Sichere LDAP-Sitzungskommunikation

ONTAP 9

NetApp
March 22, 2023

Inhaltsverzeichnis

Sichere LDAP-Sitzungskommunikation

LDAP-Signing- und Sealing-Konzepte

Ab ONTAP 9 können Sie Signing and Sealing konfigurieren, um die LDAP-Sitzungssicherheit bei Anfragen an einen Active Directory-Server (AD) zu aktivieren. Sie müssen die Sicherheitseinstellungen des CIFS-Servers auf der Storage Virtual Machine (SVM) so konfigurieren, dass sie den auf dem LDAP-Server entsprechen.

Das Signieren bestätigt die Integrität der LDAP-Nutzlastdaten mithilfe der Geheimschlüsseltechnologie. Das Sealing verschlüsselt die LDAP-Nutzlastdaten, um das Übertragen sensibler Informationen als unverschlüsselten Text zu vermeiden. Die Option *LDAP Security Level* gibt an, ob der LDAP-Datenverkehr signiert, signiert und versiegelt werden muss oder nicht. Die Standardeinstellung lautet `none`.

Das LDAP-Signing and Sealing im CIFS-Verkehr ist auf der SVM mit dem aktiviert `-session-security-for-ad-ldap` Option für die `vserver cifs security modify` Befehl.

Aktivieren Sie das LDAP-Signing und Sealing auf dem CIFS-Server

Bevor Ihr CIFS-Server Signing and Sealing für eine sichere Kommunikation mit einem Active Directory LDAP-Server verwenden kann, müssen Sie die CIFS-Server-Sicherheitseinstellungen ändern, um das LDAP-Signing und das Sealing zu aktivieren.

Bevor Sie beginnen

Sie müssen sich mit Ihrem AD-Serveradministrator in Verbindung setzen, um die entsprechenden Werte für die Sicherheitskonfiguration zu ermitteln.

Schritte

1. Konfigurieren Sie die CIFS-Serversicherheitseinstellung, die den signierten und versiegelten Datenverkehr mit Active Directory LDAP-Servern ermöglicht: `vserver cifs security modify -vserver` *`vserver_name`* `-session-security-for-ad-ldap {none|sign|seal}`

   Sie können das Signieren aktivieren (`sign`, Datenintegrität), Signing und Sealing (`seal`, Datenintegrität und Verschlüsselung) oder keines von beiden `none`, Kein Signing oder Sealing). Der Standardwert ist `none`.

2. Vergewissern Sie sich, dass die LDAP-Einstellung zum Signieren und Versiegeln richtig eingestellt ist: `vserver cifs security show -vserver` *`vserver_name`*

   Wenn die SVM denselben LDAP-Server zum Abfragen der Name-Mapping oder anderer UNIX-Informationen wie Benutzer, Gruppen und Netzgruppen verwendet, müssen Sie die entsprechende Einstellung mit dem aktivieren `-session-security` Option des `vserver services name-service ldap client modify` Befehl.

Konfigurieren Sie LDAP über TLS

Exportieren Sie eine Kopie des selbstsignierten Root-CA-Zertifikats

Um LDAP über SSL/TLS zu verwenden, um die Active Directory-Kommunikation zu sichern, müssen Sie zuerst eine Kopie des selbstsignierten Stammzertifikats des Active Directory-Zertifikatdienstes in eine Zertifikatdatei exportieren und in eine ASCII-Textdatei konvertieren. Diese Textdatei wird von ONTAP verwendet, um das Zertifikat auf der Storage Virtual Machine (SVM) zu installieren.

Bevor Sie beginnen

Der Active Directory Certificate Service muss bereits für die Domäne installiert und konfiguriert sein, zu der der CIFS-Server gehört. Informationen zum Installieren und Konfigurieren von Active Director Certificate Services finden Sie in der Microsoft TechNet Library.

"Microsoft TechNet Bibliothek: technet.microsoft.com"

Schritt

1. Erhalten Sie ein Root-CA-Zertifikat des Domain-Controllers im `.pem` Textformat

   "Microsoft TechNet Bibliothek: technet.microsoft.com"

Nachdem Sie fertig sind

Installieren Sie das Zertifikat auf der SVM.

