



# 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 vservers 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：  
`vservers cifs security modify -vservers vservers_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：  
`vservers cifs security show -vservers vservers_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 vservers 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](http://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](http://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 vservice_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 vservice_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：

## 版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

## 商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。