



管理**Web**服務

ONTAP 9

NetApp
February 12, 2026

目錄

管理Web服務	1
管理網路服務總覽	1
管理對ONTAP Web 服務的訪問	1
在 ONTAP 中管理網路傳輸協定引擎	3
用於管理 Web 協定引擎的ONTAP指令	4
配置對ONTAP Web 服務的存取	5
用於管理 Web 服務的ONTAP命令	6
用於管理ONTAP節點上的掛載點的命令	6
在ONTAP中管理 SSL	7
管理 SSL 的命令	7
將 HSTS 用於ONTAP Web 服務	8
顯示 HSTS 配置	8
啟用 HSTS 並設定最大使用期限	9
禁用 HSTS	9
解決ONTAP Web 服務存取問題	9

管理Web服務

管理網路服務總覽

您可以啟用或停用叢集或儲存虛擬機器（SVM）的Web服務、顯示Web服務的設定、以及控制角色使用者是否可以存取Web服務。

您可以使用下列方式來管理叢集或SVM的Web服務：

- 啟用或停用特定的Web服務
- 指定是否僅限加密的HTTP（SSL）存取Web服務
- 顯示Web服務的可用度
- 允許或禁止角色使用者存取Web服務
- 顯示允許存取Web服務的角色

若要讓使用者存取Web服務、必須符合下列所有條件：

- 使用者必須通過驗證。

例如、Web服務可能會提示輸入使用者名稱和密碼。使用者的回應必須符合有效的帳戶。

- 使用者必須使用正確的存取方法來設定。

驗證只會針對使用者成功、並針對指定的Web服務提供正確的存取方法。適用於 ONTAP API Web 服務 (ontapi)、使用者必須擁有 ontapi 存取方法。對於所有其他 Web 服務、使用者必須擁有 http 存取方法。



您可以使用 `security login` 管理使用者存取方法和驗證方法的命令。

- Web服務必須設定為允許使用者的存取控制角色。



您可以使用 `vserver services web access` 控制角色存取 Web 服務的命令。

如果啟用防火牆、則必須設定用於Web服務的LIF防火牆原則、以允許HTTP或HTTPS。

如果您使用HTTPS進行Web服務存取、也必須啟用提供Web服務之叢集或SVM的SSL、而且必須提供叢集或SVM的數位憑證。

管理對ONTAP Web 服務的訪問

Web服務是使用者可以使用HTTP或HTTPS存取的應用程式。叢集管理員可以設定Web傳輸協定引擎、設定SSL、啟用Web服務、以及讓角色的使用者存取Web服務。

從支援下列Web服務的支援範圍ONTAP 起、從功能支援的9.6開始：

- 服務處理器基礎架構 (spi)

此服務可透過叢集管理LIF或節點管理LIF、讓節點的記錄檔、核心傾印檔和MIBA檔案可供HTTP或HTTPS存取。預設設定為 `enabled`。

當請求存取節點的日誌檔案或核心轉儲檔案時，`spi Web` 服務會自動建立一個從一個節點到另一個節點的根磁碟區（檔案所在的根磁碟區）的掛載點。您無需手動建立掛載點。

- ONTAP API (ontapi)

這項服務可讓您執行ONTAP IsyAPI、以遠端程式執行管理功能。預設設定為 `enabled`。

某些外部管理工具可能需要此服務。例如、如果您使用System Manager、則應保持啟用此服務。

- Data ONTAP 探索 (disco)

此服務可讓隨裝即用的管理應用程式在網路中探索叢集。預設設定為 `enabled`。

- 支援診斷 (supdiag)

此服務可控制系統上的權限環境存取、以協助進行問題分析和解決問題。預設設定為 `disabled`。您只能在技術支援人員的指示下啟用此服務。

- 系統管理員 (sysmgr)

此服務可控制系統管理員的可用度、ONTAP 而此功能隨附於本服務。預設設定為 `enabled`。此服務僅在叢集上受支援。

- 韌體基礎板管理控制器（BMC）更新 (FW_BMC)

此服務可讓您下載BMC韌體檔案。預設設定為 `enabled`。

- 資訊文件ONTAP (docs)

此服務可讓您存取ONTAP 有關的資料。預設設定為 `enabled`。

- ONTAP RESTful API (docs_api)

此服務可讓您存取ONTAP 「REST風格的API」 文件。預設設定為 `enabled`。

- 檔案上傳與下載 (fud)

此服務提供檔案上傳與下載。預設設定為 `enabled`。

- ONTAP 訊息 (ontapmsg)

