Ponga en marcha servicios basados en cliente de SMB

ONTAP 9

NetApp
April 16, 2024

This PDF was generated from https://docs.netapp.com/es-es/ontap/smb-admin/offline-files-allow-caching-concept.html on April 16, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Ponga en marcha servicios basados en cliente de SMB . . . 1
Utilice archivos sin conexión para permitir el almacenamiento en caché de archivos para su uso sin conexión . . . 1
Use perfiles de itinerancia para almacenar perfiles de usuario de forma centralizada en un servidor SMB asociado con la SVM . . . 7
Utilice la redirección de carpetas para almacenar datos en un servidor SMB . . . 9
Acceda al directorio ~snapshot desde clientes de Windows mediante SMB 2.x. . . . 10
Recupere archivos y carpetas con versiones anteriores . . . 11

Ponga en marcha servicios basados en cliente de SMB

Utilice archivos sin conexión para permitir el almacenamiento en caché de archivos para su uso sin conexión

Utilizar archivos sin conexión para permitir el almacenamiento en caché de archivos para uso general sin conexión

ONTAP es compatible con la característica Archivos sin conexión de Microsoft, o con la función de almacenamiento en caché del cliente_, que permite almacenar los archivos en caché en el host local para su uso sin conexión. Los usuarios pueden utilizar la funcionalidad de archivos sin conexión para seguir trabajando en archivos incluso cuando están desconectados de la red.

Puede especificar si los documentos y programas de usuario de Windows se almacenan automáticamente en caché en un recurso compartido o si los archivos deben seleccionarse manualmente para almacenar en caché. El almacenamiento en caché manual está habilitado de forma predeterminada para nuevos recursos compartidos. Los archivos que están disponibles sin conexión se sincronizan con el disco local del cliente de Windows. La sincronización se produce cuando se restaura la conectividad de red a un recurso compartido de sistema de almacenamiento específico.

Puesto que los archivos y carpetas sin conexión conservan los mismos permisos de acceso que la versión de los archivos y carpetas guardados en el servidor CIFS, el usuario debe tener suficientes permisos en los archivos y carpetas guardados en el servidor CIFS para realizar acciones en los archivos y carpetas sin conexión.

Cuando el usuario y otra persona de la red realizan cambios en el mismo archivo, el usuario puede guardar la versión local del archivo en la red, conservar la otra versión o guardar ambas. Si el usuario conserva ambas versiones, se guarda localmente un nuevo archivo con los cambios del usuario local y el archivo almacenado en caché se sobrescribe con cambios de la versión del archivo guardado en el servidor CIFS.

Puede configurar archivos sin conexión de forma compartida mediante las opciones de configuración de recursos compartidos. Puede elegir una de las cuatro configuraciones de carpetas sin conexión al crear o modificar recursos compartidos:

- Sin almacenamiento en caché

  Deshabilita el almacenamiento en caché en el cliente para el recurso compartido. Los archivos y carpetas no se almacenan automáticamente en caché local en clientes y los usuarios no pueden optar por almacenar en caché archivos o carpetas localmente.

- Almacenamiento en caché manual

  Permite la selección manual de archivos para almacenar en caché en el recurso compartido. Esta es la configuración predeterminada. De forma predeterminada, no se almacenan en caché archivos ni carpetas en el cliente local. Los usuarios pueden elegir los archivos y carpetas que desean almacenar en caché localmente para utilizarlos sin conexión.

- Almacenamiento automático de documentos en caché

  Permite que los documentos de usuario se almacenen automáticamente en caché en el recurso compartido. Sólo los archivos y carpetas a los que se tiene acceso se almacenan en caché localmente.

- Almacenamiento automático de programas en caché

  Permite que los programas y los documentos de usuario se almacenen automáticamente en caché en el recurso compartido. Sólo los archivos, carpetas y programas a los que se tiene acceso se almacenan en caché localmente. Además, esta configuración permite al cliente ejecutar ejecutables almacenados localmente en caché incluso cuando se conecta a la red.

