Comunicación segura de sesiones LDAP

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

Comunicación segura de sesiones LDAP

Conceptos de firma y sellado LDAP

A partir de ONTAP 9, puede configurar la firma y el sellado para habilitar la seguridad de la sesión LDAP en consultas a un servidor de Active Directory (AD). Debe configurar los ajustes de seguridad del servidor CIFS en la máquina virtual de almacenamiento (SVM) para que se correspondan con los del servidor LDAP.

La firma comprueba la integridad de la carga de datos LDAP mediante una tecnología de clave secreta. El sellado cifra la carga de datos LDAP para impedir la transmisión de información confidencial en texto sin cifrar. Una opción *LDAP Security Level* indica si es necesario firmar, firmar y sellar el tráfico LDAP o no. El valor predeterminado es `none`.

La firma y el sellado LDAP en el tráfico CIFS están habilitados en la SVM con el `-session-security-for-ad-ldap` de la `vserver cifs security modify` comando.

Habilite la firma y el sellado LDAP en el servidor CIFS

Antes de que el servidor CIFS pueda utilizar la firma y el sellado para establecer una comunicación segura con un servidor LDAP de Active Directory, debe modificar la configuración de seguridad del servidor CIFS para habilitar la firma y el sellado LDAP.

Antes de empezar

Debe consultar al administrador del servidor AD para determinar los valores de configuración de seguridad adecuados.

Pasos

1. Configure la configuración de seguridad del servidor CIFS que permita el tráfico firmado y sellado con los servidores LDAP de Active Directory: `vserver cifs security modify -vserver` *`vserver_name`* `-session-security-for-ad-ldap {none|sign|seal}`

   Puede habilitar la firma (`sign`, integridad de los datos), firma y sellado (`seal`, integridad y cifrado de los datos), o ninguno de los dos `none`, sin firma ni sellado). El valor predeterminado es `none`.

2. Compruebe que la configuración de seguridad de firma y sellado LDAP está configurada correctamente: `vserver cifs security show -vserver` *`vserver_name`*

> Si la SVM utiliza el mismo servidor LDAP para consultar la asignación de nombres u otra información de UNIX, como usuarios, grupos y netgroups, debe habilitar el valor correspondiente con el `-session-security` opción de `vserver services name-service ldap client modify` comando.

Configure LDAP sobre TLS

Exporte una copia del certificado de CA raíz autofirmado

Para utilizar LDAP sobre SSL/TLS para proteger la comunicación de Active Directory, primero debe exportar una copia del certificado raíz autofirmado del Servicio de certificados de Active Directory a un archivo de certificado y convertirlo en un archivo de texto ASCII. ONTAP utiliza este archivo de texto para instalar el certificado en la máquina virtual de almacenamiento (SVM).

Antes de empezar

El servicio de certificados de Active Directory ya debe estar instalado y configurado para el dominio al que pertenece el servidor CIFS. Puede encontrar información acerca de la instalación y configuración de Active Director Certificate Services consultando la biblioteca de Microsoft TechNet.

"Biblioteca de Microsoft TechNet: technet.microsoft.com"

Paso

1. Obtenga un certificado de CA raíz del controlador de dominio que se encuentra en `.pem` formato de texto.

   "Biblioteca de Microsoft TechNet: technet.microsoft.com"

Después de terminar

Instale el certificado en la SVM.

Información relacionada

"Biblioteca de Microsoft TechNet"

Instale el certificado de CA raíz autofirmado en la SVM

Si se requiere la autenticación LDAP con TLS al enlazar con servidores LDAP, primero debe instalar el certificado de CA raíz autofirmado en la SVM.

Acerca de esta tarea

Cuando LDAP over TLS está habilitado, el cliente LDAP de ONTAP en la SVM no admite certificados revocados en ONTAP 9.0 y 9.1.

A partir de ONTAP 9.2, todas las aplicaciones de ONTAP que utilizan comunicaciones TLS pueden comprobar el estado de certificado digital mediante el protocolo de estado de certificado en línea (OCSP). Si OCSP está habilitado para LDAP over TLS, se rechazan los certificados revocados y la conexión falla.

Pasos

1. Instale el certificado de CA raíz autofirmado:

   a. Comience la instalación del certificado: `security certificate install -vserver vserver_name -type server-ca`

      El resultado de la consola muestra el siguiente mensaje: `Please enter Certificate: Press <Enter> when done`

   b. Abra el certificado `.pem` archivo con un editor de texto, copie el certificado, incluidas las líneas que empiezan por `-----BEGIN CERTIFICATE-----` y terminar con `-----END CERTIFICATE-----`y, a continuación, pegue el certificado después del símbolo del sistema.

c. Compruebe que el certificado se muestra correctamente.

d. Para completar la instalación, pulse Intro.

2. Compruebe que el certificado esté instalado: `security certificate show -vserver` *`vserver_name`*

Habilite LDAP sobre TLS en el servidor

Antes de que el servidor SMB pueda utilizar TLS para obtener comunicación segura con un servidor LDAP de Active Directory, debe modificar la configuración de seguridad del servidor SMB para habilitar LDAP over TLS.

A partir de ONTAP 9.10.1, el enlace de canal LDAP se admite de forma predeterminada tanto para las conexiones LDAP de Active Directory (AD) como de los servicios de nombres. ONTAP intentará establecer la vinculación de canal con las conexiones LDAP solo si Start-TLS o LDAPS está habilitado junto con la seguridad de la sesión establecida en Sign o Seal. Para deshabilitar o volver a habilitar el enlace de canal LDAP con servidores AD, utilice `-try-channel-binding-for-ad-ldap` con el `vserver cifs security modify` comando.

Para obtener más información, consulte:

- "Descripción general de LDAP"
- "2020 requisitos de enlace de canal LDAP y firma LDAP para Windows".

Pasos

1. Configure la opción de seguridad del servidor SMB que permite una comunicación LDAP segura con servidores LDAP de Active Directory: `vserver cifs security modify -vserver` *`vserver_name`* `-use-start-tls-for-ad-ldap true`

2. Compruebe que la configuración de seguridad de LDAP over TLS está establecida en `true`: `vserver cifs security show -vserver` *`vserver_name`*

> Si la SVM utiliza el mismo servidor LDAP para consultar la asignación de nombres u otra información de UNIX (como usuarios, grupos y grupos de red), también debe modificar el `-use-start-tls` mediante el `vserver services name-service ldap client modify` comando.