# 管理SMB伺服器安全性設定

ONTAP 9

NetApp
February 12, 2026

# 目錄

# 管理SMB伺服器安全性設定

## 瞭解如何處理 ONTAP SMB 用戶端驗證

使用者必須先由SMB伺服器所屬的網域驗證、才能建立SMB連線來存取SVM上所含的資料。SMB伺服器支援兩種驗證方法：Kerberos和NTLM（位在NTLMv1或NTLMv2之間）。Kerberos是用於驗證網域使用者的預設方法。

### Kerberos驗證

建立驗證的SMB工作階段時、支援Kerberos驗證。ONTAP

Kerberos是Active Directory的主要驗證服務。Kerberos伺服器或Kerberos金鑰發佈中心（Kdc）服務會在Active Directory中儲存及擷取安全性原則的相關資訊。與NTLM模式不同的是、Active Directory用戶端若想要與另一部電腦（例如SMB伺服器）建立工作階段、請直接聯絡Kdc以取得其工作階段認證。

### NTLM 驗證

以密碼為基礎、根據使用者專屬密碼的共享知識、使用挑戰回應傳輸協定來完成NTLM用戶端驗證。

如果使用者使用本機 Windows 使用者帳戶建立 SMB 連線、則驗證作業會由 SMB 伺服器使用 NTLMv2 在本機完成。

## 瞭解 ONTAP SVM 災難恢復組態的 SMB 伺服器安全性設定

建立 SVM 之前、請先將其設定為災難恢復目的地、但不會保留身分識別（ `-identity -preserve` 選項設定為 `false` 在 SnapMirror 組態中）、您應該知道如何在目的地 SVM 上管理 SMB 伺服器安全性設定。

- 非預設的SMB伺服器安全性設定不會複寫到目的地。

  當您在目的地SVM上建立SMB伺服器時、所有SMB伺服器安全性設定都會設為預設值。當SVM災難恢復目的地初始化、更新或重新同步時、來源上的SMB伺服器安全性設定不會複寫到目的地。

- 您必須手動設定非預設的SMB伺服器安全性設定。

  如果您在來源SVM上設定了非預設的SMB伺服器安全性設定、則必須在目的地SVM變成讀寫（SnapMirror關係中斷之後）之後、在目的地上手動設定這些相同的設定。

## 顯示 ONTAP SMB 伺服器安全性設定的相關資訊

您可以在儲存虛擬機器（SVM）上顯示SMB伺服器安全性設定的相關資訊。您可以使用此資訊來驗證安全性設定是否正確。

關於這項工作

顯示的安全性設定可以是該物件的預設值、也可以是透過ONTAP 使用列舉CLI或使用Active Directory群組原則

物件（GPO）設定的非預設值。

請勿使用 `vserver cifs security show` 工作群組模式中 SMB 伺服器的命令、因為某些選項無效。

步驟

1. 執行下列其中一項動作：

| 如果您想要顯示有關...的資訊 | 輸入命令... |
| --- | --- |
| 指定SVM上的所有安全性設定 | `vserver cifs security show -vserver` *`vserver_name`* |
| SVM上的特定安全性設定或設定 | `vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]` 您可以輸入 `-fields ?` 決定您可以使用哪些欄位。 |

範例

下列範例顯示SVM VS1的所有安全性設定：

```
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
```

請注意、顯示的設定取決於執行ONTAP 中的版本。

以下範例顯示SVM VS1的Kerberos時鐘偏移：

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

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

相關資訊

顯示有關GPO組態的資訊

# 為本機 SMB 使用者設定 ONTAP 密碼複雜度

所需的密碼複雜度可為儲存虛擬機器（SVM）上的本機SMB使用者提供更高的安全性。預設會啟用所需的密碼複雜度功能。您可以隨時停用並重新啟用。

開始之前

必須在CIFS伺服器上啟用本機使用者、本機群組和本機使用者驗證。

關於這項工作

請勿在工作群組模式中使用 `vserver cifs security modify` CIFS 伺服器的命令，因為某些選項無效。

步驟

1. 執行下列其中一項動作：

| 如果您想讓本機SMB使用者的密碼複雜度達到所需... | 輸入命令... |
| --- | --- |
| 已啟用 | `vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required true` |
| 已停用 | `vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required false` |

2. 驗證所需密碼複雜度的安全性設定： `vserver cifs security show -vserver` *`vserver_name`*

範例

以下範例顯示、SVM VS1的本機SMB使用者已啟用必要的密碼複雜度：

```
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
```

相關資訊

- 顯示有關伺服器安全設定的信息
- 了解本地用戶和群組
- 本機使用者密碼需求
- 變更本機使用者帳戶密碼

# 修改 ONTAP SMB 伺服器 Kerberos 安全性設定

您可以修改某些CIFS伺服器Kerberos安全性設定、包括允許的Kerberos時鐘偏移時間上限、Kerberos票證壽命、以及票證續約天數上限。

關於這項工作

使用修改 CIFS 伺服器 Kerberos 設定 `vserver cifs security modify` 命令只會修改您使用指定的單一儲存虛擬機器（ SVM ）上的設定 `-vserver` 參數。您可以使用Active Directory群組原則物件（GPO）、集中管理屬於同一個Active Directory網域之叢集上所有SVM的Kerberos安全性設定。

步驟

1. 執行下列一或多項動作：

| 如果您想要... | 輸入... |
| --- | --- |
| 指定允許的 Kerberos 時鐘偏差時間上限（以分鐘為單位（ 9.13.1 及更新版本）或秒（ 9.12.1 或更新版本）。 | `vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-clock-skew` *`integer_in_minutes`*<br><br>預設設定為5分鐘。 |
| 以小時為單位指定Kerberos票證壽命。 | `vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours`<br><br>預設設定為10小時。 |

| | |
|---|---|
| 指定通知單續約天數上限。 | `vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-renew-age` *`integer_in_days`*<br><br>預設設定為7天。 |
| 指定KDC上的通訊端逾時、之後所有KDC都會標示為無法連線。 | `vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-kdc-timeout` *`integer_in_seconds`*<br><br>預設設定為3秒。 |