Para obtener más información acerca de la configuración de archivos sin conexión en servidores y clientes de Windows, consulte la biblioteca de Microsoft TechNet.

Información relacionada

Uso de perfiles de itinerancia para almacenar perfiles de usuario de forma centralizada en un servidor CIFS asociado con la SVM

Uso de la redirección de carpetas para almacenar datos en un servidor CIFS

Uso de BranchCache para almacenar en caché contenido compartido de SMB en una sucursal

"Biblioteca de Microsoft TechNet: technet.microsoft.com/en-us/library/"

Requisitos para utilizar archivos sin conexión

Antes de poder utilizar la función Microsoft Offline Files con el servidor CIFS, debe conocer las versiones de ONTAP y SMB y los clientes Windows que admiten la función.

Requisitos de la versión de ONTAP

Las versiones ONTAP admiten archivos sin conexión.

Requisitos de la versión del protocolo SMB

Para las máquinas virtuales de almacenamiento (SVM), ONTAP admite archivos sin conexión en todas las versiones de SMB.

Requisitos del cliente Windows

El cliente Windows debe admitir los archivos sin conexión.

Para obtener la información más reciente sobre los clientes de Windows que admiten la función Archivos sin conexión, consulte la matriz de interoperabilidad.

"mysupport.netapp.com/matrix"

Directrices para implementar archivos sin conexión

Hay algunas directrices importantes que debe entender al implementar archivos sin conexión en los recursos compartidos de directorios iniciales que tienen `showsnapshot` propiedad share establecida en directorios iniciales.

Si la `showsnapshot` La propiedad Share se establece en un recurso compartido de directorio principal que tiene configurados archivos sin conexión, los clientes de Windows almacenan en caché todas las copias Snapshot en la `~snapshot` en el directorio principal del usuario.

Los clientes de Windows almacenan en caché todas las copias Snapshot en el directorio inicial si se cumple alguna de las siguientes condiciones:

- El usuario hace que el directorio inicial esté disponible sin conexión desde el cliente.

  El contenido del `~snapshot` la carpeta del directorio principal se incluye y se hace disponible sin conexión.

- El usuario configura la redirección de carpetas para redirigir una carpeta como, por ejemplo `My Documents` En la raíz de un directorio inicial que reside en el recurso compartido de servidor CIFS.

  Es posible que algunos clientes de Windows hagan que la carpeta redirigida esté disponible sin conexión automáticamente. Si la carpeta se redirige a la raíz del directorio principal, el `~snapshot` la carpeta se incluye en el contenido sin conexión almacenado en caché.

> Los archivos sin conexión se despliegues donde `~snapshot` la carpeta se incluye en los archivos sin conexión se debe evitar. Las copias Snapshot en la `~snapshot` La carpeta contiene todos los datos del volumen en el punto en que ONTAP creó la copia Snapshot. Por tanto, cree una copia sin conexión de `~snapshot` la carpeta consume una cantidad significativa de almacenamiento local en el cliente, consume ancho de banda de red durante la sincronización de archivos sin conexión y aumenta el tiempo necesario para sincronizar archivos sin conexión.

Configure la compatibilidad de archivos sin conexión en recursos compartidos SMB mediante la CLI

Puede configurar la compatibilidad de archivos sin conexión mediante la interfaz de línea de comandos de ONTAP especificando una de las cuatro archivos sin conexión al crear recursos compartidos de SMB o en cualquier momento modificando los recursos compartidos de SMB existentes. La compatibilidad con archivos manuales sin conexión es la configuración predeterminada.

Acerca de esta tarea

Al configurar el soporte de archivos sin conexión, puede elegir una de las siguientes cuatro opciones de archivos sin conexión:

Ajuste	Descripción
`none`	Despermite a los clientes de Windows almacenar en caché cualquier archivo en este recurso compartido.
`manual`	Permite a los usuarios de clientes de Windows seleccionar manualmente los archivos que se van a almacenar en caché.

