



Configurar un servidor SMB en un dominio de Active Directory

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

- Configurar un servidor SMB en un dominio de Active Directory 1
 - Configurar los servicios de tiempo 1
 - Comandos para gestionar la autenticación simétrica en servidores NTP 1
- Cree un servidor SMB en un dominio de Active Directory 2
- Crear archivos keytab para autenticación SMB 5

Configurar un servidor SMB en un dominio de Active Directory

Configurar los servicios de tiempo

Antes de crear un servidor SMB en una controladora de Active Domain, debe asegurarse de que la hora y la hora del clúster de los controladores de dominio al que pertenecerá el servidor SMB coincidan con en un plazo de cinco minutos.

Acerca de esta tarea

Debe configurar los servicios NTP del clúster para que usen los mismos servidores NTP para la sincronización horaria que utiliza el dominio de Active Directory.

A partir de ONTAP 9.5, puede configurar el servidor NTP con autenticación simétrica.

Pasos



1. Configure los servicios de hora mediante el `cluster time-service ntp server create` comando.
 - Para configurar los servicios de hora sin autenticación simétrica, introduzca el siguiente comando:
`cluster time-service ntp server create -server server_ip_address`
 - Para configurar los servicios de hora con autenticación simétrica, introduzca el siguiente comando:
`cluster time-service ntp server create -server server_ip_address -key-id key_id`
`cluster time-service ntp server create -server 10.10.10.1`
`cluster time-service ntp server create -server 10.10.10.2`
2. Compruebe que los servicios de hora se han configurado correctamente mediante el `cluster time-service ntp server show` comando.

```
cluster time-service ntp server show
```

Server	Version
10.10.10.1	auto
10.10.10.2	auto

Comandos para gestionar la autenticación simétrica en servidores NTP

A partir de ONTAP 9.5, se admite la versión 3 del protocolo de tiempo de redes (NTP). NTPv3 incluye autenticación simétrica mediante claves SHA-1 que aumenta la seguridad de la red.

Para hacer esto...	Se usa este comando...
Configure un servidor NTP sin autenticación simétrica	<pre>cluster time-service ntp server create -server server_name</pre>
Configure un servidor NTP con autenticación simétrica	<pre>cluster time-service ntp server create -server server_ip_address -key-id key_id</pre>
Habilitar autenticación simétrica para un servidor NTP existente se puede modificar el servidor NTP existente para habilitar la autenticación agregando el Id. De clave requerido	<pre>cluster time-service ntp server modify -server server_name -key-id key_id</pre>
Configure una clave NTP compartida	<pre>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</pre> <div>  <p>Las claves compartidas se refieren a un ID. El ID, su tipo y el valor deben ser idénticos tanto en el nodo como en el servidor NTP</p> </div>
Configure un servidor NTP con un ID de clave desconocido	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre>
Configure un servidor con un ID de clave no configurado en el servidor NTP.	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre> <div>  <p>El ID de clave, el tipo y el valor deben ser idénticos al ID de clave, el tipo y el valor configurados en el servidor NTP.</p> </div>
Deshabilitar la autenticación simétrica	<pre>cluster time-service ntp server modify -server server_name -authentication disabled</pre>

Cree un servidor SMB en un dominio de Active Directory

Puede utilizar el `vserver cifs create` Para crear un servidor SMB en la SVM y especificar el dominio de Active Directory (AD) al que pertenece.

Antes de empezar

Las SVM y los LIF que utiliza para servir datos deben haberse configurado para permitir el protocolo SMB. Las LIF deben poder conectarse a los servidores DNS configurados en la SVM y a un controlador de dominio AD del dominio al que desea unirse al servidor SMB.

Cualquier usuario con autorización para crear cuentas de máquina en el dominio de AD al que se va a unir el

servidor SMB puede crear el servidor SMB en la SVM. Esto puede incluir usuarios de otros dominios.