2. 驗證Kerberos安全性設定：

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

範例

下列範例對Kerberos安全性進行下列變更：「Kerberos時鐘偏移」設為3分鐘、而SVM VS1的「Kerberos票證時間」設為8小時：

```
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
```

相關資訊

"顯示有關伺服器安全設定的信息"

"支援的GPO"

"將群組原則物件套用至CIFS伺服器"

# 設定 ONTAP SMB 伺服器的最低驗證安全層級

您可以在SMB伺服器上設定SMB伺服器的最低安全性層級（也稱為_LMCompatibilityLevel）、以符合SMB用戶端存取的企業安全性需求。最低安全層級是SMB伺服器從SMB用戶端接受的安全性權杖最低層級。

關於這項工作

- 工作群組模式中的SMB伺服器僅支援NTLM驗證。不支援Kerberos驗證。
- LMCompatibilityLevel僅適用於SMB用戶端驗證、不適用於管理驗證。

您可以將最低驗證安全性層級設為四種支援的安全性層級之一。

| 價值 | 說明 |
| --- | --- |
| `lm-ntlm-ntlmv2-krb` （預設） | 儲存虛擬機器（SVM）接受LM、NTLM、NTLMv2及Kerberos驗證安全性。 |
| `ntlm-ntlmv2-krb` | SVM接受NTLM、NTLMv2及Kerberos驗證安全性。SVM拒絕LM驗證。 |
| `ntlmv2-krb` | SVM接受NTLMv2和Kerberos驗證安全性。SVM拒絕LM和NTLM驗證。 |
| `krb` | SVM僅接受Kerberos驗證安全性。SVM會拒絕LM、NTLM及NTLMv2驗證。 |

步驟

1. 設定最低驗證安全層級： `vserver cifs security modify -vserver vserver_name -lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. 驗證驗證安全性層級是否設為所需層級： `vserver cifs security show -vserver vserver_name`

相關資訊

為基於 Kerberos 的通訊配置 AES 加密

# 使用 AES 加密，為 Kerberos 型通訊設定強大的 ONTAP SMB 安全性

為了以Kerberos為基礎的通訊提供最強大的安全性、您可以在SMB伺服器上啟用AES-256和AES-128加密。根據預設、當您在SVM上建立SMB伺服器時、會停用進階加密標準（AES）加密。您必須讓IT能夠充分利用AES加密所提供的強大安全性。

SMB的Kerberos相關通訊是在SVM上建立SMB伺服器期間、以及SMB工作階段設定階段期間使用。SMB伺服器支援下列Kerberos通訊加密類型：

- AES 256

- AES 128
- 第
- RC4-HMAC

如果您想要使用最高的安全性加密類型進行Kerberos通訊、您應該在SVM上啟用AES加密來進行Kerberos通訊。

建立SMB伺服器時、網域控制器會在Active Directory中建立電腦帳戶。此時、Kdc會得知特定機器帳戶的加密功能。之後、會選取特定的加密類型來加密用戶端在驗證期間向伺服器顯示的服務票證。

從ONTAP 《支援資料》9.12.1開始、您可以指定要向Active Directory（AD）kdc通告的加密類型。您可以使用`-advertised-enc-types`選項來啟用建議的加密類型，也可以使用它來停用較弱的加密類型。瞭解如何"為基於 Kerberos 的通訊配置 AES 加密"。

SMB 3.0提供Intel AES新指令（Intel AES NI）、可改善AES演算法、並以支援的處理器系列產品加速資料加密。從SMB 3.3.1開始、AES-120-GCM取代AES-120-CCMs做為SMB加密所使用的雜湊演算法。

相關資訊

修改伺服器安全設定

# 為 ONTAP SMB Kerberos 型通訊設定 AES 加密

若要利用以 Kerberos 為基礎的通訊所提供的最強大安全性、您應該在 SMB 伺服器上使用 AES-256 和 AES-128 加密。從 ONTAP 9.13.1 開始、預設會啟用 AES 加密。 如果您不希望SMB伺服器選取AES加密類型、以便與Active Directory（AD）kdc進行Kerberos型通訊、您可以停用AES加密。

是否預設啟用 AES 加密、以及您是否可以選擇指定加密類型、取決於您的 ONTAP 版本。

| 版本**ONTAP** | **AES** 加密已啟用 ... | 您可以指定加密類型嗎？ |
|---|---|---|
| 9.13.1 及更新版本 | 依預設 | 是的 |
| 9.12.1 | 手動 | 是的 |
| 9.11.1 及更早版本 | 手動 | 否 |

從ONTAP 功能支援的9.12.1開始、AES加密會使用啟用和停用 `-advertised-enc-types` 選項、可讓您指定通告給AD Kdc的加密類型。預設設定為 `rc4` 和 `des`，但當指定AES類型時，將會啟用AES加密。您也可以使用選項來明確停用較弱的RC4和DES加密類型。在 ONTAP 9.11.1 及更早版本中、您必須使用 `-is-aes-encryption-enabled` 啟用和停用AES加密的選項、無法指定加密類型。

為了增強安全性、儲存虛擬機器（SVM）會在每次修改AES安全性選項時、變更AD中的機器帳戶密碼。變更密碼可能需要包含機器帳戶的組織單位（OU）的系統管理AD認證。

