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

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
```

```
               Logical
Vserver        Interface     Address          TLS Status TLS Certificate
Name
-------------- ------------- ---------------- ----------
------------------------
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
```

```
               Logical
Vserver        Interface     Address         TLS Status TLS Certificate
Name
-------------- ------------- --------------- ----------
-----------------------
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
```

```
               Logical
Vserver        Interface     Address         TLS Status TLS Certificate
Name
-------------- ------------- --------------- ----------
-----------------------
vs1            data1         10.0.1.1        disabled   -
vs2            data2         10.0.1.2        enabled    new_cert
2 entries were displayed.
```