此服務支援發佈及訂閱介面、可讓您訂閱活動。預設設定為 `enabled`。

- ONTAP 入口網站 (portal)

此服務會將閘道實作至虛擬伺服器。預設設定為 `enabled`。

- ONTAP REST 風格的介面 (rest)

此服務支援RESTful介面、可用於遠端管理叢集基礎架構的所有元素。預設設定為 enabled。

- 安全聲明標記語言 (SAML) 服務供應商支援 (saml)

此服務提供資源來支援SAML服務供應商。預設設定為 enabled。

- SAML 服務供應商 (saml-sp)

此服務可為服務供應商提供SP中繼資料和聲明使用者服務等服務。預設設定為 enabled。

從支援下列附加服務的支援範圍ONTAP 起、從支援使用者支援的範圍開始：

- 組態備份檔案 (backups)

此服務可讓您下載組態備份檔案。預設設定為 enabled。

- ONTAP 安全性 (security)

此服務支援CSRF權杖管理、以加強驗證。預設設定為 enabled。

在 ONTAP 中管理網路傳輸協定引擎

您可以在叢集上設定Web傳輸協定引擎、以控制是否允許Web存取、以及可以使用哪些SSL版本。您也可以顯示Web傳輸協定引擎的組態設定。

您可以透過下列方式、在叢集層級管理Web傳輸協定引擎：

- 您可以使用指定遠端用戶端是否可以使用 HTTP 或 HTTPS 來存取 Web 服務內容 `system services web modify` 命令 `-external` 參數。
- 您可以使用來指定是否應使用 SSLv3 來進行安全的 Web 存取 `security config modify` 命令 `-supported-protocol` 參數。
根據預設、SSLv3會停用。傳輸層安全性1.0 (TLSv1.0) 已啟用、可視需要停用。

如"[指令參考資料ONTAP](#)"需詳細 `security config modify` 資訊，請參閱。

- 您可以針對整個叢集的控制面板Web服務介面、啟用聯邦資訊處理標準 (FIPS) 140-2法規遵循模式。



預設會停用FIPS 140-2相容模式。

- 當**FIPS 140-2**相容模式停用時

您可以透過設定來啟用 FIPS 140-2 規範模式 `is-fips-enabled` 參數至 `true` 適用於 `security config modify` 命令、然後使用 `security config show` 確認線上狀態的命令。

- 啟用**FIPS 140-2**規範模式時

- 從 ONTAP 9.11.1 開始， TLSv1 ， TLSv1.1 和 SSLv3 都會停用，只有 TLSv1.2 和 TLSv1.3 會保持啟用狀態。它會影響ONTAP 到其他內部和外部的系統和通訊、而這些系統和通訊則是來自於19。如果您啟用FIPS 140-2規範模式、然後停用、則TLSv1、TLSv1.1及SSLv3會維持停用狀態。視先前的

組態而定、TLSv1.2或TLSSv1.3仍會保持啟用狀態。

- 對於9.11.1之前的ONTAP 版本、TLSv1和SSLv3都會停用、只有TLSv1.1和TLSv1.2會維持啟用狀態。啟用FIPS 140-2相容模式時、無法同時啟用TLSv1和SSLv3。ONTAP如果您啟用FIPS 140-2規範模式、然後停用該模式、則TLSv1和SSLv3仍會維持停用狀態、但根據先前的組態、TLSv1.2或同時啟用TLSv1.1和TLSv1.2。

- 您可以使用顯示叢集整體安全性的組態 `system security config show` 命令。

如"[指令參考資料ONTAP](#)"需詳細 `security config show` 資訊，請參閱。

如果啟用防火牆、則必須設定用於Web服務的邏輯介面（LIF）防火牆原則、以允許HTTP或HTTPS存取。

如果您使用HTTPS進行Web服務存取、則提供Web服務的叢集或儲存虛擬機器（SVM）的SSL也必須啟用、而且您必須提供叢集或SVM的數位憑證。

在「樣」組態中、您對叢集上的Web傳輸協定引擎所做的設定變更不會複寫到合作夥伴叢集上。MetroCluster

用於管理 Web 協定引擎的ONTAP指令

您可以使用 `system services web` 用於管理網路傳輸協定引擎的命令。您可以使用 `system services firewall policy create` 和 `network interface modify` 允許 Web 存取要求通過防火牆的命令。