如果 SVM 設定為災難恢復目的地、而該目的地不會保留身分識別（ `-identity-preserve` 選項設定為 `false` 在 SnapMirror 組態中）、非預設 SMB 伺服器安全性設定不會複寫到目的地。如果您已在來源 SVM 上啟用 AES 加密、則必須手動啟用。

範例 **1.** 步驟

更新版本**ONTAP**

1. 執行下列其中一項動作：

| 如果您希望**Kerberos**通訊的**AES**加密類型… | 輸入命令… |
| --- | --- |
| 已啟用 | `vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256` |
| 已停用 | `vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4` |

附註： The `-is-aes-encryption-enabled` 選項在ONTAP 更新版本中已過時、可能會在更新版本中移除。

2. 確認已視需要啟用或停用AES加密： `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

範例

以下範例可為 SVM VS1 上的 SMB 伺服器啟用 AES 加密類型：

```
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
```

下列範例可為SVM VS2上的SMB伺服器啟用AES加密類型。系統會提示系統管理員輸入包含SMB伺服器之OU的管理AD認證。

```
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
```

更新版本**ONTAP**

1. 執行下列其中一項動作：

| 如果您希望**Kerberos**通訊的**AES**加密類型... | 輸入命令... |
| --- | --- |
| 已啟用 | `vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled true` |
| 已停用 | `vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false` |

2. 確認已視需要啟用或停用AES加密： `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

   ◦ `is-aes-encryption-enabled` 欄位隨即顯示 `true` 如果已啟用 AES 加密、且 `false` 如果已停用。

範例

以下範例可為 SVM VS1 上的 SMB 伺服器啟用 AES 加密類型：

```
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
```

下列範例可為SVM VS2上的SMB伺服器啟用AES加密類型。系統會提示系統管理員輸入包含SMB伺服器之OU的管理AD認證。

```
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
```

相關資訊

"網域使用者無法使用網域通道登入叢集"

# 使用SMB簽署來強化網路安全性

## 瞭解如何使用 ONTAP SMB 簽署來增強網路安全性

SMB簽章有助於確保SMB伺服器與用戶端之間的網路流量不會受到影響、並可防止重播攻擊。根據預設ONTAP 、若用戶端要求、支援SMB簽署。或者、儲存管理員可以將SMB伺服器設定為需要SMB簽署。

## 瞭解簽署原則如何影響與 **ONTAP SMB** 伺服器的通訊

除了CIFS伺服器SMB簽署安全性設定之外、Windows用戶端上的兩個SMB簽署原則也會控制用戶端與CIFS伺服器之間的通訊數位簽署。您可以設定符合業務需求的設定。

用戶端SMB原則是透過Windows本機安全性原則設定來控制、這些設定是使用Microsoft管理主控台（MMC）或Active Directory GPO來設定。如需用戶端SMB簽署與安全性問題的詳細資訊、請參閱Microsoft Windows文件。

以下是Microsoft用戶端上兩種SMB簽署原則的說明：

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

  此設定可控制是否啟用用戶端的SMB簽署功能。預設為啟用。當用戶端停用此設定時、與CIFS伺服器的用戶端通訊取決於CIFS伺服器上的SMB簽署設定。

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

  此設定可控制用戶端是否需要SMB簽署才能與伺服器通訊。預設為停用。當用戶端上停用此設定時、 SMB簽署行為會根據的原則設定而定 `Microsoft network client: Digitally sign communications (if server agrees)` 以及 CIFS 伺服器上的設定。

> 如果您的環境包含設定為需要SMB簽署的Windows用戶端、則必須在CIFS伺服器上啟用SMB簽署。如果您沒有、CIFS伺服器就無法將資料提供給這些系統。

用戶端和CIFS伺服器SMB簽署設定的有效結果取決於SMB工作階段是使用SMB 1.0或SMB 2.x或更新版本。

下表摘要說明當工作階段使用SMB 1.0時的有效SMB簽署行為：

| 用戶端 | **ONTAP** -不需要簽署 | **ONTAP** -需要簽署 |
|---|---|---|
| 簽署已停用且不需要 | 未簽署 | 已簽署 |
| 簽署已啟用且不需要 | 未簽署 | 已簽署 |
| 簽署已停用且必要 | 已簽署 | 已簽署 |
| 簽署已啟用且必要 | 已簽署 | 已簽署 |

> 舊版Windows SMB 1用戶端和部分非Windows SMB 1用戶端若在用戶端上停用簽署、但CIFS伺服器上需要簽署、則可能無法連線。

下表摘要說明當工作階段使用SMB 2.x或SMB 3.0時的有效SMB簽署行為：

> 對於SMB 2.x和SMB 3.0用戶端、一律會啟用SMB簽署。無法停用。

| 用戶端 | **ONTAP** -不需要簽署 | **ONTAP** -需要簽署 |
| --- | --- | --- |
| 不需要簽署 | 未簽署 | 已簽署 |
| 需要簽署 | 已簽署 | 已簽署 |

下表摘要說明預設的Microsoft用戶端和伺服器SMB簽署行為：

| 傳輸協定 | 雜湊演算法 | 可啟用/停用 | 可能需要/不需要 | 用戶端預設值 | 伺服器預設值 | **DC**預設值 |
| --- | --- | --- | --- | --- | --- | --- |
| SMB 1.0 | md5 | 是的 | 是的 | 已啟用（非必要） | 已停用（非必要） | 必要 |
| SMB 2.x | HMAC SHA-256 | 否 | 是的 | 不需要 | 不需要 | 必要 |
| SMB 3.0 | AES-CMAC： | 否 | 是的 | 不需要 | 不需要 | 必要 |

