管理 SMB 服务器安全设置

ONTAP 9

NetApp
April 24, 2024

目录

管理 SMB 服务器安全设置

ONTAP 如何处理 SMB 客户端身份验证

用户必须先通过SMB服务器所属的域进行身份验证、然后才能创建SMB连接以访问SVM上包含的数据。SMB服务器支持两种身份验证方法：Kerberos和NTLM (NTLMv1或NTLMv2)。Kerberos 是用于对域用户进行身份验证的默认方法。

Kerberos 身份验证

在创建经过身份验证的 SMB 会话时， ONTAP 支持 Kerberos 身份验证。

Kerberos 是 Active Directory 的主身份验证服务。Kerberos 服务器或 Kerberos 密钥分发中心（ KDC ）服务可在 Active Directory 中存储和检索有关安全原则的信息。与 NTLM 模式不同，要与另一台计算机（如 SMB 服务器）建立会话的 Active Directory 客户端会直接联系 KDC 以获取其会话凭据。

NTLM身份验证

NTLM 客户端身份验证可使用质询响应协议来完成，该协议基于密码共享用户特定的机密信息。

如果用户使用本地 Windows 用户帐户创建 SMB 连接，则 SMB 服务器将使用 NTLMv2 在本地完成身份验证。

SVM 灾难恢复配置中的 SMB 服务器安全设置准则

在创建配置为不保留身份的灾难恢复目标的SVM之前(`-identity-preserve` 选项设置为 `false` 在SnapMirror配置中)、您应了解如何在目标SVM上管理SMB服务器安全设置。

- 非默认 SMB 服务器安全设置不会复制到目标。

  在目标 SVM 上创建 SMB 服务器时，所有 SMB 服务器安全设置均设置为默认值。初始化，更新或重新同步 SVM 灾难恢复目标时，源上的 SMB 服务器安全设置不会复制到目标。

- 您必须手动配置非默认 SMB 服务器安全设置。

  如果在源 SVM 上配置了非默认 SMB 服务器安全设置，则在目标变为读写（ SnapMirror 关系中断）后，必须在目标 SVM 上手动配置这些相同的设置。

显示有关SMB服务器安全设置的信息

您可以显示Storage Virtual Machine (SVM)上的SMB服务器安全设置信息。您可以使用此信息验证安全设置是否正确。

关于此任务

显示的安全设置可以是该对象的默认值，也可以是使用 ONTAP 命令行界面或使用 Active Directory 组策略对象（ GPO ）配置的非默认值。

请勿使用 `vserver cifs security show` 命令、因为某些选项无效。

步骤

1. 执行以下操作之一：

要显示的信息	输入命令 ...
指定 SVM 上的所有安全设置	`vserver cifs security show -vserver` *`vserver_name`*
SVM 上的特定安全设置	`vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]` 您可以输入 `-fields ?` 以确定您可以使用哪些字段。

示例

以下示例显示了 SVM vs1 的所有安全设置：

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                          Kerberos Clock Skew:        5 minutes
                          Kerberos Ticket Age:        10 hours
                         Kerberos Renewal Age:        7 days
                         Kerberos KDC Timeout:        3 seconds
                          Is Signing Required:        false
              Is Password Complexity Required:        true
         Use start_tls For AD LDAP connection:        false
                     Is AES Encryption Enabled:        false
                        LM Compatibility Level:        lm-ntlm-ntlmv2-krb
                    Is SMB Encryption Required:        false
                       Client Session Security:        none
              SMB1 Enabled for DC Connections:        false
              SMB2 Enabled for DC Connections:        system-default
LDAP Referral Enabled For AD LDAP connections:        false
             Use LDAPS for AD LDAP connection:        false
    Encryption is required for DC Connections:        false
 AES session key enabled for NetLogon channel:        false
  Try Channel Binding For AD LDAP Connections:        false
```

请注意，显示的设置取决于正在运行的 ONTAP 版本。

以下示例显示了 SVM vs1 的 Kerberos 时钟偏差：

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

            vserver kerberos-clock-skew
            ------- -------------------
            vs1     5
```

相关信息

显示有关 GPO 配置的信息

为本地 SMB 用户启用或禁用所需的密码复杂度

所需的密码复杂性可增强 Storage Virtual Machine （SVM）上本地 SMB 用户的安全性。默认情况下，所需的密码复杂度功能处于启用状态。您可以随时将其禁用并重新启用。

开始之前

必须在 CIFS 服务器上启用本地用户，本地组和本地用户身份验证。

关于此任务

您不能使用 `vserver cifs security modify` 命令、因为某些选项无效。

步骤

1. 执行以下操作之一：

本地 **SMB** 用户所需的密码复杂度	输入命令 ...
enabled	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required true`
已禁用	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required false`