Ajuste	Descripción
`documents`	Permite a los clientes de Windows almacenar en caché los documentos de usuario utilizados por el usuario para el acceso sin conexión.
`programs`	Permite a los clientes de Windows almacenar en caché programas que utilizan el usuario para el acceso sin conexión. Los clientes pueden utilizar los archivos de programa almacenados en caché en modo sin conexión incluso si el recurso compartido está disponible.

Sólo puede seleccionar una configuración de archivo sin conexión. Si modifica una configuración de archivos sin conexión en un recurso compartido SMB existente, la opción nuevos archivos sin conexión reemplaza la configuración original. Las demás opciones de configuración y propiedades de uso compartido de SMB existentes no se eliminan ni se reemplazan. Permanecen vigentes hasta que se eliminan o cambian explícitamente.

Pasos

1. Ejecute la acción adecuada:

Si desea configurar archivos sin conexión en…	Introduzca el comando…
Un nuevo recurso compartido de SMB	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none
manual	documents
programs}`	Un recurso compartido de SMB existente
`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none	manual
documents	programs}`

2. Compruebe que la configuración de recursos compartidos de SMB es correcta: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Ejemplo

El siguiente comando crea un recurso compartido SMB denominado «data1» con archivos sin conexión establecidos en `documents`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                 Share Properties: oplocks
                                   browsable
                                   changenotify
               Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                    Share Comment: Offline files
                        Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                      Volume Name: -
                    Offline Files: documents
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

El siguiente comando modifica un recurso compartido SMB existente llamado «data1» cambiando la configuración de archivos sin conexión a. `manual` y agregando valores para la máscara de creación de modo de archivo y directorio:

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                 Share Properties: oplocks
                                   browsable
                                   changenotify
               Symlink Properties: enable
          File Mode Creation Mask: 644
     Directory Mode Creation Mask: 777
                    Share Comment: Offline files
                        Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                      Volume Name: -
                    Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Información relacionada

Agregar o quitar propiedades de recursos compartidos en un recurso compartido SMB existente

Configure el soporte de archivos sin conexión en recursos compartidos SMB mediante la MMC de Administración de equipos

Si desea permitir a los usuarios almacenar en caché archivos localmente para su uso sin conexión, puede configurar la compatibilidad con archivos sin conexión mediante la MMC de Administración de equipos (Microsoft Management Console).

Pasos

1. Para abrir el MMC en el servidor de Windows, en el Explorador de Windows, haga clic con el botón secundario del mouse (ratón) en el icono del equipo local y, a continuación, seleccione **Administrar**.
2. En el panel izquierdo, seleccione **Administración de equipos**.
3. Seleccione **Acción** > **conectar a otro ordenador**.

   Aparece el cuadro de diálogo Seleccionar equipo.

4. Escriba el nombre del servidor CIFS o haga clic en **examinar** para buscar el servidor CIFS.

   Si el nombre del servidor CIFS es el mismo que el nombre de host de máquina virtual de almacenamiento

(SVM), escriba el nombre de SVM. Si el nombre del servidor CIFS es diferente del nombre de host de la SVM, escriba el nombre del servidor CIFS.

5. Haga clic en **Aceptar**.
6. En el árbol de la consola, haga clic en **Herramientas del sistema** > **carpetas compartidas**.
7. Haga clic en **comparticiones**.
8. En el panel de resultados, haga clic con el botón derecho en el recurso compartido.
9. Haga clic en **Propiedades**.

   Se mostrarán las propiedades del recurso compartido seleccionado.

10. En la ficha **General**, haga clic en **Configuración sin conexión**.

    Se muestra el cuadro de diálogo Configuración sin conexión.

11. Configure las opciones de disponibilidad sin conexión según corresponda.
12. Haga clic en **Aceptar**.

Use perfiles de itinerancia para almacenar perfiles de usuario de forma centralizada en un servidor SMB asociado con la SVM

Use perfiles de itinerancia para almacenar perfiles de usuario de forma centralizada en un servidor SMB asociado a la información general de SVM

ONTAP admite el almacenamiento de perfiles de itinerancia de Windows en un servidor CIFS asociado con la máquina virtual de almacenamiento (SVM). La configuración de perfiles de itinerancia de usuario ofrece ventajas al usuario, como la disponibilidad automática de recursos, independientemente de dónde inicie sesión el usuario. Los perfiles móviles también simplifican la administración y gestión de los perfiles de usuario.