Microsoft 不再建議使用 `Digitally sign communications (if client agrees)` 或 `Digitally sign communications (if server agrees)` 群組原則設定。Microsoft 也不再建議使用 `EnableSecuritySignature` 登錄設定。這些選項只會影響 SMB 1 行為、可由取代 `Digitally sign communications (always)` 群組原則設定或 `RequireSecuritySignature` 登錄設定。您也可以從 Microsoft 部落格取得更多資訊。 The SMB 簽署基礎知識（涵蓋 SMB1 和 SMB2 ）

## 瞭解 **ONTAP SMB** 簽署對效能的影響

### 當SMB工作階段使用SMB簽署時、所有往返Windows用戶端的SMB通訊都會受到效能影響、這會影響用戶端和伺服器（亦即、叢集上執行SVM的節點包含SMB伺服器）。

效能影響顯示用戶端和伺服器的CPU使用量增加、不過網路流量並未改變。

效能影響的程度取決於ONTAP 您所執行的版本的VMware®。從推出全新的加密卸載演算法、即可在ONTAP 簽署的SMB流量中提供更好的效能。啟用SMB簽署時、預設會啟用SMB簽署卸載。

增強的SMB簽署效能需要AES-NI卸載功能。請參閱Hardware Universe 《支援資料》（HWU）、確認您的平台是否支援AES-NI卸載。

如果您能夠使用支援速度更快的 GCM 演算法的 SMB 版本 3.11 、也可以進一步改善效能。

視您的網路ONTAP 、支援的版本為VMware、SMB版本及SVM實作而定、SMB簽署的效能影響可能會有很大差異；您只能在網路環境中進行測試來驗證。

如果伺服器上已啟用SMB簽署、則大部分的Windows用戶端會依預設協調SMB簽署。如果您的部分Windows用戶端需要SMB保護、而且SMB簽章造成效能問題、您可以在任何不需要保護以防止重播攻擊的Windows用戶端上停用SMB簽署。如需在Windows用戶端上停用SMB簽署的相關資訊、請參閱Microsoft Windows文件。

## ONTAP SMB 簽署組態建議

您可以設定SMB用戶端與CIFS伺服器之間的SMB簽署行為、以符合您的安全需求。您在CIFS伺服器上設定SMB簽署時所選擇的設定、取決於您的安全需求。

您可以在用戶端或CIFS伺服器上設定SMB簽署。設定SMB簽署時、請考慮下列建議：

| 如果... | 建議... |
| --- | --- |
| 您想要提高用戶端與伺服器之間通訊的安全性 | 啟用、讓用戶端需要 SMB 簽署 `Require Option (Sign always)` 用戶端上的安全性設定。 |
| 您希望所有SMB流量都簽署到特定的儲存虛擬機器（SVM） | 設定安全性設定以要求SMB簽署、使CIFS伺服器上的SMB簽署成為必要項目。 |

如需設定Windows用戶端安全性設定的詳細資訊、請參閱Microsoft文件。

## 瞭解多重資料生命的 ONTAP SMB 簽署組態

如果您在SMB伺服器上啟用或停用必要的SMB簽署、您應該瞭解SVM多重資料生命量組態的準則。

設定SMB伺服器時、可能會設定多個資料生命量。如果是、則 DNS 伺服器包含多個 `A` 記錄 CIFS 伺服器的項目、所有項目都使用相同的 SMB 伺服器主機名稱、但每個項目都有唯一的 IP 位址。例如、已設定兩個資料生命期的 SMB 伺服器可能具有下列 DNS `A` 記錄項目：

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

正常情況是、變更必要的SMB簽署設定後、只有來自用戶端的新連線會受到SMB簽署設定的變更影響。不過、這種行為有例外。在某種情況下、用戶端與共用有現有的連線、而用戶端會在變更設定之後、建立新的連線至同一個共用區、同時維持原始連線。在這種情況下、新的和現有的SMB連線都會採用新的SMB簽署要求。

請考慮下列範例：

1. Client1 連接到共享區、而不需要使用路徑簽署 SMB `O:\`。
2. 儲存管理員會修改SMB伺服器組態、以要求SMB簽署。
3. Client1 會使用路徑連線到具有必要 SMB 簽署的同一個共用區 `S:\` （同時使用路徑維持連線 `O:\`）。
4. 結果是在存取兩者的資料時、會使用 SMB 簽署 `O:\` 和 `S:\` 磁碟機。

## 為傳入的 SMB 流量設定 ONTAP 簽署

您可以啟用必要的SMB簽署、強制要求用戶端簽署SMB訊息。如果啟用ONTAP 、僅當SMB訊息具有有效的簽名時、才會接受該訊息。如果您想要允許SMB簽署、但不需要SMB簽署、可以停用必要的SMB簽署。

關於這項工作

預設會停用必要的SMB簽署。您可以隨時啟用或停用所需的SMB簽署。

在下列情況下、預設不會停用SMB簽署：

1. 啟用必要的SMB簽署、叢集將還原為ONTAP 不支援SMB簽署的版本。
2. 叢集隨後會升級至ONTAP 支援SMB簽署的版本的支援。

   在這種情況下、原本設定在支援版本ONTAP 的支援版本上的SMB簽署組態會透過還原及後續升級來保留。

當您設定儲存虛擬機器（ SVM ）災難恢復關係時、您為選取的值 `-identity-preserve` 的選項 `snapmirror create` 命令可決定在目的地 SVM 中複寫的組態詳細資料。

如果您設定 `-identity-preserve` 選項 `true` （ ID-preserve ）、 SMB 簽署安全性設定會複寫到目的地。

如果您設定 `-identity-preserve` 選項 `false` （非 ID-preserve ）、 SMB 簽署安全性設定不會複寫到目的地。在此情況下、目的地上的CIFS伺服器安全性設定會設為預設值。如果您已在來源SVM上啟用必要的SMB簽署、則必須在目的地SVM上手動啟用必要的SMB簽署。