2. 验证所需密码复杂度的安全设置： `vserver cifs security show -vserver` *`vserver_name`*

示例

以下示例显示为 SVM vs1 的本地 SMB 用户启用了所需的密码复杂度：

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
------- -------------------------------
vs1     true
```

相关信息

显示有关 CIFS 服务器安全设置的信息

使用本地用户和组进行身份验证和授权

本地用户密码的要求

更改本地用户帐户密码

修改 CIFS 服务器 Kerberos 安全设置

您可以修改某些 CIFS 服务器 Kerberos 安全设置，包括允许的最大 Kerberos 时钟偏差时间， Kerberos 票证生命周期以及票证续订天数。

关于此任务

使用修改CIFS服务器Kerberos设置 `vserver cifs security modify` 命令仅会修改您使用指定的单个Storage Virtual Machine (SVM)上的设置 `-vserver` 参数。您可以使用 Active Directory 组策略对象（ GPO ）集中管理属于同一 Active Directory 域的集群上所有 SVM 的 Kerberos 安全设置。

步骤

1. 执行以下一项或多项操作：

如果您要 ...	输入 ...
指定允许的最大Kerberos时钟偏差时间(以分钟(9.13.1及更高版本)或秒(9.12.1或更低版本)为单位。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-clock-skew` *`integer_in_minutes`* 默认设置为 5 分钟。
以小时为单位指定 Kerberos 票证的生命周期。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours` 默认设置为 10 小时。

指定最大票证续订天数。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-renew-age` *`integer_in_days`* 默认设置为 7 天。
指定 KDC 上的套接字超时，超过此超时后，所有 KDC 都将标记为不可访问。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-kdc-timeout` *`integer_in_seconds`* 默认设置为 3 秒。

2. 验证 Kerberos 安全设置：

   `vserver cifs security show -vserver` *`vserver_name`*

示例

以下示例对 Kerberos 安全性进行了以下更改：对于 SVM vs1 ， "`Kerberos Clock Skew` " 设置为 3 分钟，"`Kerberos 票证期限` " 设置为 8 小时：

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                    Kerberos Clock Skew:                   3 minutes
                    Kerberos Ticket Age:                   8 hours
                   Kerberos Renewal Age:                   7 days
                   Kerberos KDC Timeout:                   3 seconds
                    Is Signing Required:               false
        Is Password Complexity Required:                true
   Use start_tls For AD LDAP connection:               false
             Is AES Encryption Enabled:               false
                LM Compatibility Level:  lm-ntlm-ntlmv2-krb
             Is SMB Encryption Required:               false
```

相关信息

"显示有关 CIFS 服务器安全设置的信息"

"支持的 GPO"

"将组策略对象应用于 CIFS 服务器"

设置SMB服务器最低身份验证安全级别

您可以在 SMB 服务器上设置 SMB 服务器的最低安全级别，也称为 *LMCompatibilityLevel*，以满足 SMB 客户端访问的业务安全要求。最低安全级别是SMB服务器从SMB客户端接受的最低安全令牌级别。

关于此任务

- 工作组模式下的SMB服务器仅支持NTLM身份验证。不支持 Kerberos 身份验证。
- LMCompatibilityLevel 仅适用于 SMB 客户端身份验证，而不适用于管理员身份验证。

您可以将最低身份验证安全级别设置为四个受支持的安全级别之一。

价值	Description
`lm-ntlm-ntlmv2-krb` (默认)	Storage Virtual Machine （ SVM ） 接受 LM ， NTLM ， NTLMv2 和 Kerberos 身份验证安全性。
`ntlm-ntlmv2-krb`	SVM 接受 NTLM ， NTLMv2 和 Kerberos 身份验证安全性。SVM 拒绝 LM 身份验证。
`ntlmv2-krb`	SVM 接受 NTLMv2 和 Kerberos 身份验证安全性。SVM 拒绝 LM 和 NTLM 身份验证。
`krb`	SVM 仅接受 Kerberos 身份验证安全性。SVM 拒绝 LM ， NTLM 和 NTLMv2 身份验证。

步骤

1. 设置最低身份验证安全级别： `vserver cifs security modify -vserver vserver_name -lm -compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. 验证身份验证安全级别是否设置为所需级别： `vserver cifs security show -vserver vserver_name`

相关信息

为基于 Kerberos 的通信启用或禁用 AES 加密

使用 AES 加密为基于 Kerberos 的通信配置强大的安全性

为了通过基于 Kerberos 的通信实现最强的安全性，您可以在 SMB 服务器上启用 AES-256 和 AES-128 加密。默认情况下、在SVM上创建SMB服务器时、高级加密标准(Advanced Encryption Standard、AES)加密处于禁用状态。您必须启用它才能利用AES加密提供的强大安全性。

在 SVM 上创建 SMB 服务器期间以及 SMB 会话设置阶段期间，会使用 SMB 的 Kerberos 相关通信。SMB 服务器支持以下 Kerberos 通信加密类型：

- AES 256
- AES 128
- DES
- RC4-HMAC

如果要对 Kerberos 通信使用最高安全加密类型，则应在 SVM 上为 Kerberos 通信启用 AES 加密。

创建 SMB 服务器时，域控制器会在 Active Directory 中创建计算机帐户。此时， KDC 将了解特定计算机帐户的加密功能。随后，系统会选择一种特定的加密类型来加密客户端在身份验证期间向服务器提供的服务单。

