保護您的網路安全
ONTAP 9

NetApp
February 12, 2026

目錄

保護您的網路安全

使用 FIPS 為所有 SSL 連線設定 ONTAP 網路安全性

ONTAP 的所有 SSL 連線均符合聯邦資訊處理標準 (FIPS) 140-2。您可以開啟和關閉 SSL FIPS 模式，全域設定 SSL 協議，並關閉ONTAP中的任何弱密碼。

根據預設， ONTAP 上的 SSL 設為停用 FIPS 相容性，並啟用下列 TLS 通訊協定：

- TLSv1.3 （從 ONTAP 9.11.1 開始）
- TLSv1.2

先前的 ONTAP 版本預設啟用下列 TLS 通訊協定：

- TLSv1.1 （從 ONTAP 9.12.1 開始預設為停用）
- TLSv1 （從 ONTAP 9.8 開始預設為停用）

啟用SSL FIPS模式時、ONTAP 從靜止到外部用戶端或ONTAP 伺服器元件的SSL通訊、將使用FIPS相容的SSL加密。

如果您想要系統管理員帳戶使用SSH公開金鑰來存取SVM、則必須先確認主機金鑰演算法受到支援、才能啟用SSL FIPS模式。

附註： ONTAP 主機金鑰演算法支援已在更新版本的版本中變更。

發行版ONTAP	支援的金鑰類型	不支援的金鑰類型
9.11.1 及更新版本	ECDSA-SHA2-nistp256	RSA-SHA2-512 RSA-SHA2-256 SSH-ed25519 SSH-DSS SSH-RSA
9.10.1及更早版本	ECDSA-SHA2-nistp256 SSH-ed25519.	SSH-DSS SSH-RSA

沒有支援金鑰演算法的現有SSH公開金鑰帳戶、必須先以支援的金鑰類型重新設定、才能啟用FIPS、否則系統管理員驗證將會失敗。

如需詳細資訊、請參閱 "啟用SSH公開金鑰帳戶"。

ONTAP 9.18.1 引入了對 ML-KEM、ML-DSA 和 SLH-DSA 後量子計算加密演算法的支持，用於 SSL，從而為抵禦未來潛在的量子電腦攻擊提供了額外的安全保障。這些演算法僅在以下情況下可用FIPS 已停用。當 FIPS 被停用且對等方支援時，將協商後量子加密演算法。

啟用 FIPS

建議所有安全的使用者在系統安裝或升級之後、立即調整其安全組態。啟用SSL FIPS模式時、ONTAP 從靜止到

外部用戶端或ONTAP 伺服器元件的SSL通訊、將使用FIPS相容的SSL加密。

啟用FIPS時、您無法安裝或建立RSA金鑰長度為4096的憑證。

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 啟用 FIPS ：

   ```
   security config modify * -is-fips-enabled true
   ```

3. 當系統提示您繼續時、請輸入 `y`

4. 從ONTAP 9.9.1 開始，不需要重新啟動。如果您執行的是ONTAP 9.8 或更早版本，請手動逐一重新啟動叢集中的每個節點。

範例

如果您執行ONTAP 的是更新版本的版本、則不會看到警告訊息。

```
security config modify -is-fips-enabled true

Warning: This command will enable FIPS compliance and can potentially
cause some non-compliant components to fail. MetroCluster and Vserver DR
require FIPS to be enabled on both sites in order to be compatible.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

如"指令參考資料ONTAP"需有關及 SSL FIPS 模式組態的詳細 `security config modify`資訊，請參閱。

停用FIPS

從ONTAP 9.18.1 開始， ONTAP中的 SSL 支援 ML-KEM、ML-DSA 和 SLH-DSA 後量子計算加密演算法。只有在禁用 FIPS 且對等方支援這些演算法時，這些演算法才可用。

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 輸入下列命令來停用FIPS：

   ```
   security config modify -is-fips-enabled false
   ```

3. 當系統提示您繼續時、請輸入 `y`。
4. 從ONTAP 9.9.1 開始，不需要重新啟動。如果您執行的是ONTAP 9.8 或更早版本，請手動重新啟動叢集中的每個節點。

如果您需要使用 SSLv3 協議，則必須依照上述步驟停用 FIPS。只有在停用 FIPS 的情況下才能啟用 SSLv3。

您可以使用以下命令啟用 SSLv3。如果您執行的是ONTAP 9.9.1 或更高版本，則不會看到此警告訊息。

```
security config modify -supported-protocols SSLv3

Warning: Enabling the SSLv3 protocol may reduce the security of the
interface, and is not recommended.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