A partir de ONTAP 9.7, el administrador de AD puede proporcionarle un URI a un archivo keytab como alternativa a proporcionarle un nombre y una contraseña a una cuenta de Windows con privilegios. Cuando reciba el URI, inclúyalo en el `-keytab-uri` con el `vserver cifs` comandos.

Acerca de esta tarea

Al crear un servidor SMB en un dominio de directorio de actividades:

- Debe usar el nombre de dominio completo (FQDN) al especificar el dominio.
- La configuración predeterminada es agregar la cuenta de máquina del servidor SMB al objeto CN=Computer de Active Directory.
- Puede optar por agregar el servidor SMB a una unidad organizativa (OU) diferente mediante el `-ou` opción.
- Opcionalmente, puede elegir agregar una lista delimitada por comas de uno o más alias NetBIOS (hasta 200) para el servidor SMB.

La configuración de alias NetBIOS para un servidor SMB puede ser útil cuando está consolidando datos de otros servidores de archivos en el servidor SMB y desea que el servidor SMB responda a los nombres de los servidores originales.

La `vserver cifs` las páginas de manual contienen parámetros opcionales y requisitos de nomenclatura adicionales.



A partir de ONTAP 9.1, puede habilitar SMB versión 2.0 para conectarse a un controlador de dominio (DC). Hacerlo es necesario si ha deshabilitado SMB 1.0 en controladores de dominio. A partir de ONTAP 9.2, SMB 2.0 está habilitado de forma predeterminada.

A partir de ONTAP 9.8, puede especificar que se cifren las conexiones a los controladores de dominio. ONTAP requiere cifrado para las comunicaciones del controlador de dominio cuando el `-encryption-required -for-dc-connection` opción establecida en `true`; el valor predeterminado es `false`. Cuando se establece la opción, solo se utilizará el protocolo SMB3 para las conexiones ONTAP-DC, ya que el cifrado solo es compatible con SMB3. .

"Gestión de SMB" Contiene más información acerca de las opciones de configuración del servidor SMB.

Pasos

1. Compruebe que SMB tiene licencia en el clúster: `system license show -package cifs`

La licencia SMB se incluye con **"ONTAP One"**. Si no tiene ONTAP One y la licencia no está instalada, póngase en contacto con su representante de ventas.

No se requiere una licencia de CIFS si el servidor SMB se usará solo para autenticación.

2. Cree el servidor SMB en un dominio de AD: `vserver cifs create -vserver vserver_name -cifs-server smb_server_name -domain FQDN [-ou organizational_unit] [-netbios-aliases NetBIOS_name, ...] [-keytab-uri {(ftp|http)://hostname|IP_address}] [-comment text]`

Al unirse a un dominio, este comando puede tardar varios minutos en completarse.

El siguiente comando crea el servidor SMB «s' mb_server01» en el dominio "example.com":

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server  
smb_server01 -domain example.com
```

El siguiente comando crea el servidor SMB «smemoria_servidor 2» en el dominio «mydomain.com» y autentica al administrador ONTAP con un archivo keytab:

```
cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server  
smb_server02 -domain mydomain.com -keytab-uri  
http://admin.mydomain.com/ontap1.keytab
```

3. Compruebe la configuración del servidor SMB mediante el `vserver cifs show` comando.

En este ejemplo, el resultado del comando muestra que se creó en SVM `vs1.example.com` un servidor SMB denominado "MB_SERVER01", que se unió al dominio "example.com".