从ONTAP 9.12.1开始、您可以指定要向Active Directory (AD) KDC公布的加密类型。您可以使用 `-advertised-enc-types` 选项以启用建议的加密类型、您可以使用此选项禁用较弱的加密类型。了解操作方法 "为基于Kerberos的通信启用和禁用加密类型"。

> SMB 3.0 提供了 Intel AES 新指令（ Intel AES NI ），可改进 AES 算法并加快受支持处理器系列的数据加密速度。从 SMB 3.1.1 开始， AES-128-GCM 将 AES-128-CCM 替换为 SMB 加密使用的哈希算法。

相关信息

修改 CIFS 服务器 Kerberos 安全设置

为基于 Kerberos 的通信启用或禁用 AES 加密

要利用基于Kerberos的通信的最强安全性、您应在SMB服务器上使用AES-256和AES-128加密。从ONTAP 9.131开始、默认情况下会启用AES加密。 如果不希望SMB服务器为与Active Directory (AD) KDC进行基于Kerberos的通信选择AES加密类型、则可以禁用AES加密。

默认情况下是否启用AES加密以及是否可以指定加密类型取决于您的ONTAP版本。

ONTAP 版本	**AES**加密已启用…	是否可以指定加密类型?
9.13.1及更高版本	默认情况下。	是的。
9.12.1.	手动	是的。
9.11.1及更早版本	手动	否

从ONTAP 9.12.1开始、使用启用和禁用AES加密 `-advertised-enc-types` 选项、用于指定向AD KDC公布的加密类型。默认设置为 `rc4` 和 `des`、但如果指定了AES类型、则会启用AES加密。您还可以使用选项显式禁用较弱的RC4和DES加密类型。在ONTAP 9.11.1及更早版本中、必须使用 `-is-aes-encryption-enabled` 用于启用和禁用AES加密的选项、并且无法指定加密类型。

为了增强安全性， Storage Virtual Machine （ SVM ）会在每次修改 AES 安全选项时更改 AD 中的计算机帐户密码。更改密码可能需要包含计算机帐户的组织单位（ OU ）的管理 AD 凭据。

如果将SVM配置为不保留身份的灾难恢复目标(`-identity-preserve` 选项设置为 `false` 在SnapMirror配置中)、非默认SMB服务器安全设置不会复制到目标。如果已在源SVM上启用AES加密、则必须手动启用它。

示例 **1.** 步骤

ONTAP 9.12.1及更高版本

1. 执行以下操作之一：

Kerberos 通信的 **AES** 加密类型	输入命令 **...**
enabled	`vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256`
已禁用	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

   注意： `-is-aes-encryption-enabled` 选项在ONTAP 9.12.1中已弃用、可能会在更高版本中删除。

2. 验证是否已根据需要启用或禁用AES加密： `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

示例

以下示例将为SVM vs1上的SMB服务器启用AES加密类型：

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs1      aes-128,aes-256
```

以下示例为SVM VS2上的SMB服务器启用AES加密类型。系统会提示管理员输入包含SMB服务器的OU的管理AD凭据。

```
cluster1::> vserver cifs security modify -vserver vs2 -advertised-enc
-types aes-128,aes-256

Info: In order to enable SMB AES encryption, the password for the SMB
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs2      aes-128,aes-256
```

ONTAP 9.11.1及更早版本

1. 执行以下操作之一：

Kerberos 通信的 **AES** 加密类型	输入命令 **...**
enabled	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled true`
已禁用	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false`

2. 验证是否已根据需要启用或禁用AES加密： `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

   - `is-aes-encryption-enabled` 字段 `true` 如果启用了AES加密、则为和 `false` 如果已禁用。

示例

以下示例将为SVM vs1上的SMB服务器启用AES加密类型：

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- --------------------------
vs1      true
```