檢視**FIPS**法規遵循狀態

您可以查看整個叢集是否正在執行目前的安全性組態設定。

步驟

1. 如果您執行的是ONTAP 9.8 或更早版本，請手動逐一重新啟動叢集中的每個節點。
2. 檢視目前的法規遵循狀態：

   ```
   security config show
   ```

```
cluster1::> security config show
Cluster    Supported
FIPS Mode  Protocols Supported Cipher Suites
---------- ---------
-----------------------------------------------------------
false      TLSv1.3,  TLS_RSA_WITH_AES_128_CCM,
TLS_RSA_WITH_AES_128_CCM_8,
           TLSv1.2   TLS_RSA_WITH_AES_128_GCM_SHA256,
                     TLS_RSA_WITH_AES_128_CBC_SHA,
                     TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_256_CCM,
                     TLS_RSA_WITH_AES_256_CCM_8,
                     ...
```

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

相關資訊

- "FIPS 203：基於模組格的金鑰封裝機制標準（ML-KEM）"
- "FIPS 204：基於模組格的數位簽章標準（ML-DSA）"
- "FIPS 205：無狀態雜湊數位簽章標準 (SLH-DSA)"

設定 IPsec 在線上加密

準備在 ONTAP 網路上使用 IP 安全性

從 ONTAP 9 8 開始，您可以選擇使用 IP 安全性（ IPsec ）來保護網路流量。IPsec 是 ONTAP 提供的數種資料傳輸或傳輸中加密選項之一。在正式作業環境中使用 IPsec 之前，您應該做好設定的準備。

ONTAP 中的 IP 安全實作

IPsec 是由 IETF 維護的網際網路標準。它提供資料加密與完整性，以及 IP 層級網路端點之間流量傳輸的驗證。

使用 ONTAP 時， IPsec 可保護 ONTAP 和各種用戶端之間的所有 IP 流量，包括 NFS ， SMB 和 iSCSI 傳輸協定。除了隱私權和資料完整性之外，網路流量還能防範多種攻擊，例如重播和攔截式攻擊。ONTAP 使用 IPsec 傳輸模式實作。它利用網際網路金鑰交換（ IKE） 傳輸協定第 2 版，在 ONTAP 和使用 IPv4 或 IPv6 的用戶端之間協商金鑰資料。

當叢集上啟用 IPsec 功能時，網路需要 ONTAP 安全性原則資料庫（ SPD ）中的一或多個項目，才能符合各種流量特性。這些項目會對應至處理及傳送資料所需的特定保護詳細資料（例如密碼套件和驗證方法）。每個用戶端也需要對應的 SPD 項目。

對於某些類型的流量，最好使用另一個資料傳輸加密選項。例如，對於 NetApp SnapMirror 和叢集對等流量的加密，一般建議使用傳輸層安全性（ TLS ）傳輸協定，而非 IPsec 。這是因為 TLS 在大多數情況下都能提供更好的效能。

相關資訊

- "網際網路工程工作團隊"
- "RFC 4301-Security Architecture for the Internet Protocol （網際網路傳輸協定的安全架構）"

ONTAP IPsec 實作的演進

IPsec 最初是在ONTAP 9.8 中引入的。該實現在後續ONTAP版本中不斷發展，如下所述。

ONTAP 9.18.1

IPsec硬體卸載支援已擴展到IPv6流量。

ONTAP 9.17.1

IPsec 硬體卸載支援擴充至"鏈路聚合組" 。"後量子預共享密鑰（PPK）"支援 IPsec 預共用金鑰 (PSK) 驗證。

ONTAP 9.16.1.

加密和完整性檢查等多項密碼編譯作業可卸載至支援的 NIC 卡。如需詳細資訊、請參閱 IPsec 硬體卸載功能 。

ONTAP 9.12.1

MetroCluster IP 和 MetroCluster 網路附加組態提供 IPsec 前端主機傳輸協定支援。MetroCluster 叢集所提供的 IPsec 支援僅限於前端主機流量， MetroCluster 叢集間的生命體不受支援。

零點**9.10.1 ONTAP**

除了 PSK 之外，憑證還可用於 IPsec 驗證。在ONTAP 9.10.1 之前的版本中，僅支援使用 PSK 進行身份驗證。

部分**9.9.1 ONTAP**

IPsec 使用的加密演算法已通過 FIPS 140-2 驗證。這些演算法由 ONTAP 中的 NetApp 密碼編譯模組處理，該模組執行 FIPS 140-2 驗證。

部分**9.8 ONTAP**

根據傳輸模式實作， IPsec 的支援一開始就可用。

IPsec 硬體卸載功能

如果您使用的是 ONTAP 9 。 16.1 或更新版本，您可以選擇將某些運算密集的作業（例如加密和完整性檢查）卸載到儲存節點上安裝的網路介面控制器（ NIC ）卡。卸載到 NIC 卡的作業處理量約為 5% 或更低。這可大幅改善受 IPsec 保護的網路流量的效能和處理量。