如果您想要...	使用此命令...
在叢集層級設定Web傳輸協定引擎： • 啟用或停用叢集的Web傳輸協定引擎 • 啟用或停用叢集的SSLv3 • 啟用或停用安全網路服務（HTTPS）的FIPS 140-2法規遵循	<code>system services web modify</code>
在叢集層級顯示Web傳輸協定引擎的組態、判斷Web傳輸協定是否在整個叢集內正常運作、並顯示FIPS 140-2相容性是否已啟用且處於線上狀態	<code>system services web show</code>
顯示節點層級的Web傳輸協定引擎組態、以及叢集中節點的Web服務處理活動	<code>system services web node show</code>
建立防火牆原則、或將HTTP或HTTPS傳輸協定服務新增至現有的防火牆原則、以允許Web存取要求通過防火牆	<code>system services firewall policy create</code> 設定 <code>-service</code> 參數至 <code>http</code> 或 <code>https</code> 允許 Web 存取要求通過防火牆。

如果您想要...	使用此命令...
將防火牆原則與LIF建立關聯	<pre>network interface modify</pre> 您可以使用 <code>-firewall-policy</code> 修改 LIF 防火牆原則的參數。

相關資訊

- ["修改網路介面"](#)

配置對ONTAP Web 服務的存取

設定Web服務存取權可讓授權使用者使用HTTP或HTTPS存取叢集或儲存虛擬機器（SVM）上的服務內容。

步驟

1. 如果已啟用防火牆、請確定將用於Web服務的LIF防火牆原則中已設定HTTP或HTTPS存取：



您可以使用檢查是否啟用防火牆 `system services firewall show` 命令。

- a. 若要確認已在防火牆原則中設定 HTTP 或 HTTPS、請使用 `system services firewall policy show` 命令。

您可以設定 `-service` 的參數 `system services firewall policy create` 命令至 `http` 或 `https` 啟用原則以支援網路存取。

- b. 若要驗證支援 HTTP 或 HTTPS 的防火牆原則是否與提供 Web 服務的 LIF 相關聯、請使用 `network interface show` 命令 `-firewall-policy` 參數。

如["指令參考資料ONTAP"](#)需詳細 `network interface show` 資訊，請參閱。

您可以使用 `network interface modify` 命令 `-firewall-policy` 將防火牆原則對 LIF 生效的參數。

如["指令參考資料ONTAP"](#)需詳細 `network interface modify` 資訊，請參閱。

2. 若要設定叢集層級的 Web 傳輸協定引擎、並讓 Web 服務內容可供存取、請使用 `system services web modify` 命令。
3. 如果您打算使用安全 Web 服務（HTTPS）、請啟用 SSL、並使用為叢集或 SVM 提供數位憑證資訊 `security ssl modify` 命令。

如["指令參考資料ONTAP"](#)需詳細 `security ssl modify` 資訊，請參閱。

4. 若要啟用叢集或 SVM 的 Web 服務、請使用 `vserver services web modify` 命令。

您必須針對要為叢集或SVM啟用的每個服務重複此步驟。

5. 若要授權角色存取叢集或 SVM 上的 Web 服務、請使用 `vserver services web access create` 命令。

您授予存取權的角色必須已經存在。您可以使用顯示現有角色 `security login role show` 使用命令或建立新角色 `security login role create` 命令。

深入瞭解 `security login role show` 及 `security login role create` "指令參考資料ONTAP"。

6. 對於已獲授權存取 Web 服務的角色、請檢查的輸出、以確保其使用者也使用正確的存取方法進行設定 `security login show` 命令。

存取 ONTAP API Web 服務 `ontapi`）、使用者必須使用設定 `ontapi` 存取方法。若要存取所有其他 Web 服務、必須使用設定使用者 `http` 存取方法。

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



您可以使用 `security login create` 命令來新增使用者的存取方法。如"指令參考資料ONTAP"需詳細 `security login create` 資訊，請參閱。

用於管理 Web 服務的ONTAP命令

您可以使用 `vserver services web` 用於管理叢集或儲存虛擬機器（SVM）Web 服務可用度的命令。您可以使用 `vserver services web access` 控制角色存取 Web 服務的命令。

如果您想要...	使用此命令...
設定叢集或AnSVM的Web服務： - 啟用或停用Web服務 - 指定是否只能使用HTTPS存取Web服務	<code>vserver services web modify</code>
顯示叢集或anSVM的Web服務組態和可用度	<code>vserver services web show</code>
授權角色存取叢集或anSVM上的Web服務	<code>vserver services web access create</code>
顯示授權存取叢集或anSVM上Web服務的角色	<code>vserver services web access show</code>
防止角色存取叢集或anSVM上的Web服務	<code>vserver services web access delete</code>