以下示例为SVM VS2上的SMB服务器启用AES加密类型。系统会提示管理员输入包含SMB服务器的OU的管理AD凭据。

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- --------------------------
vs2      true
```

使用 SMB 签名增强网络安全性

使用 SMB 签名增强网络安全概述

SMB 签名有助于确保 SMB 服务器和客户端之间的网络流量不会受到影响；它可以通过防止重放攻击来实现这一点。默认情况下，当客户端请求 SMB 签名时， ONTAP 支持 SMB 签名。或者，存储管理员可以将 SMB 服务器配置为需要 SMB 签名。

SMB 签名策略如何影响与 CIFS 服务器的通信

除了 CIFS 服务器 SMB 签名安全设置之外， Windows 客户端上的两个 SMB 签名策略还控制客户端与 CIFS 服务器之间通信的数字签名。您可以配置满足业务要求的设置。

客户端 SMB 策略通过 Windows 本地安全策略设置进行控制，这些设置通过使用 Microsoft 管理控制台（ MMC ）或 Active Directory GPO 进行配置。有关客户端 SMB 签名和安全问题的详细信息，请参见 Microsoft Windows 文档。

下面介绍了 Microsoft 客户端上的两个 SMB 签名策略：

- `Microsoft network client: Digitally sign communications (if server agrees)`

  此设置控制是否启用客户端的 SMB 签名功能。默认情况下，此选项处于启用状态。如果在客户端上禁用此设置，则客户端与 CIFS 服务器的通信取决于 CIFS 服务器上的 SMB 签名设置。

- `Microsoft network client: Digitally sign communications (always)`

  此设置控制客户端是否需要 SMB 签名才能与服务器进行通信。默认情况下，此选项处于禁用状态。如果在客户端上禁用此设置、则SMB签名行为取决于的策略设置 `Microsoft network client: Digitally sign communications (if server agrees)` 和CIFS服务器上的设置。

> 如果您的环境包含配置为需要 SMB 签名的 Windows 客户端，则必须在 CIFS 服务器上启用 SMB 签名。否则， CIFS 服务器将无法为这些系统提供数据。

客户端和 CIFS 服务器 SMB 签名设置的有效结果取决于 SMB 会话是使用 SMB 1.0 还是 SMB 2.x 及更高版本。

下表总结了会话使用 SMB 1.0 时有效的 SMB 签名行为：

客户端	不需要 **ONTAP** 签名	需要 **ONTAP** 签名
已禁用且不需要签名	未签名	已签名
已启用签名，但不需要签名	未签名	已签名
签名已禁用且为必填项	已签名	已签名
已启用且需要签名	已签名	已签名

> 如果在客户端上禁用了签名，但在 CIFS 服务器上需要签名，则较早的 Windows SMB 1 客户端和某些非 Windows SMB 1 客户端可能无法连接。

下表总结了会话使用 SMB 2.x 或 SMB 3.0 时有效的 SMB 签名行为：

> 对于 SMB 2.x 和 SMB 3.0 客户端， SMB 签名始终处于启用状态。不能将其禁用。

客户端	不需要 **ONTAP** 签名	需要 **ONTAP** 签名
不需要签名	未签名	已签名
需要签名	已签名	已签名

下表总结了默认的 Microsoft 客户端和服务器 SMB 签名行为：

协议	哈希算法	可以启用 / 禁用	可能需要 / 不需要	客户端默认值	服务器默认值	**DC** 默认值
SMB 1.0	MD5	是的。	是的。	已启用（不需要）	已禁用（不需要）	Required
SMB 2.x	HMAC SHA-256	否	是的。	不需要	不需要	Required
SMB 3.0	AES-CMAC。	否	是的。	不需要	不需要	Required

> Microsoft不再建议使用 `Digitally sign communications (if client agrees)` 或 `Digitally sign communications (if server agrees)` 组策略设置。Microsoft也不再建议使用 `EnableSecuritySignature` 注册表设置。这些选项仅影响SMB 1行为、可以替换为 `Digitally sign communications (always)` 组策略设置或 `RequireSecuritySignature` 注册表设置。您还可以从Microsoft博客中获取更多信息。http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx[The签名基础知识(涵盖SMB1和SMB2)]

SMB 签名的性能影响

当 SMB 会话使用 SMB 签名时，与 Windows 客户端之间的所有 SMB 通信都会受到性能影响，从而影响客户端和服务器（即运行包含 SMB 服务器的 SVM 的集群上的节点）。

性能影响显示为客户端和服务器上的 CPU 利用率增加，但网络流量不会改变。

性能影响的程度取决于所运行的 ONTAP 9 版本。从 ONTAP 9.7 开始，新的非负载加密算法可以提高签名 SMB 流量的性能。如果启用了 SMB 签名，则默认情况下会启用 SMB 签名卸载。

要提高 SMB 签名性能，需要 AES-NI 卸载功能。请参见 Hardware Universe （ HWU ）以验证您的平台是否支持 AES-NI 卸载。