要求與建議

在使用 IPsec 硬體卸載功能之前，您應該考量幾項需求。

支援的乙太網路卡

您只需安裝並使用受支援的乙太網路卡。從ONTAP 9.16.1 開始，支援以下乙太網路卡：

- X50131A （ 2p ， 40G/100g/200g/400G 乙太網路控制器）
- X60132A （ 4p ， 10G/25G 乙太網路控制器）

ONTAP 9.17.1 增加了對以下乙太網路卡的支援：

- X50135A（2p，40G/100G乙太網路控制器）
- X60135A（2p，40G/100G乙太網路控制器）

以下平台支援 X50131A 和 X50135A 卡：

- ASA A1K
- ASA A90
- ASA A70
- AFF A1K
- AFF A90
- AFF A70

以下平台支援 X60132A 和 X60135A 卡：

- ASA A50
- ASA A30
- ASA A20
- AFF A50
- AFF A30
- AFF A20

查看"NetApp Hardware Universe"有關支援的平台和卡片的更多資訊。

叢集範圍

IPsec 硬體卸載功能是針對叢集進行全域設定。例如，此命令會 `security ipsec config`套用至叢集中的所有節點。

一致的組態

支援的 NIC 卡應安裝在叢集中的所有節點上。如果支援的 NIC 卡只能在某些節點上使用，則當容錯移轉後，如果部分生命負載未裝載於具有卸載功能的 NIC 上，您就會發現效能大幅降低。

停用反重播

您必須停用 ONTAP （預設組態）和 IPsec 用戶端上的 IPsec 反重新執行保護。如果未停用，將不支援分割和多重路徑（備援路由）。

如果 ONTAP IPsec 組態已從預設變更為啟用反重新執行保護，請使用此命令將其停用：

```
security ipsec config modify -replay-window 0
```

您必須確定用戶端上的 IPsec 反重新執行保護已停用。請參閱用戶端的 IPsec 文件，以停用反重播保護。

限制

在使用 IPsec 硬體卸載功能之前，您應該考慮幾項限制。

IPv6

從ONTAP 9.18.1 開始，IPsec 硬體卸載功能支援 IPv6。在ONTAP 9.18.1 之前的版本中，IPsec 硬體卸載不支援 IPv6。

延伸序號

硬體卸載功能不支援 IPsec 延伸序列號。僅使用正常的 32 位元序列號。

連結集合體

從ONTAP 9.17.1 開始，您可以將 IPsec 硬體卸載功能與"鏈路聚合組" 。

在 9.17.1 之前的版本中，IPsec 硬體卸載功能不支援連結聚合。它不能與通過 `network port ifgrp` ONTAP CLI 中的指令。

ONTAP CLI 中的組態支援

ONTAP 9 。 16.1 中更新了三個現有的 CLI 命令，以支援以下所述的 IPsec 硬體卸載功能。如需詳細資訊，請參閱"在 ONTAP 中設定 IP 安全性"。

指令**ONTAP**	更新
`security ipsec config show`	布林參數 `Offload Enabled`顯示目前的 NIC 卸載狀態。
`security ipsec config modify`	此參數 `is-offload-enabled`可用於啟用或停用 NIC 卸載功能。
`security ipsec config show-ipsecsa`	新增了四個新的計數器，以位元組和封包顯示傳入和傳出流量。

ONTAP REST API 中的組態支援

ONTAP 9 中更新了兩個現有的 REST API 端點。 16.1 可支援 IPsec 硬體卸載功能，如下所述。

REST端點	更新
`/api/security/ipsec`	此參數 `offload_enabled`已新增，可透過修補方法使用。
`/api/security/ipsec/security_association`	新增兩個計數器值，以追蹤卸載功能處理的總位元組和封包數。

從 ONTAP 自動化文件中深入瞭解 ONTAP REST API ，包括 "ONTAP REST API 的新功能"。您也應該檢閱 ONTAP 自動化文件，以取得有關的詳細資訊 "IPsec 端點"。

相關資訊

- "安全 IPSEC"