步驟

1. 執行下列其中一項動作：

| 如果您想要**SMB**簽署... | 輸入命令... |
| --- | --- |
| 已啟用 | `vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required true` |
| 已停用 | `vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required false` |

2. 判斷中的值是否已啟用或停用必要的 SMB 簽署 `Is Signing Required` 下列命令輸出中的欄位設定為所需的值： `vserver cifs security show -vserver` *`vserver_name`* `-fields is-signing-required`

範例

下列範例可為SVM VS1啟用必要的SMB簽署：

```
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
```

對加密設定的變更會對新連線生效。現有連線不受影響。

相關資訊

- "SnapMirror建立"

## 判斷 ONTAP SMB 工作階段是否已簽署

您可以在CIFS伺服器上顯示連線SMB工作階段的相關資訊。您可以使用此資訊來判斷SMB工作階段是否已簽署。這有助於判斷SMB用戶端工作階段是否與所需的安全性設定連線。

步驟

1. 執行下列其中一項動作：

| 如果您想要顯示有關...的資訊 | 輸入命令... |
| --- | --- |
| 指定儲存虛擬機器（SVM）上的所有簽署工作階段 | `vserver cifs session show -vserver vserver_name -is-session-signed true` |
| 在SVM上具有特定工作階段ID的已簽署工作階段詳細資料 | `vserver cifs session show -vserver vserver_name -session-id integer -instance` |

範例

下列命令會顯示SVM VS1上已簽署工作階段的相關工作階段資訊。預設的摘要輸出不會顯示「Is Session Signed」（已簽署的工作階段）輸出欄位：

```
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
```

下列命令會在工作階段ID為2的SMB工作階段上顯示詳細的工作階段資訊、包括工作階段是否已簽署：

```
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
```

相關資訊

監控SMB簽署的工作階段統計資料

## 監控 ONTAP SMB 簽署的工作階段統計資料

### 您可以監控SMB工作階段統計資料、並判斷哪些已建立的工作階段已簽署、哪些尚未簽署。

關於這項工作

。 `statistics` 進階權限層級的命令提供 `signed_sessions` 可用來監控已簽署 SMB 工作階段數量的計數器。。 `signed_sessions` 下列統計資料物件可使用計數器：

- `cifs` 可讓您監控所有 SMB 工作階段的 SMB 簽署。
- `smb1` 可讓您監控 SMB 1.0 工作階段的 SMB 簽署。
- `smb2` 可讓您監控 SMB 2.x 和 SMB 3.0 工作階段的 SMB 簽署。

  的輸出中包含 SMB 3.0 統計資料 `smb2` 物件：

如果您想要比較已簽署工作階段的數目與工作階段總數、您可以比較的輸出 `signed_sessions` 以的輸出進行計數 `established_sessions` 計數器。

您必須先開始收集統計資料樣本、才能檢視結果資料。如果不停止資料收集、您可以檢視範例中的資料。停止資料收集可提供固定的範例。不停止資料收集可讓您取得更新的資料、以便與先前的查詢進行比較。這項比較可協助您識別趨勢。

步驟

1. 將權限等級設為進階：
   `set -privilege advanced`
2. 開始資料收集：+ `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]`

   如果您未指定 `-sample-id` 參數、命令會為您產生範例識別碼、並將此範例定義為 CLI 工作階段的預設範例。的價值 `-sample-id` 為文字字串。如果您在相同的CLI工作階段中執行此命令、但未指定 `-sample-id` 參數時、命令會覆寫先前的預設範例。

   您可以選擇性地指定要收集統計資料的節點。如果您未指定節點、範例會收集叢集中所有節點的統計資料。

   如"指令參考資料ONTAP"需詳細 `statistics start`資訊，請參閱。
3. 使用 `statistics stop` 停止收集樣本資料的命令。

   詳細了解 `statistics stop`在"指令參考資料ONTAP" 。
4. 檢視SMB簽署統計資料：

| 如果您要檢視下列項目的資訊... | 輸入... |
| --- | --- |
| 已簽署的工作階段 | `show -sample-id sample_ID -counter signed_sessions |
| *node_name* [-node *node_name*]` | 已簽署的工作階段和已建立的工作階段 |
| `show -sample-id *sample_ID* -counter signed_sessions | established_sessions |

   如果您只想顯示單一節點的資訊、請指定選用項目 `-node` 參數。

   如"指令參考資料ONTAP"需詳細 `statistics show`資訊，請參閱。
5. 返回管理權限層級：
   `set -privilege admin`

範例

以下範例說明如何監控儲存虛擬機器（SVM）VS1上的SMB 2.x和SMB 3.0簽署統計資料。

下列命令會移至進階權限層級：

```
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
```

下列命令會啟動新範例的資料收集：

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

下列命令會停止範例的資料收集：

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

下列命令會顯示已簽署的SMB工作階段、以及範例中各節點所建立的SMB工作階段：

```
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
```

以下命令顯示節點2的簽署SMB工作階段：

```
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
```

下列命令會移回管理權限層級：

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

相關資訊

- 判斷SMB工作階段是否已簽署
- "效能監控與管理總覽"

# 在SMB伺服器上設定必要的SMB加密、以便透過SMB傳輸資料

## 瞭解 ONTAP SMB 加密

SMB加密可在SMB伺服器上啟用或停用SMB資料傳輸功能、是一項安全性增強功能。您也可以透過共用內容設定、逐一設定所需的SMB加密設定。

根據預設、當您在儲存虛擬機器（ SVM ）上建立 SMB 伺服器時、 SMB 加密會停用。您必須讓IT能夠充分利用SMB加密所提供的增強安全性。

若要建立加密的SMB工作階段、SMB用戶端必須支援SMB加密。從Windows Server 2012和Windows 8開始的Windows用戶端支援SMB加密。