```
cluster1::> vserver cifs show -vserver vs1  
  
Vserver: vs1.example.com  
CIFS Server NetBIOS Name: SMB_SERVER01  
NetBIOS Domain/Workgroup Name: EXAMPLE  
Fully Qualified Domain Name: EXAMPLE.COM  
Default Site Used by LIFs Without Site Membership:  
Authentication Style: domain  
CIFS Server Administrative Status: up  
CIFS Server Description: -  
List of NetBIOS Aliases: -
```

4. Si lo desea, habilite la comunicación cifrada con el controlador de dominio (ONTAP 9.8 y posterior):
`vserver cifs security modify -vserver svm_name -encryption-required-for-dc
-connection true`

Ejemplos

El siguiente comando crea un servidor SMB denominado «mb_server02» en la SVM `vs2.example.com` en el dominio «example.com». La cuenta de equipo se crea en el contenedor "OU=eng,OU=corp,DC=example,DC=com". Al servidor SMB se le asigna un alias NetBIOS.

```
cluster1::> vsserver cifs create -vsserver vs2.example.com -cifs-server  
smb_server02 -domain example.com -ou OU=eng,OU=corp -netbios-aliases  
old_cifs_server01
```

```
cluster1::> vsserver cifs show -vsserver vs1
```

```
                                Vserver: vs2.example.com  
                                CIFS Server NetBIOS Name: SMB_SERVER02  
                                NetBIOS Domain/Workgroup Name: EXAMPLE  
                                Fully Qualified Domain Name: EXAMPLE.COM  
Default Site Used by LIFs Without Site Membership:  
                                Authentication Style: domain  
CIFS Server Administrative Status: up  
                                CIFS Server Description: -  
                                List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

El siguiente comando permite a un usuario de un dominio diferente, en este caso un administrador de un dominio de confianza, crear un servidor SMB denominado «smemoria_servidor03» en la SVM vs3.example.com. La `-domain` La opción especifica el nombre del dominio principal (especificado en la configuración DNS) en el que desea crear el servidor SMB. La `username` la opción especifica el administrador del dominio de confianza.

- Dominio principal: example.com
- Dominio de confianza: trust.lab.com
- Nombre de usuario del dominio de confianza: Administrador1

```
cluster1::> vsserver cifs create -vsserver vs3.example.com -cifs-server  
smb_server03 -domain example.com
```

```
Username: Administrator1@trust.lab.com  
Password: . . .
```

Crear archivos keytab para autenticación SMB

A partir de ONTAP 9.7, ONTAP admite la autenticación de SVM con servidores Active Directory (AD) mediante archivos keytab. Los administradores DE AD generan un archivo keytab y lo ponen a disposición de los administradores de ONTAP como un identificador uniforme de recursos (URI), que se proporciona cuando `vsserver cifs`. Los comandos requieren autenticación Kerberos con el dominio AD.

Los administradores DE AD pueden crear los archivos keytab utilizando el servidor estándar de Windows `ktpass` comando. El comando debe ejecutarse en el dominio principal donde la autenticación es necesaria. La `ktpass` el comando se puede utilizar para generar archivos keytab sólo para usuarios de dominio principal; las claves generadas con usuarios de dominio de confianza no son compatibles.

Los archivos keytab se generan para usuarios específicos de administrador de ONTAP. Siempre que la

contraseña del usuario administrador no cambie, las claves generadas para el tipo de cifrado específico y el dominio no cambiarán. Por lo tanto, se requiere un nuevo archivo keytab cada vez que se cambia la contraseña del usuario admin.

Se admiten los siguientes tipos de cifrado:

- AES256-SHA1
- DES-CBC-MD5



ONTAP no admite el tipo de cifrado DES-CBC-CRC.

- RC4-HMAC

AES256 es el tipo de cifrado más alto y se debe utilizar si está activado en el sistema ONTAP.

Los archivos keytab se pueden generar especificando la contraseña de administrador o mediante una contraseña generada aleatoriamente. Sin embargo, en cualquier momento sólo se puede utilizar una opción de contraseña, ya que en el servidor AD se necesita una clave privada específica para el usuario administrador para descifrar las claves del archivo keytab. Cualquier cambio en la clave privada de un administrador específico anulará el archivo keytab.

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 INTERRUPTIÓN 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.