設定 **ONTAP** 網路的 **IP** 安全性

在 ONTAP 叢集上設定及啟動 IPsec 進行中加密需要執行數項工作。

設定 IPsec 之前，請務必先檢閱"準備使用 IP 安全性"。例如，您可能需要決定是否使用以 ONTAP 9 開頭的可用 IPsec 硬體卸載功能。 16.1

在叢集上啟用**IPsec**

您可以在叢集上啟用 IPsec ，以確保資料在傳輸過程中持續加密且安全。

步驟

1. 探索是否已啟用IPsec：

   ```
   security ipsec config show
   ```

   如果結果包括 `IPsec Enabled: false`，繼續下一步。

2. 啟用IPsec：

   ```
   security ipsec config modify -is-enabled true
   ```

   您可以使用布爾參數來啟用 IPsec 硬體卸載功能 `is-offload-enabled`。

3. 再次執行探索命令：

   ```
   security ipsec config show
   ```

   現在的結果包括 `IPsec Enabled: true`。

準備使用憑證驗證建立 **IPsec** 原則

如果您只使用預先共用金鑰（ PSK ）進行驗證、而且不會使用憑證驗證、則可以略過此步驟。

在建立使用憑證進行驗證的 IPsec 原則之前、您必須確認符合下列先決條件：

- ONTAP 和用戶端都必須安裝另一方的 CA 憑證、以便雙方可驗證終端實體（ ONTAP 或用戶端）憑證
- 系統會為ONTAP 參與該原則的Sfor the Sfor the Sfor the Sfor the Sfor the Sfor the Sfor the Sfor the

> 可共享證書的產品。ONTAP不需要在憑證與lifs之間建立一對一對應關係。

步驟

1. 除非已安裝 ONTAP 憑證管理（例如 ONTAP 自我簽署的根 CA ）、否則請將在相互驗證期間使用的所有 CA 憑證（包括 ONTAP 端和用戶端 CA ）安裝到憑證管理。
   - 命令範例 *
     ```
     cluster::> security certificate install -vserver svm_name -type server-ca
     -cert-name my_ca_cert
     ```
2. 若要確保在驗證期間安裝的 CA 位於 IPsec CA 搜尋路徑內、請使用將 ONTAP 憑證管理 CA 新增至 IPsec 模組 `security ipsec ca-certificate add` 命令。
   - 命令範例 *
     ```
     cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
     my_ca_cert
     ```
3. 建立並安裝認證以供ONTAP 《Sfor the Suse LIF（供《Sfor the Suse：此憑證的發卡行CA必須已安裝ONTAP 至ESA並新增至IPsec。

◦ 命令範例 *

```
cluster::> security certificate install -vserver svm_name -type server -cert
-name my_nfs_server_cert
```

如需ONTAP 更多有關資訊、請參閱ONTAP 《》介紹文件中的安全認證命令。

定義安全性原則資料庫（**SPD**）

在允許流量在網路上傳輸之前、IPsec需要SPD項目。無論您使用的是用於驗證的PSK或憑證、都是如此。

步驟

1. 使用 `security ipsec policy create` 命令至：
   a. 選取ONTAP 要參與IPsec傳輸的IP位址或子網路。
   b. 選取要連線ONTAP 至「靜態IP位址」的用戶端IP位址。

      用戶端必須使用預先共用金鑰（PSK）來支援網際網路金鑰交換版本2（IKEv2）。

   c. 可選擇細粒度的流量參數，例如上層協定（UDP、TCP、ICMP 等）、本機連接埠號碼和遠端連接埠號，以保護流量。對應的參數如下 `protocols` ， `local-ports`和 `remote-ports`分別。

      跳過此步驟以保護ONTAP 所有介於整個過程中的資訊流量、例如：靜態IP位址和用戶端IP位址。保護所有流量是預設設定。

   d. 輸入的 PSK 或公開金鑰基礎架構（ PKI ） `auth-method` 所需驗證方法的參數。
      i. 如果您輸入一個 PSK 、請包含參數、然後按 <enter> 鍵提示您輸入並驗證預先共用金鑰。

         `local-identity`如果主機和用戶端都使用強化天鵝，而且沒有為主機或用戶端選取萬用字元原則，則和 `remote-identity`參數是選用的。

      ii. 如果您輸入 PKI 、也需要輸入 `cert-name`、 `local-identity`、 `remote-identity` 參數。如果遠端端憑證身分不明、或是需要多個用戶端身分識別、請輸入特殊身分識別 `ANYTHING`。
   e. 從ONTAP 9.17.1 開始，可以選擇輸入後量子預共享金鑰 (PPK) 身份 `ppk-identity`參數。 PPK提供了額外的安全保障，以抵禦未來潛在的量子電腦攻擊。輸入 PPK 身分時，系統會提示您輸入 PPK 金鑰。PPK僅支援 PSK 身份驗證。

詳細了解 `security ipsec policy create`在"指令參考資料ONTAP" 。

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

除非 ONTAP 和用戶端都設定了相符的 IPsec 原則、而且雙方都有驗證認證（可以是 PSK 或憑證）、否則 IP 流量無法在用戶端和伺服器之間傳輸。

使用**IPsec**身分識別

對於預先共用金鑰驗證方法、如果主機和用戶端都使用強化天鵝、而且沒有為主機或用戶端選取萬用字元原則、則本機和遠端身分識別是選用的。

對於公開密碼匙基礎建設/憑證驗證方法、本機和遠端身分識別都是必要的。身分識別會指定在每一方憑證中認證的身分識別、並用於驗證程序。如果遠端身分識別不明、或是可能有許多不同的身分識別、請使用特殊身分識別 `ANYTHING`。

