安全 LDAP 会话通信

ONTAP 9

NetApp
April 24, 2024

目录

安全 LDAP 会话通信 1
LDAP 签名和签章概念 1
在 CIFS 服务器上启用 LDAP 签名和签章 1
配置基于 TLS 的 LDAP 1

安全 LDAP 会话通信

LDAP 签名和签章概念

从 ONTAP 9 开始，您可以配置签名和签章，以便对 Active Directory （ AD ）服务器的查询启用 LDAP 会话安全性。您必须在 Storage Virtual Machine （ SVM ）上配置 CIFS 服务器安全设置，使其与 LDAP 服务器上的设置相对应。

签名可使用密钥技术确认 LDAP 有效负载数据的完整性。密封功能对 LDAP 有效负载数据进行加密，以避免以明文形式传输敏感信息。"_LDAP 安全级别 _ " 选项指示 LDAP 流量是需要签名，签名和签章，还是两者都不需要。默认值为 `none`。

已使用在SVM上启用CIFS流量的LDAP签名和签章 `-session-security-for-ad-ldap` 选项 `vserver cifs security modify` 命令：

在 CIFS 服务器上启用 LDAP 签名和签章

在 CIFS 服务器使用签名和签章与 Active Directory LDAP 服务器进行安全通信之前，您必须修改 CIFS 服务器安全设置以启用 LDAP 签名和签章。

开始之前

您必须咨询 AD 服务器管理员以确定适当的安全配置值。

步骤

1. 配置CIFS服务器安全设置、以启用与Active Directory LDAP服务器之间的已签名和已密封流量： `vserver cifs security modify -vserver` *`vserver_name`* `-session-security-for-ad-ldap {none|sign|seal}`

   您可以启用签名 (`sign`、数据完整性)、签名和签章 (`seal``数据完整性和加密）、或者两者都不是 `none`，无签名或签章)。默认值为 `none`。

2. 验证是否已正确设置LDAP签名和签章安全设置： `vserver cifs security show -vserver` *`vserver_name`*

   > 如果SVM使用同一个LDAP服务器查询名称映射或其他UNIX信息(例如用户、组和网络组)、则必须使用启用相应的设置 `-session-security` 的选项 `vserver services name-service ldap client modify` 命令：

配置基于 TLS 的 LDAP

导出自签名根 CA 证书的副本

要使用基于 SSL/TLS 的 LDAP 确保 Active Directory 通信安全，必须先将 Active Directory 证书服务的自签名根 CA 证书副本导出到证书文件，然后将其转换为 ASCII 文本文件。ONTAP 使用此文本文件在 Storage Virtual Machine （ SVM ）上安装证书。

开始之前

必须已为 CIFS 服务器所属的域安装和配置 Active Directory 证书服务。有关安装和配置 Active Director 证书服务的信息，请参见 Microsoft TechNet 库。

"Microsoft TechNet 库： technet.microsoft.com"

步骤

1. 获取中域控制器的根CA证书 `.pem` 文本格式。

   "Microsoft TechNet 库： technet.microsoft.com"

完成后

在 SVM 上安装证书。

相关信息

"Microsoft TechNet 库"

在 SVM 上安装自签名根 CA 证书

如果在绑定到 LDAP 服务器时需要使用 TLS 进行 LDAP 身份验证，则必须先在 SVM 上安装自签名根 CA 证书。

关于此任务

启用基于 TLS 的 LDAP 后， SVM 上的 ONTAP LDAP 客户端在 ONTAP 9.0 和 9.1 中不支持已撤销的证书。

从 ONTAP 9.2 开始， ONTAP 中使用 TLS 通信的所有应用程序都可以使用联机证书状态协议（ Online Certificate Status Protocol ， OCSP ）检查数字证书状态。如果为基于 TLS 的 LDAP 启用了 OCSP ，则已撤销的证书将被拒绝，并且连接将失败。

步骤

1. 安装自签名根 CA 证书：

   a. 开始安装证书： `security certificate install -vserver vserver_name -type server-ca`

      控制台输出将显示以下消息： `Please enter Certificate: Press <Enter> when done`

   b. 打开证书 `.pem` 文件，使用文本编辑器复制证书，包括以开头的行 `-----BEGIN CERTIFICATE-----` 并以结尾 `-----END CERTIFICATE-----`，然后在命令提示符后粘贴证书。

   c. 验证证书是否显示正确。

   d. 按 Enter 键完成安装。

2. 验证是否已安装此证书： `security certificate show -vserver vserver_name`

在服务器上启用基于 TLS 的 LDAP

在SMB服务器使用TLS与Active Directory LDAP服务器进行安全通信之前、您必须修改SMB服务器安全设置以启用基于TLS的LDAP。

从 ONTAP 9.10.1 开始，默认情况下， Active Directory （AD）和名称服务 LDAP 连接均支持 LDAP 通道绑定。只有在启用了 Start-TLS 或 LDAPS 且会话安全设置为 sign 或 seal 的情况下， ONTAP 才会尝试使用 LDAP 连接进行通道绑定。要禁用或重新启用与AD服务器的LDAP通道绑定、请使用 `-try-channel-binding-for-ad-ldap` 参数 `vserver cifs security modify` 命令：

要了解更多信息、请参见：

- "LDAP概述"
- "2020 年 Windows 的 LDAP 通道绑定和 LDAP 签名要求"。

步骤

1. 配置SMB服务器安全设置、以允许与Active Directory LDAP服务器进行安全LDAP通信： `vserver cifs security modify -vserver` *`vserver_name`* `-use-start-tls-for-ad-ldap true`
2. 验证基于TLS的LDAP安全设置是否设置为 `true`： `vserver cifs security show -vserver` *`vserver_name`*

> 如果SVM使用同一个LDAP服务器来查询名称映射或其他UNIX信息(例如用户、组和网络组)、则还必须修改 `-use-start-tls` 选项 `vserver services name-service ldap client modify` 命令：