Secure LDAP session communication

ONTAP 9

NetApp
August 25, 2022

Table of Contents

Secure LDAP session communication . . . 1
LDAP signing and sealing concepts . . . 1
Enable LDAP signing and sealing on the CIFS server . . . 1
Configure LDAP over TLS . . . 1

Secure LDAP session communication

LDAP signing and sealing concepts

Beginning with ONTAP 9, you can configure signing and sealing to enable LDAP session security on queries to an Active Directory (AD) server. You must configure the CIFS server security settings on the storage virtual machine (SVM) to correspond to those on the LDAP server.

Signing confirms the integrity of the LDAP payload data using secret key technology. Sealing encrypts the LDAP payload data to avoid transmitting sensitive information in clear text. An *LDAP Security Level* option indicates whether the LDAP traffic needs to be signed, signed and sealed, or neither. The default is `none`.

LDAP signing and sealing on CIFS traffic is enabled on the SVM with the `-session-security-for-ad-ldap` option to the `vserver cifs security modify` command.

Enable LDAP signing and sealing on the CIFS server

Before your CIFS server can use signing and sealing for secure communication with an Active Directory LDAP server, you must modify the CIFS server security settings to enable LDAP signing and sealing.

Before you begin

You must consult with your AD server administrator to determine the appropriate security configuration values.

Steps

1. Configure the CIFS server security setting that enables signed and sealed traffic with Active Directory LDAP servers: `vserver cifs security modify -vserver` *`vserver_name`* `-session-security-for-ad-ldap {none|sign|seal}`

   You can enable signing (`sign`, data integrity), signing and sealing (`seal`, data integrity and encryption), or neither (`none`, no signing or sealing). The default value is `none`.

2. Verify that the LDAP signing and sealing security setting is set correctly: `vserver cifs security show -vserver` *`vserver_name`*

> If the SVM uses the same LDAP server for querying name-mapping or other UNIX information, such as users, groups, and netgroups, then you must enable the corresponding setting with the `-session-security` option of the `vserver services name-service ldap client modify` command.

Configure LDAP over TLS

Export a copy of the self-signed root CA certificate

To use LDAP over SSL/TLS for securing Active Directory communication, you must first export a copy of the Active Directory Certificate Service's self-signed root CA certificate to

a certificate file and convert it to an ASCII text file. This text file is used by ONTAP to install the certificate on the storage virtual machine (SVM).

Before you begin

The Active Directory Certificate Service must already be installed and configured for the domain to which the CIFS server belongs. You can find information about installing and configuring Active Director Certificate Services by consulting the Microsoft TechNet Library.

Microsoft TechNet Library: technet.microsoft.com

Step

1. Obtain a root CA certificate of the domain controller that is in the `.pem` text format.

   Microsoft TechNet Library: technet.microsoft.com

After you finish

Install the certificate on the SVM.

Related information

Microsoft TechNet Library

Install the self-signed root CA certificate on the SVM

If LDAP authentication with TLS is required when binding to LDAP servers, you must first install the self-signed root CA certificate on the SVM.

About this task

When LDAP over TLS is enabled, the ONTAP LDAP client on the SVM does not support revoked certificates in ONTAP 9.0 and 9.1.

Beginning with ONTAP 9.2, all applications within ONTAP that use TLS communications can check digital certificate status using Online Certificate Status Protocol (OCSP). If OCSP is enabled for LDAP over TLS, revoked certificates are rejected and the connection fails.

Steps

1. Install the self-signed root CA certificate:
   a. Begin the certificate installation: `security certificate install -vserver vserver_name -type server-ca`

      The console output displays the following message: `Please enter Certificate: Press <Enter> when done`

   b. Open the certificate `.pem` file with a text editor, copy the certificate, including the lines beginning with `-----BEGIN CERTIFICATE-----` and ending with `-----END CERTIFICATE-----`, and then paste the certificate after the command prompt.
   c. Verify that the certificate is displayed correctly.
   d. Complete the installation by pressing Enter.
2. Verify that the certificate is installed: `security certificate show -vserver *vserver_name*`

Enable LDAP over TLS on the server

Before your SMB server can use TLS for secure communication with an Active Directory LDAP server, you must modify the SMB server security settings to enable LDAP over TLS.

Beginning with ONTAP 9.10.1, LDAP channel binding is supported by default for both Active Directory (AD) and name services LDAP connections. ONTAP will try channel binding with LDAP connections only if Start-TLS or LDAPS is enabled along with session security set to either sign or seal. To disable or reenable LDAP channel binding with AD servers, use the `-try-channel-binding-for-ad-ldap` parameter with the `vserver cifs security modify` command.

For more information, see 2020 LDAP channel binding and LDAP signing requirements for Windows.

Steps

1. Configure the SMB server security setting that allows secure LDAP communication with Active Directory LDAP servers: `vserver cifs security modify -vserver` *`vserver_name`* `-use-start-tls -for-ad-ldap true`
2. Verify that the LDAP over TLS security setting is set to `true`: `vserver cifs security show -vserver` *`vserver_name`*

> If the SVM uses the same LDAP server for querying name-mapping or other UNIX information (such as users, groups, and netgroups), then you must also modify the `-use -start-tls` option by using the `vserver services name-service ldap client modify` command.

Related information

LDAPS concepts

NFS management