關於這項工作

在不受限的情況下、可透過修改SPD項目或在SPD原則建立期間來指定身分識別。ONTAPSPD可以是IP位址或字串格式身分識別名稱。

步驟

1. 使用下列命令修改現有的 SPD 身分識別設定：

```
security ipsec policy modify
```

命令範例

```
security ipsec policy modify -vserver vs1 -name test34 -local-identity
192.168.134.34 -remote-identity client.fooboo.com
```

IPsec多個用戶端組態

當少數用戶端需要使用IPsec時、每個用戶端只需使用一個SPD項目就足夠了。但是、當數百甚至數千個用戶端需要使用IPsec時、NetApp建議使用IPsec多重用戶端組態。

關於這項工作

支援將多個網路上的多個用戶端連線至單一SVM IP位址、並啟用IPsec。ONTAP您可以使用下列其中一種方法來達成此目的：

- 子網路組態

  若要允許特定子網路上的所有用戶端（例如 192.168.134.0/24 ）使用單一 SPD 原則項目連線到單一 SVM IP 位址、您必須指定 `remote-ip-subnets` 子網路形式。此外、您必須指定 `remote-identity` 具有正確用戶端身分識別的欄位。

在子網路組態中使用單一原則項目時、該子網路中的IPsec用戶端會共用IPsec身分識別和預先共用金鑰（PSK）。不過、憑證驗證並不符合此要求。使用憑證時、每個用戶端都可以使用自己的唯一憑證或共用憑證進行驗證。IPsec會根據安裝在本機信任存放區上的CA來檢查憑證的有效性。ONTAP支援憑證撤銷清單（CRL）檢查。ONTAP

- 允許所有用戶端組態

  若要允許任何用戶端連線至 SVM IPsec 啟用的 IP 位址、無論其來源 IP 位址為何、請使用 `0.0.0.0/0` 指定時使用萬用字元 `remote-ip-subnets` 欄位。

  此外、您必須指定 `remote-identity` 具有正確用戶端身分識別的欄位。對於憑證驗證、您可以輸入 `ANYTHING`。

  此外、當 `0.0.0.0/0` 使用萬用字元時、您必須設定要使用的特定本機或遠端連接埠號碼。例如、 `NFS port 2049`。

  步驟

  a. 使用下列其中一個命令來設定多個用戶端的 IPsec 。

     i. 如果您使用 * 子網路組態 * 來支援多個 IPsec 用戶端：

     ```
     security ipsec policy create -vserver vserver_name -name policy_name
     -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets
     IP_address/subnet -local-identity local_id -remote-identity remote_id
     ```

     命令範例

     ```
     security ipsec policy create -vserver vs1 -name subnet134 -local-ip-subnets
     192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local-identity
     ontap_side_identity -remote-identity client_side_identity
     ```

     i. 如果您使用 * 允許所有用戶端組態 * 來支援多個 IPsec 用戶端：

     ```
     security ipsec policy create -vserver vserver_name -name policy_name
     -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local
     -ports port_number -local-identity local_id -remote-identity remote_id
     ```

  命令範例

  ```
  security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
  IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local
  -identity ontap_side_identity -remote-identity client_side_identity
  ```

顯示 **IPsec** 統計資料

透過協商、ONTAP 可在「穩定SVM IP位址」和「用戶端IP位址」之間建立稱為「IKE安全性關聯」（SA）的安全通道。兩個端點都安裝了IPsec SAS、以執行實際的資料加密與解密工作。您可以使用統計資料命令來檢查IPsec SAS和IKE SAS的狀態。

如果您使用 IPsec 硬體卸載功能，則會使用命令顯示數個新的計數器 `security ipsec config show-ipsecsa`。

命令範例

IKE SA命令範例：

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

IPsec SA命令和輸出範例：

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ----------------
-----------
vs1         test34
                   192.168.134.34  192.168.134.44  c764f9ee020cec69
ESTABLISHED
```

IPsec SA命令和輸出範例：

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
            Policy  Local           Remote          Inbound  Outbound
Vserver     Name    Address         Address         SPI      SPI
State
----------- ------- --------------- --------------- -------- --------
---------
vs1         test34
                    192.168.134.34  192.168.134.44  c4c5b3d6 c2515559
INSTALLED
```

相關資訊

- "安全性憑證安裝"
- "安全 IPSEC"