SVM上的SMB加密可透過兩種設定加以控制：

- SMB 伺服器安全選項、可在 SVM 上啟用功能
- SMB 共用屬性，可依每個共用區設定 SMB 加密設定

您可以決定是否需要加密才能存取SVM上的所有資料、或是需要SMB加密才能存取所選共用區中的資料。SVM層級的設定會取代共用層級的設定。

有效的SMB加密組態取決於兩項設定的組合、如下表所述：

| 啟用**SMB**伺服器**SMB**加密 | 共用加密資料設定已啟用 | 伺服器端加密行為 |
| --- | --- | --- |
| 是的 | 錯 | SVM中的所有共用都啟用伺服器層級加密。有了這項組態、整個SMB工作階段就會進行加密。 |
| 是的 | 是的 | 無論共用層級加密為何、SVM中的所有共用都會啟用伺服器層級加密。有了這項組態、整個SMB工作階段就會進行加密。 |
| 錯 | 是的 | 特定共用區已啟用共用層級加密。使用此組態、即可從樹狀結構連線進行加密。 |
| 錯 | 錯 | 未啟用加密。 |

不支援加密的 SMB 用戶端無法連線至需要加密的 SMB 伺服器或共用區。

對加密設定的變更會對新連線生效。現有連線不受影響。

## 瞭解 **ONTAP SMB** 加密對效能的影響

### 當SMB工作階段使用SMB加密時、所有往返Windows用戶端的SMB通訊都會受到效能影響、影響用戶端和伺服器（亦即叢集上執行SVM的節點、其中包含SMB伺服器）。

效能影響顯示用戶端和伺服器的CPU使用量增加、不過網路流量並未改變。

效能影響的程度取決於ONTAP 您所執行的版本的VMware®。從推出全新的加密卸載演算法、即可在ONTAP 加密的SMB流量中提供更好的效能。啟用SMB加密時、預設會啟用SMB加密卸載。

增強的SMB加密效能需要AES-NI卸載功能。請參閱Hardware Universe 《支援資料》（HWU）、確認您的平台是否支援AES-NI卸載。

如果您能夠使用支援速度更快的 GCM 演算法的 SMB 版本 3.11 、也可以進一步改善效能。

視您的網路ONTAP 、支援的版本為VMware、SMB版本及SVM實作而定、SMB加密的效能影響可能會有很大差異、您只能在網路環境中進行測試來驗證。

SMB加密在SMB伺服器上預設為停用。您只能在需要加密的SMB共用區或SMB伺服器上啟用SMB加密。藉由SMB加密、ONTAP 支援進一步處理解密要求、並加密每個要求的回應。因此、只有在必要時才應啟用SMB加密。

## 啟用或停用傳入流量的 **ONTAP SMB** 加密

### 如果您想為傳入的SMB流量要求SMB加密、可以在CIFS伺服器或共用層級啟用SMB加密。根據預設、不需要SMB加密。

關於這項工作

您可以在CIFS伺服器上啟用SMB加密、此功能適用於CIFS伺服器上的所有共用。如果您不希望CIFS伺服器上的所有共用都需要SMB加密、或是想要針對每個共用區的傳入SMB流量啟用必要的SMB加密、可以停用CIFS伺服器上所需的SMB加密。

當您設定儲存虛擬機器（ SVM ）災難恢復關係時、您為選取的值 `-identity-preserve` 的選項 `snapmirror create` 命令可決定在目的地 SVM 中複寫的組態詳細資料。

如果您設定 `-identity-preserve` 選項 `true` （ ID-preserve ）、 SMB 加密安全性設定會複寫到目的地。

如果您設定 `-identity-preserve` 選項 `false` （非 ID-preserve ）、 SMB 加密安全性設定不會複寫到目的地。在此情況下、目的地上的CIFS伺服器安全性設定會設為預設值。如果您已在來源SVM上啟用SMB加密、則必須在目的地上手動啟用CIFS伺服器SMB加密。

步驟

1. 執行下列其中一項動作：

| 如果您想要**CIFS**伺服器上傳入**SMB**流量的**SMB**加密功能**...** | 輸入命令**...** |
| --- | --- |
| 已啟用 | `vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required true` |

| 如果您想要CIFS伺服器上傳入SMB流量的SMB加密功能... | 輸入命令... |
| --- | --- |
| 已停用 | `vserver cifs security modify -vserver vserver_name -is-smb-encryption -required false` |

2. 確認 CIFS 伺服器上所需的 SMB 加密已視需要啟用或停用： `vserver cifs security show -vserver vserver_name -fields is-smb-encryption-required`

   。 `is-smb-encryption-required` 欄位隨即顯示 `true` 如果需要、會在 CIFS 伺服器和上啟用 SMB 加密 `false` 如果已停用。

範例

下列範例為SVM VS1上的CIFS伺服器啟用必要的SMB加密功能：

```
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
```

相關資訊

- "SnapMirror建立"

## 判斷用戶端是否使用加密的 ONTAP SMB 工作階段連線

您可以顯示連線SMB工作階段的相關資訊、以判斷用戶端是否使用加密的SMB連線。這有助於判斷SMB用戶端工作階段是否與所需的安全性設定連線。

關於這項工作

SMB用戶端工作階段可以有三種加密層級之一：

- `unencrypted`

  SMB工作階段未加密。未設定儲存虛擬機器（SVM）層級或共用層級的加密。

- `partially-encrypted`

  當樹狀結構連線發生時、會啟動加密。已設定共用層級加密。未啟用SVM層級的加密。

- `encrypted`

  SMB工作階段已完全加密。已啟用SVM層級的加密。共用層級加密可能已啟用、也可能未啟用。SVM層級

的加密設定會取代共用層級的加密設定。

步驟

1. 執行下列其中一項動作：

| 如果您想要顯示有關...的資訊 | 輸入命令... |
| --- | --- |
| 針對指定SVM上的工作階段、具有指定加密設定的工作階段 | `vserver cifs session show -vserver *vserver_name* {unencrypted |
| partially-encrypted | encrypted} -instance` |
| 指定SVM上特定工作階段ID的加密設定 | `vserver cifs session show -vserver *vserver_name* -session-id *integer* -instance` |