相關資訊

"指令參考資料ONTAP"

用於管理ONTAP節點上的掛載點的命令

◦ `spi` Web 服務會在要求存取節點的記錄檔或核心檔案時、自動從一個節點建立掛載點到另一個節點的根磁碟區。雖然您不需要手動管理掛載點、但可以使用來進行 `system`

node root-mount 命令。

如果您想要...	使用此命令...
手動從一個節點建立掛載點到另一個節點的根磁碟區	<code>system node root-mount create</code> 只有一個掛載點可以從一個節點存在到另一個節點。
在叢集中的節點上顯示現有的掛載點、包括建立掛載點的時間及其目前狀態	<code>system node root-mount show</code>
從一個節點刪除掛載點到另一個節點的根磁碟區、並強制關閉與掛載點的連線	<code>system node root-mount delete</code>

相關資訊

["指令參考資料ONTAP"](#)

在ONTAP中管理 SSL

使用 `security ssl` 用於管理叢集或儲存虛擬機器（SVM）SSL 傳輸協定的命令。SSL 通訊協定可利用數位憑證在 Web 伺服器與瀏覽器之間建立加密連線、進而改善網路存取的安全性。

您可以透過下列方式管理叢集或儲存虛擬機器（SVM）的SSL：

- 啟用SSL
- 產生及安裝數位憑證、並將其與叢集或SVM建立關聯
- 顯示SSL組態以查看是否已啟用SSL、以及SSL憑證名稱（如果有）
- 設定叢集或SVM的防火牆原則、以便Web存取要求能夠通過
- 定義可以使用的SSL版本
- 限制僅存取Web服務的HTTPS要求

管理 SSL 的命令

您可以使用 `security ssl` 用於管理叢集或儲存虛擬機器（SVM）SSL 傳輸協定的命令。

如果您想要...	使用此命令...
為叢集或 SVM 啟用 SSL、並將數位憑證與其建立關聯	<code>security ssl modify</code>
顯示叢集或 SVM 的 SSL 組態和憑證名稱	<code>security ssl show</code>

深入瞭解 `security ssl modify` 及 `security ssl show` ["指令參考資料ONTAP"](#)。

將 HSTS 用於 ONTAP Web 服務

HTTP 嚴格傳輸安全性 (HSTS) 是一種 Web 安全性原則機制，可協助保護網站免受中間人攻擊，例如協定降級攻擊和 Cookie 劫持。透過強制使用 HTTPS，HSTS 可確保使用者瀏覽器與伺服器之間的所有通訊都經過加密。從 ONTAP 9.17.1 開始，ONTAP 可以為 ONTAP Web 服務強制使用 HTTPS 連線。



只有在與 ONTAP 建立初始安全 HTTPS 連線後，Web 瀏覽器才會強制執行 HSTS。如果瀏覽器未建立初始安全連接，則不會強制執行 HSTS。有關 HSTS 管理的信息，請參閱您的瀏覽器文件。

關於這項工作

- 對於 9.17.1 及更高版本，新安裝的 ONTAP 叢集預設為啟用 HSTS。升級到 9.17.1 後，HSTS 預設不啟用。您必須在升級後啟用 HSTS。
- 所有產品均支援 HSTS "ONTAP Web 服務"。

開始之前

- 以下任務需要進階權限。

顯示 HSTS 配置

您可以顯示目前的 HSTS 配置以檢查它是否已啟用並查看最大年齡設定。

步驟

1. 使用 `system services web show` 指令顯示目前的 Web 服務配置，包括 HSTS 設定：

```
cluster-1::system services web*> show

      External Web Services: true
              HTTP Port: 80
              HTTPS Port: 443
      Protocol Status: online
      Per Address Limit: 80
      Wait Queue Capacity: 192
              HTTP Enabled: true
      CSRF Protection Enabled: true
Maximum Number of Concurrent CSRF Tokens: 500
      CSRF Token Idle Timeout (Seconds): 900
      CSRF Token Absolute Timeout (Seconds): 0
      Allow Web Management via Cloud: true
Enforce Network Interface Service-Policy: -
              HSTS Enabled: true
      HSTS max age (Seconds): 63072000
```

啟用 HSTS 並設定最大使用期限

從ONTAP 9.17.1 開始，新的ONTAP叢集預設啟用 HSTS。如果您將現有叢集升級至 9.17.1 或更高版本，則需要在叢集上手動啟用 HSTS 以強制使用 HTTPS。您可以啟用 HSTS 並設定最長使用期限。如果已啟用 HSTS，您可以隨時變更最長使用期限。啟用 HSTS 後，瀏覽器僅在建立初始安全連線後才會開始強制執行安全連線。