配置ONTAP後端集群網路加密

從ONTAP 9.18.1 開始，您可以為後端叢集網路上的傳輸中資料配置傳輸層安全性 (TLS) 加密。此加密技術可在後端叢集網路上的ONTAP節點之間傳輸客戶資料時，保護儲存在ONTAP中的客戶資料。

關於這項工作

- 後端集群網路加密預設為停用狀態。

- 啟用後端叢集網路加密後，儲存在ONTAP中的所有客戶資料在後端叢集網路上的ONTAP節點之間傳輸時都會被加密。集群網路的部分流量（例如控制路徑資料）未加密。
- 預設情況下，後端叢集網路加密將使用叢集中每個節點自動產生的憑證。你可以[管理集群網路加密證書]每個節點都使用自訂安裝的憑證。

開始之前

- 您必須是ONTAP管理員。 `admin`執行下列任務所需的權限等級。
- 叢集中的所有節點必須執行ONTAP 9.18.1 或更高版本才能啟用後端叢集網路加密。

啟用或停用叢集網路通訊加密

步驟

1. 查看目前集群網路加密狀態：

   ```
   security cluster-network show
   ```

   此命令顯示集群網路加密的目前狀態：

   ```
   Cluster-1::*> security cluster-network show

   Enabled: true

   Mode: tls

   Status: READY
   ```

2. 啟用或停用TLS後端叢集網路加密：

   ```
   security cluster-network modify -enabled <true|false>
   ```

   此命令啟用或停用後端叢集網路上客戶傳輸資料的加密通訊。

管理集群網路加密證書

1. 查看目前集群網路加密證書資訊：

   ```
   security cluster-network certificate show
   ```

   此命令顯示目前集群網路加密證書資訊：

```
security cluster-network certificate show
Node                  Certificate Name                       CA
--------------------- -------------------------------------
--------------
node1                 -                                      Cluster-
1_Root_CA
node2                 -                                      Cluster-
1_Root_CA
node3                 google_issued_cert1                    Google_CA1
node4                 google_issued_cert2                    Google_CA1
```

叢集中每個節點的憑證和憑證授權單位 (CA) 名稱均已顯示。

2. 修改節點的叢集網路加密證書：

```
security cluster-network certificate modify -node <node_name> -name
<certificate_name>
```

此指令修改特定節點的叢集網路加密證書。在執行此命令之前，必須先安裝憑證並由已安裝的 CA 進行簽署。有關證書管理的更多信息，請參閱"使用系統管理員管理 ONTAP 憑證"。如果 `-name`如果未指定，則使用自動產生的預設憑證。

在 ONTAP 網路中設定生命安全的防火牆原則

設定防火牆可增強叢集的安全性、並有助於防止未獲授權的存取儲存系統。根據預設、內建防火牆會設定為允許遠端存取特定的IP服務集、以供資料、管理及叢集間生命體使用。

從功能部分9.10.1開始ONTAP ：

- 防火牆原則已過時、並由LIF服務原則取代。之前、內建防火牆是使用防火牆原則來管理。此功能現在是使用LIF服務原則來完成。
- 所有的防火牆原則都是空的、而且不會開啟基礎防火牆中的任何連接埠。而是必須使用LIF服務原則開啟所有連接埠。
- 升級至9.10.1或更新版本、從防火牆原則轉換至LIF服務原則之後、不需要採取任何行動。系統會自動建構符合先前ONTAP 版本的防火牆原則的LIF服務原則。如果您使用指令碼或其他工具來建立及管理自訂防火牆原則、則可能需要升級這些指令碼、以建立自訂服務原則。

若要深入瞭解、請參閱 "更新版本中的生命與服務政策ONTAP"。

防火牆原則可用來控制對管理服務傳輸協定的存取、例如SSH、HTTP、HTTPS、Telnet、NTP、 NDMP、NDMPS、RSH、DNS或SNMP。無法為NFS或SMB等資料傳輸協定設定防火牆原則。

您可以使用下列方式來管理防火牆服務和原則：

- 啟用或停用防火牆服務

- 顯示目前的防火牆服務組態
- 使用指定的原則名稱和網路服務建立新的防火牆原則
- 將防火牆原則套用至邏輯介面
- 建立新的防火牆原則、該原則是現有原則的確切複本

  您可以使用這項功能、在同一個SVM中建立具有類似特性的原則、或將原則複製到不同的SVM。

- 顯示防火牆原則的相關資訊
- 修改防火牆原則所使用的IP位址和網路遮罩
- 刪除LIF未使用的防火牆原則

防火牆原則與生命

LIF防火牆原則是用來限制透過每個LIF存取叢集。您需要瞭解預設防火牆原則如何影響每種LIF類型的系統存取、以及如何自訂防火牆原則以提高或降低LIF的安全性。

使用 OR `network interface modify` 命令設定 LIF 時 `network interface create`，為參數指定的值會決定允許存取 LIF 的 `-firewall-policy`服務傳輸協定和 IP 位址。如"指令參考資料ONTAP"需詳細 `network interface`資訊，請參閱。