Los perfiles de usuario móviles tienen las siguientes ventajas:

- Disponibilidad de recursos automática

  El perfil único de un usuario está automáticamente disponible cuando ese usuario inicia sesión en cualquier equipo de la red que ejecuta Windows 8, Windows 7, Windows 2000 o Windows XP. Los usuarios no necesitan crear un perfil en cada equipo que utilizan en una red.

- Sustitución simplificada del ordenador

  Dado que toda la información del perfil del usuario se mantiene por separado en la red, el perfil de un usuario se puede descargar fácilmente en un equipo nuevo y de repuesto. Cuando el usuario inicia sesión en el nuevo equipo por primera vez, la copia del servidor del perfil del usuario se copia en el nuevo equipo.

Información relacionada

Uso de archivos sin conexión para permitir el almacenamiento en caché de archivos para su uso sin conexión

Uso de la redirección de carpetas para almacenar datos en un servidor CIFS

Requisitos para utilizar perfiles de itinerancia

Antes de poder utilizar los perfiles de itinerancia de Microsoft en su servidor CIFS, necesita saber qué versiones de ONTAP y SMB y qué clientes de Windows admiten esta función.

Requisitos de la versión de ONTAP

ONTAP admite perfiles de itinerancia.

Requisitos de la versión del protocolo SMB

En el caso de máquinas virtuales de almacenamiento (SVM), ONTAP admite perfiles de itinerancia en todas las versiones de SMB.

Requisitos del cliente Windows

Para que un usuario pueda utilizar los perfiles de itinerancia, el cliente de Windows debe admitir la función.

Para obtener la información más reciente acerca de los clientes de Windows que admiten perfiles de itinerancia, consulte matriz de interoperabilidad.

"Herramienta de matriz de interoperabilidad de NetApp"

Configurar perfiles móviles

Si desea que el perfil de un usuario esté disponible automáticamente cuando ese usuario inicie sesión en cualquier equipo de la red, puede configurar perfiles de itinerancia mediante el complemento MMC usuarios y equipos de Active Directory. Si está configurando perfiles de itinerancia en Windows Server, puede utilizar el Centro de administración de Active Directory.

Pasos

1. En el servidor Windows, abra el MMC de Usuarios y equipos de Active Directory (o el Centro de administración de Active Directory en servidores Windows).
2. Busque el usuario para el que desea configurar un perfil de itinerancia.
3. Haga clic con el botón derecho del ratón en el usuario y haga clic en **Propiedades**.
4. En la ficha **Perfil**, introduzca la ruta del perfil en el recurso compartido en el que desea almacenar el perfil de itinerancia del usuario, seguido de `%username%`.

   Por ejemplo, una ruta de acceso de perfil puede ser la siguiente: `\\vs1.example.com\profiles\%username%`. La primera vez que un usuario inicia sesión, `%username%` se sustituye por el nombre del usuario.

   > En la ruta `\\vs1.example.com\profiles\%username%`, `profiles` Es el nombre compartido de un recurso compartido de una máquina virtual de almacenamiento (SVM) vs1 con derechos de control total para todos.

5. Haga clic en **Aceptar**.

Utilice la redirección de carpetas para almacenar datos en un servidor SMB

Utilice la redirección de carpetas para almacenar los datos en una introducción al servidor SMB

ONTAP admite la redirección de carpetas de Microsoft, lo que permite que los usuarios o administradores redirijan la ruta de una carpeta local a una ubicación en el servidor CIFS. Parece que si las carpetas redirigidas se almacenan en el cliente local de Windows, aunque los datos se almacenen en un recurso compartido de SMB.

