Configurar el acceso de SMB/CIFS a una SVM existente

System Manager Classic

NetApp
June 22, 2024

Tabla de contenidos

Configurar el acceso de SMB/CIFS a una SVM existente

Añadir acceso de clientes SMB/CIFS a una SVM existente implica agregar configuraciones CIFS a la SVM, añadir una asignación en el servidor DNS y comprobar el acceso CIFS desde un host de administración de Windows. A continuación, puede configurar el acceso de cliente CIFS.

Añada el acceso CIFS a una SVM existente

Añadir acceso CIFS/SMB a una SVM existente implica crear una LIF de datos, configurar un servidor CIFS, aprovisionar un volumen, compartir el volumen y configurar los permisos de recursos compartidos.

Antes de empezar

- Debe saber cuáles de los siguientes componentes de red utilizará la SVM:
  - El nodo y el puerto específico en ese nodo en el que se creará la interfaz lógica de datos (LIF)
  - Subred desde la que se aprovisionará la dirección IP de la LIF de datos o, si lo desea, la dirección IP específica que desea asignar a la LIF de datos
  - El dominio de Active Directory (AD) al que se unirá esta SVM, junto con las credenciales necesarias para añadir dicha SVM
- Todos los firewalls externos deben estar configurados correctamente para permitir el acceso a los servicios de red.
- Se debe permitir el protocolo CIFS en la SVM.

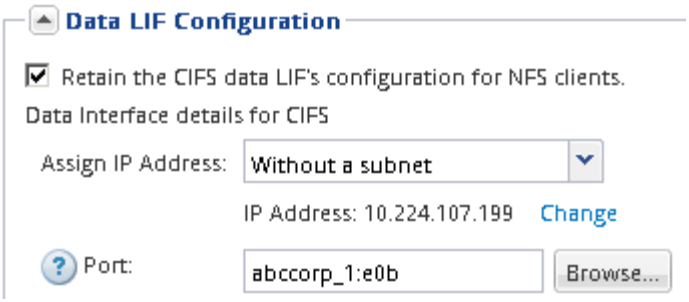
  Este es el caso si no ha creado la SVM siguiendo el procedimiento para configurar un protocolo SAN.

Pasos

1. Desplácese hasta el área en la que pueda configurar los protocolos de la SVM:
   a. Seleccione la SVM que desea configurar.
   b. En el panel **Detalles**, junto a **Protocolos**, haz clic en **CIFS**.

2. En la sección **Configuración de LIF de datos** del cuadro de diálogo **Configurar protocolo CIFS**, cree una LIF de datos para la SVM:
   a. Asigne una dirección IP a la LIF de forma automática desde una subred que especifique o introduzca manualmente la dirección.
   b. Haga clic en **examinar** y seleccione un nodo y un puerto que se asociarán a la LIF.



3. En la sección **Configuración del servidor CIFS**, defina el servidor CIFS y configúrelo para que acceda al dominio AD:

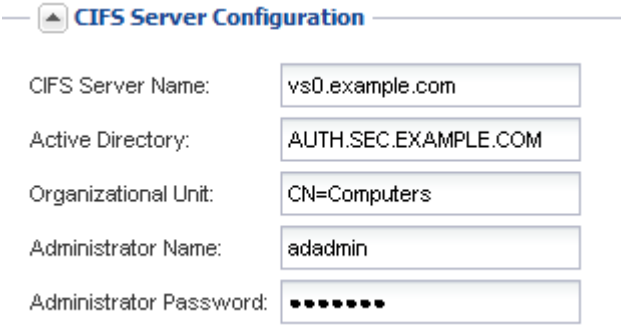
   a. Especifique un nombre para el servidor CIFS que sea único en el dominio de AD.

   b. Especifique el FQDN del dominio AD al que se puede unir el servidor CIFS.

   c. Si desea asociar una unidad organizativa (OU) en el dominio AD que no sea CN=Computers, introduzca la unidad organizativa.

   d. Especifique el nombre y la contraseña de una cuenta administrativa que tenga privilegios suficientes para agregar el servidor CIFS a la unidad organizativa.

   e. Si desea evitar el acceso no autorizado a todos los recursos compartidos de esta SVM, seleccione la opción de cifrar datos mediante SMB 3.0.

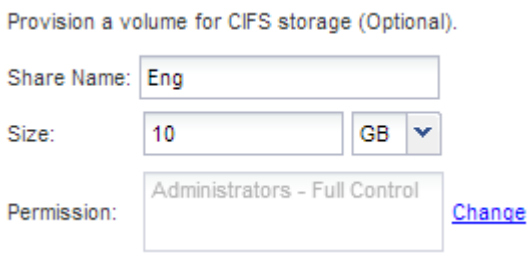


4. Cree un volumen para el acceso CIFS/SMB y aprovisione un recurso compartido en él:

   a. Asigne un nombre al recurso compartido que utilizarán los clientes CIFS/SMB para acceder al volumen.