在許多情況下、您可以接受預設的防火牆原則值。在其他情況下、您可能需要限制特定IP位址和特定管理服務傳輸協定的存取。可用的管理服務傳輸協定包括SSH、HTTP、HTTPS、Telnet、NTP、 NDMP、NDMPS、RSH, DNS及SNMP。

所有叢集生命的防火牆原則預設為 `""` 且無法修改。

下表說明在ONTAP 建立LIF時指派給每個LIF的預設防火牆原則、具體取決於其角色（版本號為9.5或更早）或服務原則ONTAP （版本為9.6及更新版本）：

防火牆原則	預設服務傳輸協定	預設存取	LIF套用至
管理	DNS、http、https、NDMP、ndmps、 NTP、SNMP、ssh	任何位址（0.00.0.0/0）	叢集管理、SVM管理及節點管理生命里
MGMT-NFS	DNS、http、https、NDMP、ndmps、 NTP、portmap、SNMP、ssh	任何位址（0.00.0.0/0）	也支援SVM管理存取的資料生命量
叢集間	HTTPS、NDMP、ndmps	任何位址（0.00.0.0/0）	所有叢集間LIF
資料	DNS、NDMP、ndms、portmap	任何位址（0.00.0.0/0）	所有資料生命量

portmap服務組態

portmap服務會將RPC服務對應至其接聽的連接埠。

Portmap服務可在ONTAP 不間斷的情況下於更新版本中使用、ONTAP 從版本9.4到ONTAP 版本9.6均可設定、並從ONTAP 版本9.7開始自動管理。

- 在更新版本的版本中、連接埠對應服務（rpcbind）一律可在連接埠111上存取、因為網路組態必須仰賴內建的不只是第三方防火牆的功能。ONTAP ONTAP
- 從S得9.4到S得9.6、您可以修改防火牆原則、以控制portmap服務是否可在特定的生命期中存取。ONTAP ONTAP
- 從功能更新至功能更新至功能更新至功能更新至功能更新至功能更新。ONTAP而是會自動為所有支援NFS服務的LIF開啟portmap連接埠。
- Portmap服務可在ONTAP 防火牆內設定、範圍從版本9.4到ONTAP 版本9.6。*

本主題的其餘部分將討論如何設定ONTAP 從版本ONTAP 號至版本號之間的適用效能提升介面防火牆服務。

視組態而定、您可能無法在特定類型的生命期（通常是管理生命期和叢集間生命期）上存取服務。在某些情況下、您甚至可能無法存取資料生命期。

您可以期望的行為

從版本9.4到版本9.6的功能設計、可在升級時提供無縫轉換。ONTAP ONTAP如果已透過特定類型的lifs存取portmap服務、則可透過這些類型的lifs繼續存取。如同在 ONTAP 9.3 及更早版本中、您可以在 LIF 類型的防火牆原則中指定可在防火牆內存取的服務。

叢集中的所有節點都必須執行ONTAP 從功能上到ONTAP 功能上的從功能上的資訊、才能使行為生效。只有傳入流量會受到影響。

新規則如下：

- 升級至9.4到9.6版時ONTAP 、根據預設或自訂、將portmap服務新增至所有現有的防火牆原則。
- 建立新叢集或新的IPspace時ONTAP 、不將portmap服務新增至預設資料原則、而只新增至預設管理或叢集間原則。
- 您可以視需要將portmap服務新增至預設或自訂原則、並視需要移除服務。

如何新增或移除**portmap**服務

若要將portmap服務新增至SVM或叢集防火牆原則（可在防火牆內存取）、請輸入：

```
system services firewall policy create -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

若要從SVM或叢集防火牆原則中移除portmap服務（使其在防火牆內無法存取）、請輸入：

```
system services firewall policy delete -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

您可以使用網路介面modify命令、將防火牆原則套用至現有的LIF。如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

建立防火牆原則並將其指派給 LIF

當您建立LIF時、預設的防火牆原則會指派給每個LIF。在許多情況下、預設的防火牆設定運作良好、您不需要變更這些設定。如果您想要變更可存取LIF的網路服務或IP位址、可以建立自訂防火牆原則並將其指派給LIF。

