Communication de session LDAP sécurisée

ONTAP 9

NetApp
April 24, 2024

Sommaire

Communication de session LDAP sécurisée

Concepts de signature et d'étanchéité LDAP

Depuis ONTAP 9, vous pouvez configurer la signature et le chiffrement pour activer la sécurité des sessions LDAP sur les requêtes vers un serveur Active Directory (AD). Vous devez configurer les paramètres de sécurité du serveur CIFS sur la machine virtuelle de stockage (SVM) de sorte qu'ils correspondent à ceux du serveur LDAP.

La signature valide l'intégrité des données LDAP à l'aide d'une technologie à clé secrète. Le chiffrement crypte les données LDAP afin de ne pas transmettre de données sensibles en clair. Une option *LDAP Security Level* indique si le trafic LDAP doit être signé, signé et scellé, ou non. La valeur par défaut est `none`.

La signature et le chiffrement LDAP sur le trafic CIFS sont activés sur le SVM avec le `-session-security -for-ad-ldap` à la `vserver cifs security modify` commande.

Activez le chiffrement et la signature LDAP sur le serveur CIFS

Avant que votre serveur CIFS puisse utiliser la signature et le chiffrement pour sécuriser la communication avec un serveur LDAP Active Directory, vous devez modifier les paramètres de sécurité du serveur CIFS pour activer la signature et le chiffrement LDAP.

Avant de commencer

Vous devez consulter votre administrateur de serveur AD pour déterminer les valeurs de configuration de sécurité appropriées.

Étapes

1. Configurez le paramètre de sécurité du serveur CIFS qui autorise le trafic signé et scellé avec les serveurs LDAP Active Directory : `vserver cifs security modify -vserver` *`vserver_name`* `-session -security-for-ad-ldap {none|sign|seal}`

   Vous pouvez activer la signature (`sign`, intégrité des données), signature et scellage (`seal`, intégrité et chiffrement des données), ou ni l'un ni l'autre `none`, pas de signature ou d'étanchéité). La valeur par défaut est `none`.

2. Vérifiez que le paramètre de sécurité de signature et de chiffrement LDAP est défini correctement : `vserver cifs security show -vserver` *`vserver_name`*

> Si le SVM utilise le même serveur LDAP pour effectuer des requêtes name-mapping ou d'autres informations UNIX, comme les utilisateurs, les groupes et les netgroups, alors vous devez activer le paramètre correspondant avec le `-session-security` de la `vserver services name-service ldap client modify` commande.

Configurer LDAP sur TLS

Exporter une copie du certificat de l'autorité de certification racine auto-signé

Pour utiliser LDAP sur SSL/TLS pour sécuriser la communication Active Directory, vous devez d'abord exporter une copie du certificat d'autorité de certification racine auto-signé du service de certificats Active Directory en fichier de certificat et la convertir en fichier texte ASCII. Ce fichier texte est utilisé par ONTAP pour installer le certificat sur la machine virtuelle de stockage (SVM).

Avant de commencer

Le service de certificat Active Directory doit déjà être installé et configuré pour le domaine auquel le serveur CIFS appartient. Vous trouverez des informations sur l'installation et la configuration des services de certificats Active Director en consultant la bibliothèque Microsoft TechNet.

"Bibliothèque Microsoft TechNet : technet.microsoft.com"

Étape

1. Obtenez un certificat d'autorité de certification racine du contrôleur de domaine qui se trouve dans le `.pem` format de texte.

   "Bibliothèque Microsoft TechNet : technet.microsoft.com"

Une fois que vous avez terminé

Installer le certificat sur le SVM.

Informations associées

"Bibliothèque Microsoft TechNet"

Installer le certificat d'autorité de certification racine auto-signé sur le SVM

Si l'authentification LDAP avec TLS est requise lorsqu'il s'agit de serveurs LDAP, vous devez d'abord installer le certificat AC racine auto-signé sur le SVM.

Description de la tâche

Lorsque LDAP sur TLS est activé, le client LDAP ONTAP sur la SVM ne prend pas en charge les certificats révoqués dans ONTAP 9.0 et 9.1.

Depuis ONTAP 9.2, toutes les applications de ONTAP qui utilisent les communications TLS peuvent vérifier le statut du certificat numérique à l'aide du protocole OCSP (Online Certificate Status Protocol). Si OCSP est activé pour LDAP sur TLS, les certificats révoqués sont rejetés et la connexion échoue.

Étapes

1. Installez le certificat d'autorité de certification racine auto-signé :

   a. Commencez l'installation du certificat : `security certificate install -vserver vserver_name -type server-ca`

      La sortie de la console affiche le message suivant : `Please enter Certificate: Press <Enter> when done`

   b. Ouvrez le certificat `.pem` fichier avec un éditeur de texte, copiez le certificat, y compris les lignes commençant par `-----BEGIN CERTIFICATE-----` et se terminant par `-----END`

`CERTIFICATE-----`, puis collez le certificat après l'invite de commande.

c. Vérifiez que le certificat s'affiche correctement.

d. Terminez l'installation en appuyant sur entrée.

2. Vérifiez que le certificat est installé : `security certificate show -vserver vserver_name`

Activez LDAP sur TLS sur le serveur

Avant que votre serveur SMB puisse utiliser TLS pour sécuriser les communications avec un serveur LDAP Active Directory, vous devez modifier les paramètres de sécurité du serveur SMB pour activer LDAP sur TLS.

Depuis ONTAP 9.10.1, la liaison des canaux LDAP est prise en charge par défaut pour les connexions LDAP Active Directory (AD) et services de noms. ONTAP essaiera la liaison des canaux avec les connexions LDAP uniquement si Start-TLS ou LDAPS est activé avec la sécurité de session définie sur Sign ou SEAL. Pour désactiver ou réactiver la liaison des canaux LDAP avec les serveurs AD, utilisez le `-try-channel-binding-for-ad-ldap` paramètre avec le `vserver cifs security modify` commande.

Pour en savoir plus, voir :

- "Présentation LDAP"
- "2020 exigences de liaison des canaux LDAP et de signature LDAP pour Windows".

Étapes

1. Configurez le paramètre de sécurité du serveur SMB permettant une communication LDAP sécurisée avec les serveurs LDAP Active Directory : `vserver cifs security modify -vserver vserver_name -use-start-tls-for-ad-ldap true`
2. Vérifiez que le paramètre de sécurité LDAP sur TLS est défini sur `true`: `vserver cifs security show -vserver vserver_name`

> Si le SVM utilise le même serveur LDAP pour effectuer des requêtes name-mapping ou d'autres informations UNIX (par exemple, utilisateurs, groupes et netgroups), alors vous devez également modifier `-use-start-tls` à l'aide de `vserver services name-service ldap client modify` commande.