步驟

1. 使用 `system services web modify` 啟用 HSTS 或修改最大年齡的命令：

```
system services web modify -hsts-enabled true -hsts-max-age <seconds>
```

`-hsts-max-age` 指定瀏覽器記住強制執行 HTTPS 的時長（以秒為單位）。預設值為 63072000 秒（兩年）。

禁用 HSTS

瀏覽器會在每次連接時保存 HSTS 最長使用期限設置，即使在ONTAP上停用 HSTS，它們也會在整個連接期間繼續強制執行 HSTS。停用 HSTS 後，瀏覽器需要等待配置的最長使用期限才能停止強制執行 HSTS。如果在此期間無法建立安全連接，則強制執行 HSTS 的瀏覽器將不允許存取ONTAP Web 服務，直到問題解決或瀏覽器的最長使用期限到期。

步驟

1. 使用 `system services web modify` 命令：

```
system services web modify -hsts-enabled false
```

相關資訊

["RFC 6797 - HTTP 嚴格傳輸安全性 \(HSTS\)"](#)

解決ONTAP Web 服務存取問題

組態錯誤會導致網路服務存取問題。您可以確保LIF、防火牆原則、Web傳輸協定引擎、Web服務、數位憑證、而且使用者存取授權均設定正確。

下表可協助您識別及解決Web服務組態錯誤：

此存取問題...	發生原因是此組態錯誤...	若要解決錯誤...
您的 Web 瀏覽器會傳回 unable to connect 或 failure to establish a connection 嘗試存取 Web 服務時發生錯誤。	您的LIF設定可能不正確。	請確定您可以ping提供Web服務的LIF。  您可以使用 `network ping` 命令 ping LIF。

此存取問題...	發生原因是此組態錯誤...	若要解決錯誤...
您的防火牆可能設定不正確。	請確定防火牆原則已設定為支援HTTP或HTTPS、而且原則已指派給提供Web服務的LIF。  您可以使用 <code>system services firewall policy</code> 管理防火牆原則的命令。您可以使用 <code>network interface modify</code> 命令 <code>-firewall -policy</code> 將原則與 LIF 建立關聯的參數。	您的網路傳輸協定引擎可能已停用。
確保已啟用Web傳輸協定引擎、以便存取Web服務。  您可以使用 <code>system services web</code> 用於管理叢集 Web 傳輸協定引擎的命令。	您的網路瀏覽器會傳回 A not found 嘗試存取 Web 服務時發生錯誤。	Web服務可能已停用。
確保您要允許存取的每個Web服務都已個別啟用。  您可以使用 <code>vserver services web modify</code> 命令以啟用 Web 服務進行存取。	Web瀏覽器無法以使用者的帳戶名稱和密碼登入Web服務。	無法驗證使用者、存取方法不正確、或使用者無權存取Web服務。

此存取問題...	發生原因是此組態錯誤...	若要解決錯誤...
請確定使用者帳戶存在、並使用正確的存取方法和驗證方法進行設定。此外、請確認使用者的角色已獲授權可存取Web服務。  您可以使用 <code>security login</code> 管理使用者帳戶及其存取方法和驗證方法的命令。存取 ONTAP API Web 服務需要 <code>ontapi</code> 存取方法。存取所有其他 Web 服務需要 <code>http</code> 存取方法。您可以使用 <code>vserver services web access</code> 用於管理角色存取 Web 服務的命令。	您使用HTTPS連線至Web服務、而您的Web瀏覽器則表示連線中斷。	您可能未在提供Web服務的叢集或儲存虛擬機器（SVM）上啟用SSL。
確認叢集或SVM已啟用SSL、且數位憑證有效。  您可以使用 <code>security ssl</code> 用於管理 HTTP 伺服器 和的 SSL 組態的命令 <code>security certificate show</code> 顯示數位憑證資訊的命令。	您使用HTTPS連線至Web服務、Web瀏覽器則表示該連線不受信任。	您可能使用自我簽署的數位憑證。

相關資訊

- ["ONTAP網路配置的最佳實務是什麼？"](#)
- ["網路ping"](#)
- ["修改網路介面"](#)
- ["產生安全性憑證-CSR"](#)
- ["安全性憑證安裝"](#)
- ["安全證書展示"](#)
- ["安全 SSL"](#)

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。