如果您能够使用SMB版本3.11、该版本支持更快的GCM算法、则性能也可能进一步提高。

根据您的网络， ONTAP 9 版本， SMB 版本和 SVM 实施情况， SMB 签名对性能的影响可能差别很大；您只能通过在网络环境中进行测试来验证它。

如果在服务器上启用了 SMB 签名，则大多数 Windows 客户端默认协商 SMB 签名。如果您需要为某些 Windows 客户端提供 SMB 保护，并且 SMB 签名导致性能问题，则可以在任何不需要防止重放攻击的 Windows 客户端上禁用 SMB 签名。有关在 Windows 客户端上禁用 SMB 签名的信息，请参见 Microsoft

Windows 文档。

配置 SMB 签名的建议

您可以在 SMB 客户端和 CIFS 服务器之间配置 SMB 签名行为，以满足您的安全要求。在 CIFS 服务器上配置 SMB 签名时选择的设置取决于您的安全要求。

您可以在客户端或 CIFS 服务器上配置 SMB 签名。配置 SMB 签名时，请考虑以下建议：

条件	建议
您希望提高客户端与服务器之间通信的安全性	通过启用、在客户端上设置所需的SMB签名 `Require Option (Sign always)` 客户端上的安全设置。
您希望对特定 Storage Virtual Machine （ SVM ）的所有 SMB 流量进行签名	通过将安全设置配置为需要 SMB 签名，在 CIFS 服务器上设置需要 SMB 签名。

有关配置 Windows 客户端安全设置的详细信息，请参见 Microsoft 文档。

配置多个数据 LIF 时的 SMB 签名准则

如果在 SMB 服务器上启用或禁用所需的 SMB 签名，则应了解 SVM 的多个数据 LIF 配置的准则。

配置 SMB 服务器时，可能会配置多个数据 LIF 。如果是、则DNS服务器包含多个 `A` 记录CIFS服务器的条目、所有条目都使用相同的SMB服务器主机名、但每个条目都具有唯一的IP地址。例如、配置了两个数据生命周期的SMB服务器可能具有以下DNS `A` 记录条目：

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

正常情况下，更改所需的 SMB 签名设置后，只有来自客户端的新连接才会受到 SMB 签名设置更改的影响。但是，此行为存在例外情况。在某些情况下，客户端已与共享建立连接，并且客户端会在更改此设置后创建与同一共享的新连接，同时保持原始连接。在这种情况下，新的和现有的 SMB 连接都采用新的 SMB 签名要求。

请考虑以下示例：

1. 客户端1使用路径连接到共享、而不需要SMB签名 `O:\`。
2. 存储管理员将 SMB 服务器配置修改为需要 SMB 签名。
3. 客户端1使用路径连接到具有所需SMB签名的同一共享 `S:\` (同时使用路径保持连接 `O:\`）。
4. 这样、在通过这两个访问数据时、将使用SMB签名 `O:\` 和 `S:\` 驱动器。

为传入的 SMB 流量启用或禁用所需的 SMB 签名

您可以通过启用所需的 SMB 签名来强制实施客户端对 SMB 消息签名的要求。如果启用，

则 ONTAP 仅在 SMB 消息具有有效签名时才接受这些消息。如果要允许 SMB 签名，但不需要它，可以禁用所需的 SMB 签名。

关于此任务

默认情况下，所需的 SMB 签名处于禁用状态。您可以随时启用或禁用所需的 SMB 签名。

> 在以下情况下，默认情况下不会禁用 SMB 签名：
>
> 1. 已启用所需的 SMB 签名，并且集群将还原到不支持 SMB 签名的 ONTAP 版本。
> 2. 集群随后升级到支持 SMB 签名的 ONTAP 版本。
>
> 在这些情况下，最初在受支持的 ONTAP 版本上配置的 SMB 签名配置将通过还原和后续升级保留。

在设置Storage Virtual Machine (SVM)灾难恢复关系时、是为选择的值 `-identity-preserve` 的选项 `snapmirror create` 命令用于确定复制到目标SVM中的配置详细信息。

如果您设置了 `-identity-preserve` 选项 `true` (ID保留)、则SMB签名安全设置将复制到目标。

如果您设置了 `-identity-preserve` 选项 `false` (非ID保留)、则SMB签名安全设置不会复制到目标。在这种情况下，目标上的 CIFS 服务器安全设置将设置为默认值。如果已在源 SVM 上启用所需的 SMB 签名，则必须在目标 SVM 上手动启用所需的 SMB 签名。

步骤

1. 执行以下操作之一：

所需的 **SMB** 签名状态	输入命令 **...**
enabled	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required true`
已禁用	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required false`

2. 通过确定中的值来验证是否已启用或禁用所需的SMB签名 `Is Signing Required` 字段设置为所需值：
   `vserver cifs security show -vserver` *`vserver_name`* `-fields is-signing-required`

示例

以下示例将为 SVM vs1 启用所需的 SMB 签名：

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver  is-signing-required
-------- -------------------
vs1      true
```