La redirección de carpetas está destinada principalmente a las empresas que ya han implementado directorios iniciales y que desean mantener la compatibilidad con su entorno de directorio raíz existente.

- `Documents`, `Desktop`, y. `Start Menu` son ejemplos de carpetas que puede redirigir.
- Los usuarios pueden redirigir carpetas desde su cliente Windows.
- Los administradores pueden configurar y administrar centralmente la redirección de carpetas configurando GPO en Active Directory.
- Si los administradores han configurado perfiles de itinerancia, la redirección de carpetas permite a los administradores dividir los datos de usuario de los datos de perfil.
- Los administradores pueden usar la redirección de carpetas y los archivos sin conexión juntos para redirigir el almacenamiento de datos de carpetas locales al servidor CIFS, permitiendo a los usuarios almacenar el contenido en la memoria caché localmente.

Información relacionada

Uso de archivos sin conexión para permitir el almacenamiento en caché de archivos para su uso sin conexión

Uso de perfiles de itinerancia para almacenar perfiles de usuario de forma centralizada en un servidor CIFS asociado con la SVM

Requisitos para utilizar la redirección de carpetas

Para poder utilizar la redirección de carpetas de Microsoft con el servidor CIFS, debe conocer las versiones de ONTAP y SMB y los clientes de Windows que admiten la función.

Requisitos de la versión de ONTAP

ONTAP admite redirección de carpetas de Microsoft.

Requisitos de la versión del protocolo SMB

Para la máquina virtual de almacenamiento (SVM), ONTAP admite el redireccionamiento de carpetas de Microsoft en todas las versiones de SMB.

Requisitos del cliente Windows

Para que un usuario pueda utilizar la redirección de carpetas de Microsoft, el cliente de Windows debe admitir la función.

Para obtener la información más reciente acerca de los clientes de Windows que admiten la redirección de carpetas, consulte la matriz de interoperabilidad.

"mysupport.netapp.com/matrix"

Configurar la redirección de carpetas

Puede configurar la redirección de carpetas mediante la ventana Propiedades de Windows. La ventaja de utilizar este método es que el usuario de Windows puede configurar la redirección de carpetas sin la ayuda del administrador de SVM.

Pasos

1. En el Explorador de Windows, haga clic con el botón secundario en la carpeta que desea redirigir a un recurso compartido de red.
2. Haga clic en **Propiedades**.

   Se mostrarán las propiedades del recurso compartido seleccionado.

3. En la ficha **acceso directo**, haga clic en **destino** y especifique la ruta de acceso a la ubicación de red en la que desea redirigir la carpeta seleccionada.

   Por ejemplo, si desea redirigir una carpeta al `data` carpeta de un directorio principal al que está asignado `Q:\`, especifique `Q:\data` como destino.

4. Haga clic en **Aceptar**.

   Para obtener más información acerca de la configuración de carpetas sin conexión, consulte la Biblioteca de Microsoft TechNet.

Información relacionada

"Biblioteca de Microsoft TechNet: technet.microsoft.com/en-us/library/"

Acceda al directorio ~snapshot desde clientes de Windows mediante SMB 2.x.

El método que utiliza para acceder a `~snapshot` el directorio de clientes de Windows que utilizan SMB 2.x difiere del método utilizado para SMB 1.0. Debe comprender cómo acceder al `~snapshot` directorio al utilizar las conexiones SMB 2.x para acceder correctamente a los datos almacenados en copias Snapshot.

El administrador de SVM controla si los usuarios de clientes de Windows pueden ver y acceder a `~snapshot` active o desactive el directorio en un recurso compartido `showsnapshot` comparta la propiedad mediante comandos de las familias de propiedades compartidas cifs del vserver.

Cuando la `showsnapshot` La propiedad Share está deshabilitada, un usuario de un cliente Windows que utilice SMB 2.x no puede ver la `~snapshot` Y no puede acceder a las copias Snapshot dentro de la `~snapshot` directorio, incluso cuando se introduce manualmente la ruta de acceso al `~snapshot` directorio o a copias Snapshot específicas dentro del directorio.