範例

下列命令會在工作階段ID為2的SMB工作階段上顯示詳細的工作階段資訊、包括加密設定：

```
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
```

## 監控 **ONTAP SMB** 加密統計資料

您可以監控SMB加密統計資料、並判斷哪些已建立的工作階段和共用連線已加密、哪些尚未加密。

關於這項工作

。 `statistics` 進階權限層級的命令會提供下列計數器、您可以使用這些計數器來監控加密的 SMB 工作階段數目及共用連線：

| 計數器名稱 | 說明 |
| --- | --- |
| `encrypted_sessions` | 提供加密的SMB 3.0工作階段數量 |
| `encrypted_share_connections` | 提供樹狀結構連線所在的加密共用數 |
| `rejected_unencrypted_sessions` | 提供因缺乏用戶端加密功能而遭拒的工作階段設定數 |
| `rejected_unencrypted_shares` | 提供因缺乏用戶端加密功能而遭拒的共用對應數目 |

這些計數器可與下列統計資料物件一起使用：

- `cifs` 可讓您監控所有 SMB 3.0 工作階段的 SMB 加密。

  的輸出中包含 SMB 3.0 統計資料 `cifs` 物件： 如果您想要比較加密工作階段的數目與工作階段總數、可以比較的輸出 `encrypted_sessions` 以的輸出進行計數 `established_sessions` 計數器。

  如果您要比較加密共用連線的數目與共用連線的總數、可以比較的輸出 `encrypted_share_connections` 以的輸出進行計數 `connected_shares` 計數器。

- `rejected_unencrypted_sessions` 提供嘗試建立 SMB 工作階段的次數、該工作階段需要從不支援 SMB 加密的用戶端進行加密。
- `rejected_unencrypted_shares` 提供嘗試連線至 SMB 共用的次數、該共用需要來自不支援 SMB 加密的用戶端進行加密。

您必須先開始收集統計資料樣本、才能檢視結果資料。如果不停止資料收集、您可以檢視範例中的資料。停止資料收集可提供固定的範例。不停止資料收集可讓您取得更新的資料、以便與先前的查詢進行比較。這項比較可協助您識別趨勢。

步驟

1. 將權限等級設為進階：
   `set -privilege advanced`
2. 開始資料收集：+ `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   如果您未指定 `-sample-id` 參數、命令會為您產生範例識別碼、並將此範例定義為 CLI 工作階段的預設範例。的價值 `-sample-id` 為文字字串。如果您在相同的CLI工作階段中執行此命令、但未指定 `-sample-id` 參數時、命令會覆寫先前的預設範例。

   您可以選擇性地指定要收集統計資料的節點。如果您未指定節點、範例會收集叢集中所有節點的統計資料。

   如"指令參考資料ONTAP"需詳細 `statistics start`資訊，請參閱。

3. 使用 `statistics stop` 停止收集樣本資料的命令。

詳細了解 `statistics stop`在"指令參考資料ONTAP" 。

4. 檢視SMB加密統計資料：

| 如果您要檢視下列項目的資訊... | 輸入... |
| --- | --- |
| 加密工作階段 | `show -sample-id *sample_ID* -counter encrypted_sessions |
| *node_name* [-node *node_name*]` | 加密的工作階段和已建立的工作階段 |
| `show -sample-id *sample_ID* -counter encrypted_sessions | established_sessions |
| *node_name* [-node *node_name*]` | 加密的共用連線 |
| `show -sample-id *sample_ID* -counter encrypted_share_connections | *node_name* [-node *node_name*]` |
| 加密的共用連線和連線共用 | `show -sample-id *sample_ID* -counter encrypted_share_connections |
| connected_shares | *node_name* [-node *node_name*]` |
| 拒絕未加密的工作階段 | `show -sample-id *sample_ID* -counter rejected_unencrypted_sessions |
| *node_name* [-node *node_name*]` | 拒絕未加密的共用連線 |
| `show -sample-id *sample_ID* -counter rejected_unencrypted_share | *node_name* [-node *node_name*]` |

如果您只想顯示單一節點的資訊、請指定選用項目 `-node` 參數。

如"指令參考資料ONTAP"需詳細 `statistics show`資訊，請參閱。

5. 返回管理權限層級：
`set -privilege admin`

範例

以下範例說明如何監控儲存虛擬機器（SVM）VS1上的SMB 3.0加密統計資料。

下列命令會移至進階權限層級：

```
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
```

下列命令會啟動新範例的資料收集：

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

下列命令會停止該範例的資料收集：

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

下列命令顯示節點從範例中所建立的加密SMB工作階段和已建立的SMB工作階段：

```
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
```

下列命令顯示節點從範例中拒絕的未加密SMB工作階段數目：

```
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.
```

下列命令顯示範例中節點所連線的SMB共用數和加密的SMB共用數：

```
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.
```

下列命令顯示節點從範例中拒絕的未加密SMB共用連線數目：

```
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.
```

相關資訊

- 確定伺服器上可用的統計資料、物件和計數器
- "效能監控與管理總覽"