对加密设置所做的更改将对新连接生效。现有连接不受影响。

确定 SMB 会话是否已签名

您可以显示有关 CIFS 服务器上已连接的 SMB 会话的信息。您可以使用此信息确定 SMB 会话是否已签名。这有助于确定 SMB 客户端会话是否使用所需的安全设置进行连接。

步骤

1. 执行以下操作之一：

要显示的信息	输入命令 ...
指定 Storage Virtual Machine （ SVM ）上的所有已签名会话	`vserver cifs session show -vserver` *`vserver_name`* `-is-session-signed true`
SVM 上具有特定会话 ID 的已签名会话的详细信息	`vserver cifs session show -vserver` *`vserver_name`* `-session-id integer -instance`

示例

以下命令显示 SVM vs1 上已签名会话的会话信息。默认摘要输出不会显示 "`Is Session Signed` " 输出字段：

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
----------  ------- ---------------- ------------- ------- ------------
3151272279  1       10.1.1.1         DOMAIN\joe          2          23s
```

以下命令显示会话 ID 为 2 的 SMB 会话的详细会话信息，包括会话是否已签名：

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
                Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                  Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                 Windows User: DOMAIN\joe
                    UNIX User: pcuser
                  Open Shares: 1
                   Open Files: 1
                   Open Other: 0
               Connected Time: 10m 43s
                    Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                 NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

相关信息

监控 SMB 签名会话统计信息

监控 SMB 签名会话统计信息

您可以监控 SMB 会话统计信息，并确定哪些已建立的会话已签名，哪些未签名。

关于此任务

。 `statistics` 命令可在高级权限级别提供 `signed_sessions` 可用于监控已签名SMB会话数的计数器。。 `signed_sessions` 计数器可用于以下统计信息对象：

- `cifs` 用于监控所有SMB会话的SMB签名。
- `smb1` 用于监控SMB 1.0会话的SMB签名。
- `smb2` 用于监控SMB 2.x和SMB 3.0会话的SMB签名。

  SMB 3.0统计信息包括在的输出中 `smb2` 对象。

如果要将已签名会话数与会话总数进行比较、可以比较的输出 `signed_sessions` 计数器与的输出 `established_sessions` 计数器。

您必须先启动统计信息样本收集，然后才能查看生成的数据。如果不停止数据收集，您可以查看样本中的数据。停止数据收集可提供一个固定样本。如果不停止数据收集，则可以获取更新后的数据，以便与先前的查询进行比较。此比较可帮助您确定趋势。

步骤

1. 将权限级别设置为高级：+ `set -privilege advanced`
2. 开始数据收集：+ `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]`

   如果未指定 `-sample-id` 参数时、该命令将为您生成示例标识符、并将此示例定义为命令行界面会话的默认示例。的值 `-sample-id` 是文本字符串。如果您在同一命令行界面会话期间运行此命令、但未指定 `-sample-id` 参数、则此命令将覆盖先前的默认样本。

   您也可以指定要收集统计信息的节点。如果未指定节点，则此示例将收集集群中所有节点的统计信息。

3. 使用 `statistics stop` 命令停止收集样本数据。
4. 查看 SMB 签名统计信息：

要查看的信息	输入 ...
已签名的会话	`show -sample-id sample_ID -counter signed_sessions
node_name [-node *node_name*]`	已签名的会话和已建立的会话
`show -sample-id *sample_ID* -counter signed_sessions	established_sessions

   如果要仅显示单个节点的信息、请指定可选 `-node` 参数。

5. 返回到管理权限级别：+ `set -privilege admin`

示例

以下示例显示了如何监控 Storage Virtual Machine （ SVM ） vs1 上的 SMB 2.x 和 SMB 3.0 签名统计信息。

以下命令将移至高级权限级别：

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

以下命令将开始收集新样本的数据：

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

以下命令将停止收集样本的数据：

```
cluster1::*> statistics stop -sample-id smbsigning_sample
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

以下命令按示例中的节点显示已签名的 SMB 会话和已建立的 SMB 会话：

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|established_sessions|node_name

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- -------------------------
    established_sessions                                            0
    node_name                                                   node1
    signed_sessions                                                 0
    established_sessions                                            1
    node_name                                                   node2
    signed_sessions                                                 1
    established_sessions                                            0
    node_name                                                   node3
    signed_sessions                                                 0
    established_sessions                                            0
    node_name                                                   node4
    signed_sessions                                                 0
```

以下命令显示样本中 node2 的已签名 SMB 会话：

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|node_name -node node2

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- -------------------------
    node_name                                                   node2
    signed_sessions                                                 1
```

以下命令将移回管理权限级别：

```
cluster1::*> set -privilege admin
```

相关信息

确定 SMB 会话是否已签名

"性能监控和管理概述"

在 SMB 服务器上配置通过 SMB 传输数据所需的 SMB 加密

SMB加密概述

通过 SMB 进行数据传输的 SMB 加密是一种安全增强功能，您可以在 SMB 服务器上启用或禁用此功能。您还可以通过共享属性设置在共享基础上配置所需的 SMB 加密设置。

默认情况下、在Storage Virtual Machine (SVM)上创建SMB服务器时、SMB加密处于禁用状态。您必须启用 SMB 加密才能利用 SMB 加密提供的增强安全性。

要创建加密的 SMB 会话， SMB 客户端必须支持 SMB 加密。从 Windows Server 2012 和 Windows 8 开始的 Windows 客户端支持 SMB 加密。

SVM 上的 SMB 加密通过两种设置控制：

- 在SVM上启用此功能的SMB服务器安全选项
- 一种SMB共享属性、用于基于共享配置SMB加密设置

您可以决定是要求加密才能访问 SVM 上的所有数据，还是要求 SMB 加密才能仅访问选定共享中的数据。SVM 级别的设置将取代共享级别的设置。

有效的 SMB 加密配置取决于这两种设置的组合，下表对此进行了介绍：

已启用 **SMB** 服务器 **SMB** 加密	已启用共享加密数据设置	服务器端加密行为
true	false	已为 SVM 中的所有共享启用服务器级别加密。使用此配置时，整个 SMB 会话都会进行加密。
true	true	无论共享级别加密如何， SVM 中的所有共享都会启用服务器级别加密。使用此配置时，整个 SMB 会话都会进行加密。
false	true	已为特定共享启用共享级别加密。使用此配置时，会从树连接进行加密。
false	false	未启用加密。