Verwandte Informationen

"Microsoft TechNet-Bibliothek"

Installieren Sie das selbstsignierte Root-CA-Zertifikat auf der SVM

Wenn bei der Anbindung an LDAP-Server eine LDAP-Authentifizierung mit TLS erforderlich ist, müssen Sie zuerst das selbstsignierte Root-CA-Zertifikat auf der SVM installieren.

Über diese Aufgabe

Wenn LDAP über TLS aktiviert ist, unterstützt der ONTAP-LDAP-Client der SVM nicht widerrief Zertifikate in ONTAP 9.0 und 9.1.

Ab ONTAP 9.2 können alle Anwendungen innerhalb von ONTAP, die TLS-Kommunikation verwenden, den digitalen Zertifikatsstatus mithilfe des Online Certificate Status Protocol (OCSP) überprüfen. Wenn OCSP für LDAP über TLS aktiviert ist, werden zurückgeworfene Zertifikate abgelehnt und die Verbindung schlägt fehl.

Schritte

1. Installieren Sie das selbstsignierte Root-CA-Zertifikat:
   a. Starten Sie die Zertifikatinstallation: `security certificate install -vserver vserver_name -type server-ca`

      Über die Konsolenausgabe wird die folgende Meldung angezeigt: `Please enter Certificate: Press <Enter> when done`

b. Öffnen Sie das Zertifikat `.pem` Datei mit einem Texteditor, kopieren Sie das Zertifikat, einschließlich der Zeilen beginnend mit `-----BEGIN CERTIFICATE-----` Und endet mit `-----END CERTIFICATE-----`, Und fügen Sie dann das Zertifikat nach der Eingabeaufforderung ein.

c. Vergewissern Sie sich, dass das Zertifikat ordnungsgemäß angezeigt wird.

d. Schließen Sie die Installation durch Drücken der Eingabetaste ab.

2. Vergewissern Sie sich, dass das Zertifikat installiert ist: `security certificate show -vserver` *`vserver_name`*

Aktivieren Sie LDAP über TLS auf dem Server

Bevor Ihr SMB-Server TLS für eine sichere Kommunikation mit einem Active Directory LDAP-Server verwenden kann, müssen Sie die SMB-Serversicherheitseinstellungen ändern, um LDAP über TLS zu aktivieren.

Ab ONTAP 9.10.1 wird die LDAP-Kanalbindung standardmäßig sowohl für Active Directory (AD)- als auch für Name-Services-LDAP-Verbindungen unterstützt. ONTAP versucht die Channel-Bindung mit LDAP-Verbindungen nur dann, wenn Start-TLS oder LDAPS aktiviert ist und die Sitzungssicherheit entweder auf Signieren oder Seal gesetzt ist. Um die LDAP-Kanalbindung mit AD-Servern zu deaktivieren oder erneut zu aktivieren, verwenden Sie das `-try-channel-binding-for-ad-ldap` Parameter mit `vserver cifs security modify` Befehl.

Weitere Informationen finden Sie unter:

- "LDAP-Übersicht"
- "2020 LDAP-Channel-Binding und LDAP-Signing-Anforderungen für Windows".

Schritte

1. Konfigurieren Sie die SMB-Server-Sicherheitseinstellung, die eine sichere LDAP-Kommunikation mit Active Directory LDAP-Servern ermöglicht: `vserver cifs security modify -vserver` *`vserver_name`* `-use-start-tls-for-ad-ldap true`
2. Vergewissern Sie sich, dass die Sicherheitseinstellung LDAP über TLS auf festgelegt ist `true`: `vserver cifs security show -vserver` *`vserver_name`*

> Wenn die SVM denselben LDAP-Server zum Abfragen der Name-Zuordnung oder anderer UNIX-Informationen (z. B. Benutzer, Gruppen und Netgroups) verwendet, müssen Sie auch das ändern `-use-start-tls` Mit der Option `vserver services name-service ldap client modify` Befehl.