties show -vserver *vserver_name* -share-name share_name

Ejemplos

El siguiente ejemplo muestra cómo configurar un recurso compartido existente llamado «shara1» en la máquina virtual de almacenamiento (SVM) vs1 para NDOS con un servidor de aplicaciones en SMB:

- Los enlaces simbólicos se desactivan en el recurso compartido estableciendo la `-symlink` parámetro a `""`.

- La `-offline-file` el parámetro se modifica y se establece en `manual`.
- La `continuously-available` la propiedad share se agrega al recurso compartido.
- La `oplocks` la propiedad share ya está en la lista de propiedades de recurso compartido; por lo tanto, no es necesario añadirla.
- La `attributecache` la propiedad share se quita del recurso compartido.
- La `browsable` La propiedad Share es opcional para un recurso compartido disponible continuamente que se utiliza para NDOS con servidores de aplicaciones en SMB y se conserva como una de las propiedades compartidas.

```
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 de estadísticas y contadores están disponibles

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`***

   Consulte las páginas de manual para obtener más información acerca de los objetos y contadores disponibles.

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 contadores de `cifs` objeto como se ve en el nivel de privilegio avanzado:

> En este ejemplo no se muestran todos los contadores disponibles para el `cifs` objeto; la salida se truncará.

```
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


[...]
```

Mostrar estadísticas de SMB

Puede mostrar varias estadísticas de SMB para supervisar el rendimiento y diagnosticar

problemas.

Pasos

1. Utilice la `statistics start` y opcional `statistics stop` comandos para recoger 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`**

Obtenga más información sobre la `statistics` comandos:

- "se muestran las estadísticas"
- "inicio de las estadísticas"
- "se detienen las estadísticas"

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 utilizar el `system health` Comandos para mostrar información sobre el estado general del sistema del clúster y el estado del subsistema CIFS-NDO, para responder a las alertas, configurar alertas futuras y mostrar información sobre cómo se configura 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`**
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 la `-instance` 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:

- La `-offline-files` el parámetro está establecido en cualquiera de los dos `manual` (el valor predeterminado) 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 sin conexión están establecidos 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 sin conexión se establecen en `manual` y los enlaces simbólicos están desactivados (designados por un guión en el `Symlink Properties` salida de 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
```

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, «'lia1'» debería ser trasladado de vuelta a su puerto de origen, `node1:e0d`.

3. Si alguna de las interfaces de red del puerto de inicio a las que se deberían asociar las LIF no está en la `up` state, resuelva el problema para que estas interfaces estén en funcionamiento.
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

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 usar el opcional `-fields` parámetro para mostrar el resultado de los campos seleccionados.

  Puede entrar `-fields ?` para determinar qué campos se pueden utilizar.

- Puede utilizar el `-instance` Parámetro para mostrar información detallada sobre las sesiones SMB establecidas.
- Puede utilizar el `-fields` o el `-instance` parámetro independiente 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` Valor para `-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` Valor para `-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`* Valor para `-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
```

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

al menos un archivo abierto continuam a no están abiertos con protección continua disponible.

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 acerca de los archivos SMB 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. 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 archivos abiertos están abiertos con protección continua disponible y algunos no están abiertos con protección continua disponible (el valor de la `-continuously-available` campo en `vserver cifs session show` el resultado 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 la `vserver cifs session file show` 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 usar el opcional `-fields` parámetro para mostrar la salida en los campos que elija.

  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` Valor para `-continuously-available` puede ser uno de los siguientes: • `No` • `Yes` Si el estado continuamente disponible es `No`, esto significa que estos archivos abiertos no son capaces de recuperarse de forma no disruptiva 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. Consulte la página del manual para obtener más información.

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

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

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

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

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

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

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

Información de la marca comercial

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