Cuando la `showsnapshot` La propiedad Share está habilitada; un usuario de un cliente Windows que utilice

SMB 2.x todavía no puede ver la `~snapshot` directorio en la raíz del recurso compartido o dentro de cualquier unión o directorio debajo de la raíz del recurso compartido. Sin embargo, después de conectarse a un recurso compartido, el usuario puede acceder al oculto `~snapshot` directorio anexando manualmente `\~snapshot` al final de la ruta de uso compartido. El oculto `~snapshot` se puede acceder al directorio desde dos puntos de entrada:

- En la raíz del recurso compartido
- En cada punto de unión del espacio compartido

El oculto `~snapshot` no se puede acceder al directorio desde los subdirectorios que no son de unión dentro del recurso compartido.

Ejemplo

Con la configuración que se muestra en el ejemplo siguiente, un usuario de un cliente Windows con una conexión SMB 2.x al recurso compartido «'eng'» puede acceder al `~snapshot` directorio anexando manualmente `\~snapshot` a la ruta de uso compartido en la raíz del recurso compartido y en cada punto de unión del camino. El oculto `~snapshot` se puede acceder al directorio desde las tres rutas siguientes:

- `\\vs1\eng\~snapshot`
- `\\vs1\eng\projects1\~snapshot`
- `\\vs1\eng\projects2\~snapshot`

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume       junction-path
------- ------------ ----------------------------------------
vs1     vs1_root      /
vs1     vs1_vol1      /eng
vs1     vs1_vol2      /eng/projects1
vs1     vs1_vol3      /eng/projects2

