



# 使用 **TLS** 搭配 **NFS** 以獲得強大的安全性

## ONTAP 9

NetApp  
June 19, 2024

# 目錄

使用 TLS 搭配 NFS 以獲得強大的安全性 .....	1
使用 TLS 搭配 NFS 以增強安全性的總覽 .....	1
啟用或停用 TLS for NFS 用戶端 .....	1

# 使用 TLS 搭配 NFS 以獲得強大的安全性

## 使用 TLS 搭配 NFS 以增強安全性的總覽

相較於 Kerberos 和 IPsec、TLS 能以同等安全性和較低複雜度來實現加密網路通訊。身為系統管理員、您可以使用系統管理員、ONTAP CLI 或 ONTAP REST API、啟用、設定及停用 TLS、以增強 NFSv3 和 NFSv4.x 連線的安全性。



9.15.1 提供 ONTAP over TLS 的公開預覽功能。ONTAP 9.15.1 的正式作業工作負載不支援 NFS over TLS 作為預覽產品。

ONTAP 使用 TLS 1.3 for NFS over TLS 連線。

### 需求

NFS over TLS 需要 X.509 憑證。您可以在 ONTAP 叢集上建立安裝 CA 簽署的伺服器憑證、也可以安裝 NFS 服務直接使用的憑證。您的憑證應符合下列準則：

- 每個憑證都必須以 NFS 伺服器的完整網域名稱（FQDN）（將啟用 / 設定 TLS 的資料 LIF）做為一般名稱（CN）進行設定。
- 每個憑證都必須以 NFS 伺服器（或兩者）的 IP 位址或 FQDN 做為主體替代名稱（SAN）。如果同時設定 IP 位址和 FQDN、NFS 用戶端就可以使用 IP 位址或 FQDN 進行連線。
- 您可以為同一個 LIF 安裝多個 NFS 服務憑證、但一次只能使用其中一個憑證作為 NFS TLS 組態的一部分。

## 啟用或停用 TLS for NFS 用戶端

您可以設定 NFS over TLS 來加密所有透過網路在 NFS 用戶端和 ONTAP 之間傳送的資料、藉此改善 NFS 連線的安全性。如此可提高 NFS 連線的安全性。您可以在已啟用的現有儲存 VM 上進行設定 "NFS"。



9.15.1 提供 ONTAP over TLS 的公開預覽功能。ONTAP 9.15.1 的正式作業工作負載不支援 NFS over TLS 作為預覽產品。

### 啟用 TLS

您可以為 NFS 用戶端啟用 TLS 加密、以提高傳輸中資料的安全性。

#### 開始之前

- 請參閱 "需求" 在開始之前使用 NFS over TLS。
- 如需此程序中命令的詳細資訊、請參閱 ONTAP 手冊頁。

#### 步驟

1. 選擇要啟用 TLS 的儲存 VM 和邏輯介面（LIF）。
2. 在該儲存 VM 和介面上啟用 TLS for NFS 連線。

```
vserver nfs tls interface enable -vserver <STORAGE_VM> -lif <LIF_NAME>
-certificate-name <CERTIFICATE_NAME>
```

3. 使用 `vserver nfs tls interface show` 檢視結果的命令：

```
vserver nfs tls interface show
```

## 範例

下列命令可在上啟用 NFS over TLS data1 的 LIF vs1 儲存 VM：

```
vserver nfs tls interface enable -vserver vs1 -lif data1 -certificate-name
cert_vs1
```

```
vserver nfs tls interface show
```

Vserver Name	Logical Interface	Address	TLS Status	TLS Certificate
vs1	data1	10.0.1.1	enabled	cert_vs1
vs2	data2	10.0.1.2	disabled	-

2 entries were displayed.

## 停用 TLS

如果不再需要傳輸中資料的增強安全性、您可以停用 TLS for NFS Client。

### 開始之前

如需此程序中命令的詳細資訊、請參閱 ONTAP 手冊頁。

### 步驟

1. 選擇要停用 TLS 的儲存 VM 和邏輯介面（LIF）。
2. 在該儲存 VM 和介面上停用 TLS for NFS 連線。

```
vserver nfs tls interface disable -vserver <STORAGE_VM> -lif <LIF_NAME>
```

3. 使用 `vserver nfs tls interface show` 檢視結果的命令：

```
vserver nfs tls interface show
```

## 範例

下列命令會停用上的 NFS over TLS data1 的 LIF vs1 儲存 VM ：

```
vserver nfs tls interface disable -vserver vs1 -lif data1
```

```
vserver nfs tls interface show
```

Vserver Name	Logical Interface	Address	TLS Status	TLS Certificate
vs1	data1	10.0.1.1	disabled	-
vs2	data2	10.0.1.2	disabled	-

2 entries were displayed.

## 編輯 TLS 組態

您可以變更現有 NFS over TLS 組態的設定。例如、您可以使用此程序來更新 TLS 憑證。

### 開始之前

如需此程序中命令的詳細資訊、請參閱 ONTAP 手冊頁。

### 步驟

1. 選擇要修改 NFS 用戶端 TLS 組態的儲存 VM 和邏輯介面（LIF）。
2. 修改組態。如果您指定 status 的 enable、您也需要指定 certificate-name 參數。以您環境的資訊取代括弧 <> 中的值：

```
vserver nfs tls interface modify -vserver <STORAGE_VM> -lif <LIF_NAME>  
-status <STATUS> -certificate-name <CERTIFICATE_NAME>
```

3. 使用 `vserver nfs tls interface show` 檢視結果的命令：

```
vserver nfs tls interface show
```

## 範例

下列命令會修改上的 NFS over TLS 組態 data2 的 LIF vs2 儲存 VM :

```
vserver nfs tls interface modify -vserver vs2 -lif data2 -status enable  
-certificate-name new_cert
```

```
vserver nfs tls interface show
```

Vserver Name	Logical Interface	Address	TLS Status	TLS Certificate
vs1	data1	10.0.1.1	disabled	-
vs2	data2	10.0.1.2	enabled	new_cert

2 entries were displayed.

## 版權資訊

Copyright © 2024 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 保留隨時變更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。