不支持加密的SMB客户端无法连接到需要加密的SMB服务器或共享。

对加密设置所做的更改将对新连接生效。现有连接不受影响。

SMB 加密对性能的影响

当 SMB 会话使用 SMB 加密时，与 Windows 客户端之间的所有 SMB 通信都会受到性能影响，从而影响客户端和服务器（即运行包含 SMB 服务器的 SVM 的集群上的节点）。

性能影响显示为客户端和服务器上的 CPU 利用率增加，但网络流量不会改变。

性能影响的程度取决于所运行的 ONTAP 9 版本。从 ONTAP 9.7 开始，新的加密负载下算法可以提高加密 SMB 流量的性能。如果启用了 SMB 加密，则默认情况下会启用 SMB 加密卸载。

增强的 SMB 加密性能需要 AES-NI 卸载功能。请参见 Hardware Universe （ HWU ）以验证您的平台是否支持 AES-NI 卸载。

如果您能够使用SMB版本3.11、该版本支持更快的GCM算法、则性能也可能进一步提高。

根据您的网络， ONTAP 9 版本， SMB 版本和 SVM 实施情况， SMB 加密对性能的影响可能差别很大；您只能通过在网络环境中进行测试来验证它。

SMB 服务器默认禁用 SMB 加密。您应仅在需要加密的 SMB 共享或 SMB 服务器上启用 SMB 加密。通过 SMB 加密， ONTAP 可以对请求进行解密，并对每个请求的响应进行加密。因此，只有在必要时才应启用 SMB 加密。

为传入的 SMB 流量启用或禁用所需的 SMB 加密

如果您希望为传入的 SMB 流量要求 SMB 加密，可以在 CIFS 服务器或共享级别启用它。默认情况下，不需要 SMB 加密。

关于此任务

您可以在 CIFS 服务器上启用 SMB 加密，该服务器会对 CIFS 服务器上的所有共享进行适用场景。如果您不希望 CIFS 服务器上的所有共享都需要 SMB 加密，或者您希望为基于共享的传入 SMB 流量启用所需的 SMB 加密，则可以在 CIFS 服务器上禁用所需的 SMB 加密。

在设置Storage Virtual Machine (SVM)灾难恢复关系时、您为选择的值 `-identity-preserve` 的选项 `snapmirror create` 命令用于确定复制到目标SVM中的配置详细信息。

如果您设置了 `-identity-preserve` 选项 `true` (ID保留)、则SMB加密安全设置将复制到目标。

如果您设置了 `-identity-preserve` 选项 `false` (非ID保留)、则SMB加密安全设置不会复制到目标。在这种情况下，目标上的 CIFS 服务器安全设置将设置为默认值。如果已在源 SVM 上启用 SMB 加密，则必须在目标上手动启用 CIFS 服务器 SMB 加密。

步骤

1. 执行以下操作之一：

CIFS 服务器上传入的 **SMB** 流量所需的 **SMB** 加密	输入命令 **...**
enabled	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required true`

CIFS 服务器上传入的 SMB 流量所需的 SMB 加密	输入命令 ...
已禁用	`vserver cifs security modify -vserver vserver_name -is-smb-encryption -required false`

2. 验证是否已根据需要在CIFS服务器上启用或禁用所需的SMB加密： `vserver cifs security show -vserver vserver_name -fields is-smb-encryption-required`

   。 `is-smb-encryption-required` 字段 `true` 如果需要、可在CIFS服务器和上启用SMB加密 `false` 如果已禁用。

示例

以下示例将为 SVM vs1 上的 CIFS 服务器的传入 SMB 流量启用所需的 SMB 加密：

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

确定客户端是否使用加密的 SMB 会话进行连接

您可以显示有关已连接 SMB 会话的信息，以确定客户端是否正在使用加密的 SMB 连接。这有助于确定 SMB 客户端会话是否使用所需的安全设置进行连接。

关于此任务

SMB 客户端会话可以具有以下三种加密级别之一：

- `unencrypted`

  SMB 会话未加密。未配置 Storage Virtual Machine （ SVM ）级别或共享级别的加密。

- `partially-encrypted`

  发生树连接时会启动加密。已配置共享级别加密。未启用 SVM 级别的加密。

- `encrypted`

  SMB 会话已完全加密。已启用 SVM 级别的加密。可能已启用，也可能未启用共享级别加密。SVM 级别的加密设置将取代共享级别的加密设置。

步骤

1. 执行以下操作之一：

要显示的信息	输入命令 ...
具有指定 SVM 上会话的指定加密设置的会话	`vserver cifs session show -vserver *vserver_name* {unencrypted
partially-encrypted	encrypted} -instance`
指定 SVM 上特定会话 ID 的加密设置	`vserver cifs session show -vserver *vserver_name* -session-id *integer* -instance`