關於這項工作

- 您無法使用建立防火牆原則 `policy` 名稱 `data`、 `intercluster`、 `cluster`或 `mgmt`。

  這些值保留給系統定義的防火牆原則。

- 您無法設定或修改叢集I生命 的防火牆原則。

  所有服務類型的叢集LIF防火牆原則都設為0.00.0.0/0。

- 如果您需要從原則中移除服務、則必須刪除現有的防火牆原則並建立新原則。
- 如果叢集上已啟用IPv6、您可以使用IPv6位址建立防火牆原則。

  啟用 IPv6 之後、 `data`、 `intercluster`和 `mgmt` 防火牆原則包括： /0 （ IPv6 萬用字元）在其接受的位址清單中。

- 使用System Manager設定跨叢集的資料保護功能時、您必須確保叢集間LIF IP位址包含在允許的清單中、而且叢集間LIF和公司擁有的防火牆都允許HTTPS服務。

  依預設 `intercluster` 防火牆原則允許從所有 IP 位址（ 0.0.0/0 或： /0 （ IPv6 ））存取、並啟用 HTTPS 、 NDMP 和 NDMPS 服務。如果您修改此預設原則、或是為叢集間LIF建立自己的防火牆原則、則必須將每個叢集間LIF IP位址新增至允許的清單、並啟用HTTPS服務。

- 從支援SJS9.6開始ONTAP 、不支援HTTPS和SSH防火牆服務。

  在 ONTAP 9.6 中 `management-https` 和 `management-ssh` LIF 服務可用於 HTTPS 和 SSH 管理存取。

步驟

1. 建立防火牆原則、讓特定SVM上的LIF可以使用：

   ```
   system services firewall policy create -vserver vserver_name -policy
   policy_name -service network_service -allow-list ip_address/mask
   ```

   您可以多次使用此命令、為防火牆原則中的每個服務新增多個網路服務和允許的IP位址清單。

2. 使用確認原則已正確新增 `system services firewall policy show` 命令。
3. 將防火牆原則套用至LIF：

   ```
   network interface modify -vserver vserver_name -lif lif_name -firewall-policy
   policy_name
   ```

4. 使用確認原則已正確新增至 LIF `network interface show -fields firewall-policy` 命令。

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

建立防火牆原則並將其指派給 **LIF** 的範例

下列命令會建立名為data_http的防火牆原則、以啟用從10.10子網路IP位址存取HTTP和HTTPS傳輸協定、將該原則套用至SVM VS1上名為data1的LIF、然後顯示叢集上的所有防火牆原則：

```
system services firewall policy create -vserver vs1 -policy data_http
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show

Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
vs1
        data_http
                     http       10.10.0.0/16
                     https      10.10.0.0/16

network interface modify -vserver vs1 -lif data1 -firewall-policy
data_http

network interface show -fields firewall-policy

vserver  lif                  firewall-policy
-------  -------------------- ---------------
Cluster  node1_clus_1
Cluster  node1_clus_2
Cluster  node2_clus_1
Cluster  node2_clus_2
cluster-1 cluster_mgmt         mgmt
cluster-1 node1_mgmt1          mgmt
cluster-1 node2_mgmt1          mgmt
vs1      data1                data_http
vs3      data2                data
```

管理防火牆服務和原則的 ONTAP 命令

您可以使用 `system services firewall` 管理防火牆服務的命令 `system services firewall policy` 管理防火牆原則的命令、以及 `network interface modify` 管理生命的防火牆設定的命令。

從功能部分9.10.1開始ONTAP ：

- 防火牆原則已過時、並由LIF服務原則取代。之前、內建防火牆是使用防火牆原則來管理。此功能現在是使用LIF服務原則來完成。
- 所有的防火牆原則都是空的、而且不會開啟基礎防火牆中的任何連接埠。而是必須使用LIF服務原則開啟所有連接埠。
- 升級至9.10.1或更新版本、從防火牆原則轉換至LIF服務原則之後、不需要採取任何行動。系統會自動建構符合先前ONTAP 版本的防火牆原則的LIF服務原則。如果您使用指令碼或其他工具來建立及管理自訂防火牆原則、則可能需要升級這些指令碼、以建立自訂服務原則。

若要深入瞭解、請參閱 "更新版本中的生命與服務政策ONTAP"。

如果您想要...	使用此命令...
啟用或停用防火牆服務	`system services firewall modify`
顯示目前的防火牆服務組態	`system services firewall show`
建立防火牆原則或新增服務至現有的防火牆原則	`system services firewall policy create`
將防火牆原則套用至LIF	`network interface modify -lif lifname -firewall-policy`
修改與防火牆原則相關的IP位址和網路遮罩	`system services firewall policy modify`
顯示防火牆原則的相關資訊	`system services firewall policy show`
建立一個新的防火牆原則、該原則是現有原則的確切複本	`system services firewall policy clone`
刪除LIF未使用的防火牆原則	`system services firewall policy delete`

相關資訊

- "系統服務防火牆"
- "修改網路介面"

版權資訊

商標資訊