      El nombre que se introduce para el recurso compartido también se utiliza como nombre del volumen.

   b. Especifique el tamaño del volumen.



No es necesario especificar el agregado para el volumen porque se encuentra automáticamente en el agregado con el mayor espacio disponible.

5. **Opcional**: Restringir el acceso al recurso compartido modificando el ACL compartido:
   a. En el campo **Permission**, haga clic en **Change**.
   b. Seleccione el grupo todos y haga clic en **Quitar**.
   c. **Opcional**: Haga clic en **Agregar** e introduzca el nombre de un grupo de administradores definido en el dominio de Windows Active Directory que incluye la SVM.
   d. Seleccione el nuevo grupo de administradores y, a continuación, seleccione **Control total**.
   e. Haga clic en **Guardar y cerrar**.
6. Haga clic en **Enviar y cerrar** y, a continuación, haga clic en **Aceptar**.

Asigne el servidor SMB en el servidor DNS

El servidor DNS del sitio debe tener una entrada que apunte el nombre del servidor SMB y cualquier alias NetBIOS a la dirección IP de la LIF de datos para que los usuarios de Windows puedan asignar una unidad al nombre del servidor SMB.

Antes de empezar

Debe tener acceso administrativo al servidor DNS del sitio. Si no tiene acceso administrativo, debe solicitar al administrador DNS que realice esta tarea.

Acerca de esta tarea

Si utiliza alias NetBIOS para el nombre del servidor SMB, es una práctica recomendada crear puntos de entrada del servidor DNS para cada alias.

Pasos

1. Inicie sesión en el servidor DNS.
2. Cree entradas de búsqueda hacia delante (a - Registro de dirección) e inversa (PTR - Registro de puntero) para asignar el nombre del servidor SMB a la dirección IP de la LIF de datos.
3. Si utiliza alias NetBIOS, cree una entrada de búsqueda Alias nombre canónico (registro de recursos CNAME) para asignar cada alias a la dirección IP de la LIF de datos del servidor SMB.

Resultados

Una vez que la asignación se propaga a través de la red, los usuarios de Windows pueden asignar una unidad al nombre del servidor SMB o sus alias NetBIOS.

Comprobar el acceso de cliente de SMB

Debe verificar si ha configurado SMB correctamente accediendo y escribiendo los datos en el recurso compartido. Debe probar el acceso utilizando el nombre del servidor SMB y todos los alias NetBIOS.

Pasos

1. Inicie sesión en un cliente Windows.
2. Probar el acceso mediante el nombre del servidor SMB:
   a. En el Explorador de Windows, asigne una unidad al recurso compartido con el siguiente formato: `\\SMB_Server_Name\Share_Name`

Si la asignación no se realiza correctamente, es posible que la asignación DNS aún no se haya propagado por toda la red. Debe probar el acceso más adelante con el nombre del servidor SMB.

Si el servidor SMB se llama vs1.example.com y el recurso compartido se llama SHARE1, debe introducir lo siguiente: `\\vs0.example.com\SHARE1`

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

Verificó el acceso de escritura al recurso compartido mediante el nombre del servidor SMB.

3. Repita el paso 2 para cualquier alias NetBIOS.

Configurar y comprobar el acceso del cliente CIFS

Una vez que esté listo, puede conceder a los clientes seleccionados acceso al recurso compartido estableciendo permisos de archivo NTFS en el Explorador de Windows y modificando la ACL de recurso compartido en System Manager. A continuación, debe probar que los grupos o usuarios afectados pueden acceder al volumen.

Pasos

1. Decida qué clientes, usuarios o grupos tendrán acceso al recurso compartido.
2. En un cliente de Windows, utilice una función de administrador para otorgar permisos a los usuarios o grupos a los archivos y carpetas.
   a. Inicie sesión en un cliente de Windows como administrador que tenga derechos administrativos suficientes para administrar los permisos NTFS.
   b. En el Explorador de Windows, haga clic con el botón secundario del mouse (ratón) en la unidad y, a continuación, seleccione **Propiedades**.
   c. Seleccione la ficha **Seguridad** y ajuste la configuración de seguridad para los grupos y usuarios según sea necesario.
3. En System Manager, modifique la ACL de recurso compartido para proporcionar acceso a los grupos o usuarios de Windows al recurso compartido.
   a. Vaya a la ventana **shares**.
   b. Seleccione el recurso compartido y haga clic en **Editar**.
   c. Seleccione la ficha **permisos** y proporcione a los usuarios o grupos acceso al recurso compartido.
4. En un cliente Windows, inicie sesión como uno de los usuarios que ahora tiene acceso al recurso compartido y a los archivos, y compruebe que puede tener acceso al recurso compartido y crear un archivo.

Información de copyright

Información de la marca comercial