示例

以下命令显示会话 ID 为 2 的 SMB 会话的详细会话信息，包括加密设置：

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

监控 SMB 加密统计信息

您可以监控 SMB 加密统计信息，并确定哪些已建立的会话和共享连接已加密，哪些未加密。

关于此任务

。 `statistics` 高级权限级别的命令提供了以下计数器、您可以使用这些计数器监控加密的SMB会话和共享连接的数量：

计数器名称	说明
encrypted_sessions	提供加密的 SMB 3.0 会话的数量
encrypted_share_connections	提供发生树连接的加密共享的数量
rejected_unencrypted_sessions	提供因缺少客户端加密功能而拒绝的会话设置数量
rejected_unencrypted_shares	提供因缺少客户端加密功能而拒绝的共享映射的数量

这些计数器可用于以下统计信息对象：

- `cifs` 用于监控所有SMB 3.0会话的SMB加密。

  SMB 3.0统计信息包括在的输出中 `cifs` 对象。 如果要将加密会话数与会话总数进行比较、可以比较的输出 `encrypted_sessions` 计数器与的输出 `established_sessions` 计数器。

  如果要将加密共享连接数与共享连接总数进行比较、则可以比较的输出 `encrypted_share_connections` 计数器与的输出 `connected_shares` 计数器。

- `rejected_unencrypted_sessions` 提供尝试建立需要从不支持SMB加密的客户端加密的SMB会话的次数。
- `rejected_unencrypted_shares` 提供尝试连接到需要从不支持SMB加密的客户端加密的SMB共享的次数。

您必须先启动统计信息样本收集，然后才能查看生成的数据。如果不停止数据收集，您可以查看样本中的数据。停止数据收集可提供一个固定样本。如果不停止数据收集，则可以获取更新后的数据，以便与先前的查询进行比较。此比较可帮助您确定趋势。

步骤

1. 将权限级别设置为高级：+ `set -privilege advanced`
2. 开始数据收集：+ `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   如果未指定 `-sample-id` 参数时、该命令将为您生成示例标识符、并将此示例定义为命令行界面会话的默认示例。的值 `-sample-id` 是文本字符串。如果您在同一命令行界面会话期间运行此命令、但未指定 `-sample-id` 参数、则此命令将覆盖先前的默认样本。

   您也可以指定要收集统计信息的节点。如果未指定节点，则此示例将收集集群中所有节点的统计信息。

3. 使用 `statistics stop` 命令停止收集样本数据。
4. 查看 SMB 加密统计信息：

要查看的信息	输入 ...
加密会话	`show -sample-id *sample_ID* -counter encrypted_sessions

要查看的信息	输入 ...
node_name [-node *node_name*]`	已加密会话和已建立的会话
`show -sample-id *sample_ID* -counter encrypted_sessions	established_sessions
node_name [-node *node_name*]`	加密的共享连接
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`
加密的共享连接和连接的共享	`show -sample-id *sample_ID* -counter encrypted_share_connections
connected_shares	*node_name* [-node *node_name*]`
拒绝的未加密会话	`show -sample-id *sample_ID* -counter rejected_unencrypted_sessions
node_name [-node *node_name*]`	拒绝未加密的共享连接
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

如果要仅显示单个节点的信息、请指定可选 `-node` 参数。

5. 返回到管理权限级别：+ `set -privilege admin`

示例

以下示例显示了如何监控 Storage Virtual Machine （ SVM ） vs1 上的 SMB 3.0 加密统计信息。

以下命令将移至高级权限级别：

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

以下命令将开始收集新样本的数据：

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

以下命令将停止收集该样本的数据：

```
cluster1::*> statistics stop -sample-id smbencryption_sample
Statistics collection is being stopped for Sample-id:
smbencryption_sample
```

以下命令显示样本中节点的加密 SMB 会话和已建立的 SMB 会话：

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2

    Counter                                Value
    ----------------------------  -----------------------
    established_sessions                      1
    encrypted_sessions                        1

2 entries were displayed
```

以下命令显示样本中节点拒绝的未加密 SMB 会话的数量：

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2

    Counter                                     Value
    ----------------------------    ----------------------
    rejected_unencrypted_sessions                 1

1 entry was displayed.
```

以下命令显示样本中节点的已连接 SMB 共享和加密 SMB 共享的数量：

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

    Counter                                      Value
    ----------------------------    ----------------------
    connected_shares                               2
    encrypted_share_connections                    1

2 entries were displayed.
```

以下命令显示样本中节点拒绝的未加密 SMB 共享连接的数量：

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

    Counter                                     Value
    --------------------------------    ----------------------
    rejected_unencrypted_shares                   1

1 entry was displayed.
```

相关信息

确定可用的统计信息对象和计数器

"性能监控和管理概述"

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：