# 安全的LDAP工作階段通訊

## 瞭解 ONTAP SMB LDAP 簽署與封裝

從ONTAP 功能支援功能支援功能支援功能支援功能、從功能支援功能支援功能升級至功能性管理功能。您必須在儲存虛擬機器（SVM）上設定CIFS伺服器安全性設定、以對應於LDAP伺服器上的設定。

簽署可確認LDAP有效負載資料使用秘密金鑰技術的完整性。「密封」會加密LDAP有效負載資料、以避免以純文字傳輸敏感資訊。「*LDAP*安全性層級」選項會指出LDAP流量是否需要簽署、簽署及密封、或兩者皆不需要。預設值為 `none`。

在 SVM 上啟用 CIFS 流量的 LDAP 簽署與密封功能 `-session-security-for-ad-ldap` 選項 `vserver cifs security modify` 命令。

## 在 ONTAP SMB 伺服器上啟用 LDAP 簽署和密封

CIFS伺服器必須先修改CIFS伺服器安全性設定、才能使用簽署和密封功能與Active Directory LDAP伺服器進行安全通訊。

開始之前

您必須洽詢AD伺服器管理員、以判斷適當的安全性組態值。

步驟

1. 設定 CIFS 伺服器安全性設定、以啟用 Active Directory LDAP 伺服器的簽署和密封流量： `vserver cifs`

```
security modify -vserver vserver_name -session-security-for-ad-ldap
{none|sign|seal}
```

您可以啟用簽署 (`sign`、資料完整性）、簽署及密封 (`seal`或兩者皆非 `none`、無簽署或密封）。預設值為 `none`。

2. 確認 LDAP 簽署與密封安全設定已正確設定： `vserver cifs security show -vserver vserver_name`

> 如果 SVM 使用相同的 LDAP 伺服器來查詢名稱對應或其他 UNIX 資訊、例如使用者、群組和網路群組、則必須使用啟用對應的設定 `-session-security` 的選項 `vserver services name-service ldap client modify` 命令。

## 設定LDAP over TLS

### 匯出 ONTAP SMB SVM 的自我簽署根 CA 憑證

若要使用LDAP over SSL/TLS來保護Active Directory通訊安全、您必須先將Active Directory憑證服務的自我簽署根CA憑證複本匯出至憑證檔案、然後將其轉換成Ascii文字檔。這個文字檔是ONTAP 由SITALL用來在儲存虛擬機器（SVM）上安裝憑證。

#### 開始之前

Active Directory憑證服務必須已針對CIFS伺服器所屬的網域進行安裝和設定。如需安裝及設定Active Director憑證服務的相關資訊、請參閱Microsoft TechNet程式庫。

"Microsoft TechNet程式庫：technet.microsoft.com"

#### 步驟

1. 取得中網域控制站的根 CA 憑證 `.pem` 文字格式。

   "Microsoft TechNet程式庫：technet.microsoft.com"

#### 完成後

在SVM上安裝憑證。

#### 相關資訊

"Microsoft TechNet程式庫"

### 在 ONTAP SMB SVM 上安裝自我簽署的根 CA 憑證

如果在連結至LDAP伺服器時需要使用TLS進行LDAP驗證、您必須先在SVM上安裝自我簽署的根CA憑證。

#### 關於這項工作

ONTAP 中所有使用 TLS 通訊的應用程式，都可以使用線上憑證狀態傳輸協定（ OCSP ）來檢查數位憑證狀態。如果在TLS上為LDAP啟用OCSP、則撤銷的憑證會遭到拒絕、連線也會失敗。

#### 步驟

1. 安裝自我簽署的根CA憑證：
   a. 開始安裝憑證： `security certificate install -vserver vserver_name -type server-ca`

      主控台輸出會顯示下列訊息： `Please enter Certificate: Press <Enter> when done`

   b. 開啟憑證 `.pem` 使用文字編輯器檔案、複製憑證、包括開頭的行 `-----BEGIN CERTIFICATE-----` 並以結束 `-----END CERTIFICATE-----`，然後在命令提示字元之後貼上憑證。
   c. 確認已正確顯示憑證。
   d. 按Enter完成安裝。
2. 確認已安裝憑證： `security certificate show -vserver vserver_name`

相關資訊

- "安全性憑證安裝"
- "安全證書展示"

### 在 **ONTAP SMB** 伺服器上啟用 **LDAP over TLS**

## 您的SMB伺服器必須先修改SMB伺服器安全性設定、才能使用TLS與Active Directory LDAP伺服器進行安全通訊。

從ONTAP 《支援範圍》9.10.1開始、Active Directory（AD）和名稱服務LDAP連線預設都支援LDAP通道繫結。僅當啟用Start-TLS或LDAPS並將工作階段安全性設定為簽署或密封時、才能嘗試透過LDAP連線進行通道繫結。ONTAP若要停用或重新啟用與 AD 伺服器的 LDAP 通道繫結、請使用 `-try-channel-binding-for-ad-ldap` 參數 `vserver cifs security modify` 命令。

若要深入瞭解、請參閱：

- "了解適用於 ONTAP NFS SVM 的 LDAP"
- "2020 LDAP通道繫結和LDAP簽署要求、適用於Windows"。

步驟

1. 設定 SMB 伺服器安全性設定、以允許與 Active Directory LDAP 伺服器進行安全的 LDAP 通訊： `vserver cifs security modify -vserver vserver_name -use-start-tls-for-ad-ldap true`
2. 確認 LDAP over TLS 安全性設定已設定為 `true`： `vserver cifs security show -vserver vserver_name`

> 如果 SVM 使用相同的 LDAP 伺服器來查詢名稱對應或其他 UNIX 資訊（例如使用者、群組和網路群組）、則您也必須修改 `-use-start-tls` 選項：使用 `vserver services name-service ldap client modify` 命令。