cluster1::> vserver cifs share show
Vserver  Share   Path     Properties    Comment  ACL
-------- ------  -------  ----------    -------- ----------
vs1      eng     /eng     oplocks       -        Everyone / Full Control
                          changenotify
                          browsable
                          showsnapshot
```

Recupere archivos y carpetas con versiones anteriores

Recupere archivos y carpetas usando la información general de versiones anteriores

La capacidad de usar las versiones anteriores de Microsoft es aplicable a los sistemas de archivos que admiten copias snapshot de algún modo y que las tengan habilitadas. La tecnología Snapshot forma parte de ONTAP. Los usuarios pueden recuperar archivos y

carpetas de copias Snapshot de su cliente Windows mediante la función versiones anteriores de Microsoft.

La funcionalidad de versiones anteriores ofrece un método para que los usuarios navegen por las copias Snapshot o para restaurar datos de una copia Snapshot sin la intervención de un administrador de almacenamiento. Las versiones anteriores no se pueden configurar. Está siempre habilitada. Si el administrador de almacenamiento ha creado copias Snapshot en un recurso compartido, el usuario puede usar versiones anteriores para realizar las siguientes tareas:

- Recuperar archivos eliminados accidentalmente.
- Recuperación de la sobrescritura accidental de un archivo.
- Compare las versiones del archivo mientras está trabajando.

Los datos almacenados en las copias Snapshot son de solo lectura. Los usuarios deben guardar una copia de un archivo en otra ubicación para realizar cualquier cambio en el archivo. Las copias Snapshot se eliminan periódicamente y, por lo tanto, los usuarios deben crear copias de los archivos contenidos en las versiones anteriores si desean conservar de forma indefinida una versión anterior de un archivo.

Requisitos para usar versiones anteriores de Microsoft

Antes de poder utilizar las versiones anteriores con el servidor CIFS, debe conocer qué versiones de ONTAP y SMB, y qué clientes de Windows, admiten. También necesita saber acerca de los requisitos de configuración de la copia Snapshot.

Requisitos de la versión de ONTAP

Admite versiones anteriores.

Requisitos de la versión del protocolo SMB

Para las máquinas virtuales de almacenamiento (SVM), ONTAP admite las versiones anteriores de todas las versiones de SMB.

Requisitos del cliente Windows

Para que un usuario pueda utilizar versiones anteriores para acceder a los datos de las copias Snapshot, el cliente Windows debe admitir la función.

Para obtener la información más reciente sobre los clientes de Windows compatibles con versiones anteriores, consulte matriz de interoperabilidad.

"Herramienta de matriz de interoperabilidad de NetApp"

Requisitos para la configuración de copias Snapshot

Para usar versiones anteriores y acceder a los datos de las copias Snapshot, se debe asociar una política de Snapshot habilitada al volumen que contiene los datos, los clientes deben poder acceder a los datos de Snapshot y deben existir copias Snapshot.

Utilice la pestaña versiones anteriores para ver y gestionar datos de copias snapshot

Los usuarios de equipos cliente Windows pueden usar la pestaña versiones anteriores de la ventana Propiedades de Windows para restaurar los datos almacenados en copias Snapshot sin necesidad de implicar al administrador de máquinas virtuales de almacenamiento (SVM).

Acerca de esta tarea

Solo puede usar la pestaña versiones anteriores para ver y gestionar los datos de las copias Snapshot de los datos almacenados en la SVM si el administrador ha habilitado copias Snapshot en el volumen que contiene el recurso compartido y si el administrador configura el recurso compartido para mostrar copias Snapshot.

Pasos

1. En el Explorador de Windows, muestre el contenido de la unidad asignada de los datos almacenados en el servidor CIFS.
2. Haga clic con el botón derecho del ratón en el archivo o carpeta de la unidad de red asignada cuyas copias Snapshot desee ver o administrar.
3. Haga clic en **Propiedades**.

   Se muestran las propiedades del archivo o carpeta seleccionado.

4. Haga clic en la ficha **versiones anteriores**.

   En el cuadro versiones de carpeta se muestra una lista de las copias Snapshot disponibles del archivo o carpeta seleccionados. Las copias Snapshot mostradas se identifican mediante el prefijo del nombre de la copia Snapshot y la Marca de hora de creación.

5. En el cuadro **versiones de carpeta:**, haga clic con el botón secundario del mouse (ratón) en la copia del archivo o carpeta que desee administrar.
6. Ejecute la acción adecuada:

Si desea…	Haga lo siguiente…
Vea los datos de esa copia Snapshot	Haga clic en **Abrir**.
Cree una copia de los datos a partir de esa copia Snapshot	Haga clic en **Copiar**.

   Los datos de las copias Snapshot son de solo lectura. Si desea realizar modificaciones en los archivos y carpetas enumerados en la ficha versiones anteriores, debe guardar una copia de los archivos y carpetas que desea modificar en una ubicación editable y realizar modificaciones en las copias.

7. Después de terminar de administrar los datos de instantánea, cierre el cuadro de diálogo **Propiedades** haciendo clic en **Aceptar**.

   Para obtener más información acerca de cómo utilizar la ficha versiones anteriores para ver y administrar datos de instantánea, consulte la biblioteca de Microsoft TechNet.

Información relacionada

"Biblioteca de Microsoft TechNet: technet.microsoft.com/en-us/library/"

Determine si están disponibles copias Snapshot para versiones anteriores

Puede ver copias Snapshot en la pestaña versiones anteriores solo si se aplica una política de Snapshot habilitada al volumen que contiene el recurso compartido, y si la configuración del volumen permite acceder a copias Snapshot. Determinar la disponibilidad de copias Snapshot es útil cuando se ayuda a un usuario con acceso de versiones anteriores.

Pasos

1. Determine si el volumen en el que residen los datos compartidos tiene habilitadas las copias automáticas de Snapshot y si los clientes tienen acceso a los directorios de Snapshot: `volume show -vserver vserver-name -volume volume-name -fields vserver,volume,snapdir-access,snapshot-policy,snapshot-count`

   El resultado muestra qué política de Snapshot está asociada con el volumen, si el acceso al directorio Snapshot de cliente está habilitado y el número de copias Snapshot disponibles.

2. Determine si la política de Snapshot asociada está habilitada: `volume snapshot policy show -policy policy-name`
3. Enumere las copias Snapshot disponibles: `volume snapshot show -volume volume_name`

   Para obtener más información sobre la configuración y gestión de políticas de Snapshot y programaciones de Snapshot, consulte "Protección de datos".

Ejemplo

En el siguiente ejemplo se muestra información sobre las políticas de Snapshot asociadas con el volumen denominado «data1», que contiene los datos compartidos y las copias Snapshot disponibles en «data1».

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-------- ------ -------------- --------------- --------------
vs1      data1  true           default         10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1
                   Number of Is
Policy Name        Schedules Enabled Comment
------------------ --------- ------- ---------------------------------
default                    3 true    Default policy with hourly, daily &
weekly schedules.
    Schedule         Count     Prefix                 SnapMirror Label
    ---------------- -----     ---------------------- -------------------
    hourly               6     hourly                 -
    daily                2     daily                  daily
    weekly               2     weekly                 weekly

cluster1::> volume snapshot show -volume data1
                                                            ---Blocks---
Vserver  Volume  Snapshot                  State        Size Total% Used%
-------- ------- ------------------------- -------- -------- ------ -----
vs1      data1
                 weekly.2012-12-16_0015    valid       408KB     0%    1%
                 daily.2012-12-22_0010     valid       420KB     0%    1%
                 daily.2012-12-23_0010     valid       192KB     0%    0%
                 weekly.2012-12-23_0015    valid       360KB     0%    1%
                 hourly.2012-12-23_1405    valid       196KB     0%    0%
                 hourly.2012-12-23_1505    valid       196KB     0%    0%
                 hourly.2012-12-23_1605    valid       212KB     0%    0%
                 hourly.2012-12-23_1705    valid       136KB     0%    0%
                 hourly.2012-12-23_1805    valid       200KB     0%    0%
                 hourly.2012-12-23_1905    valid       184KB     0%    0%
```

Información relacionada

Crear una configuración de instantánea para permitir el acceso a versiones anteriores

"Protección de datos"

Cree una configuración de instantánea para habilitar el acceso a versiones anteriores

La funcionalidad de versiones anteriores está siempre disponible, siempre y cuando exista acceso de los clientes a las copias Snapshot. Si la configuración de su copia Snapshot no cumple estos requisitos, puede crear una configuración de copia Snapshot

que sí lo haga.

Pasos

1. Si el volumen que contiene el recurso compartido al que desea permitir el acceso a versiones anteriores no tiene una política de Snapshot asociada, asocie una política de Snapshot al volumen y habilite esa política mediante el uso de `volume modify` comando.

   Para obtener más información acerca del uso de `volume modify` consulte las páginas de manual.

2. Habilite el acceso a las copias de Snapshot mediante el `volume modify` para establecer el `-snap-dir` opción a. `true`.

   Para obtener más información acerca del uso de `volume modify` consulte las páginas de manual.

3. Compruebe que se han habilitado las políticas de Snapshot y que el acceso a los directorios de Snapshot se habilita mediante el `volume show` y.. `volume snapshot policy show` comandos.

   Para obtener más información acerca del uso de `volume show` y.. `volume snapshot policy show` consulte las páginas de manual.

   Para obtener más información sobre la configuración y gestión de políticas de Snapshot y programaciones de Snapshot, consulte "Protección de datos".

Información relacionada

"Protección de datos"

Directrices para restaurar directorios que contienen uniones

Hay ciertas directrices que debe tener en cuenta al utilizar versiones anteriores para restaurar carpetas que contienen puntos de unión.

Cuando se usan versiones anteriores para restaurar carpetas que tienen carpetas secundarias que son puntos de unión, la restauración puede fallar con un `Access Denied` error.

Puede determinar si la carpeta que intenta restaurar contiene una unión mediante la `vol show` con el `-parent` opción. También puede utilizar el `vserver security trace` comandos para crear registros detallados sobre problemas de acceso a archivos y carpetas.

Información relacionada

Crear y gestionar volúmenes de datos en espacios de nombres NAS

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.