NFSでのTLSの使用によるセキュリティ強化

ONTAP 9

NetApp
June 19, 2024

目次

NFSでのTLSの使用によるセキュリティ強化

NFSでのTLSを使用したセキュリティ強化の概要

TLSを使用すると、暗号化されたネットワーク通信をKerberosやIPsecと同等のセキュリティで実現でき、複雑さも軽減されます。管理者は、System Manager、ONTAP CLI、またはONTAP REST APIを使用して、NFSv3およびNFSv4.x接続でのセキュリティを強化するためのTLSの有効化、設定、および無効化を行うことができます。

> ONTAP 9.15.1では、NFS over TLSがパブリックプレビューとして提供されています。プレビュー版として、ONTAP 9.15.1では本番ワークロードでNFS over TLSはサポートされていません。

ONTAPでは、TLS経由のNFS接続にTLS 1.3が使用されます。

要件

NFS over TLSにはX.509証明書が必要です。ONTAPクラスタにCA署名済みサーバ証明書をインストールするか、NFSサービスが直接使用する証明書をインストールできます。証明書は次のガイドラインに従っている必要があります。

- 各証明書は、NFSサーバ（TLSを有効または設定するデータLIF）のFully Qualified Domain Name（FQDN；完全修飾ドメイン名）を共通名（CN）として設定する必要があります。
- 各証明書には、サブジェクト代替名（SAN）としてNFSサーバ（またはその両方）のIPアドレスまたはFQDNを設定する必要があります。IPアドレスとFQDNの両方が設定されている場合、NFSクライアントはIPアドレスまたはFQDNを使用して接続できます。
- 同じLIFに複数のNFSサービス証明書をインストールできますが、NFS TLS設定で一度に使用できるのはそのうちの1つだけです。

NFSクライアントに対するTLSの有効化または無効化

NFSクライアントとONTAPの間でネットワーク経由で送信されるすべてのデータを暗号化するようにNFS over TLSを設定すると、NFS接続のセキュリティを強化できます。これにより、NFS接続のセキュリティが向上します。有効になっている既存のStorage VMでこの設定を行うことができます： "NFS"。

> ONTAP 9.15.1では、NFS over TLSがパブリックプレビューとして提供されています。プレビュー版として、ONTAP 9.15.1では本番ワークロードでNFS over TLSはサポートされていません。

TLSを有効にする

NFSクライアントに対してTLS暗号化を有効にすると、転送中のデータのセキュリティを強化できます。

作業を開始する前に

- を参照してください "要件" （NFS over TLSの場合）を参照してください。
- この手順のコマンドの詳細については、ONTAPのマニュアルページを参照してください。

手順

1. TLSを有効にするStorage VMと論理インターフェイス（LIF）を選択してください。
2. そのStorage VMおよびインターフェイスのNFS接続に対してTLSを有効にします。

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

3. を使用します `vserver nfs tls interface show` コマンドを使用して結果を表示します。

```
vserver nfs tls interface show
```

例

次のコマンドは、でNFS over TLSを有効にします。 `data1` SVMノLIF `vs1` Storage 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.
```

TLSを無効にする

転送中のデータのセキュリティを強化する必要がなくなった場合は、NFSクライアントのTLSを無効にすることができます。

作業を開始する前に

この手順のコマンドの詳細については、ONTAPのマニュアルページを参照してください。

手順

1. TLSを無効にするStorage VMと論理インターフェイス（LIF）を選択してください。
2. そのStorage VMおよびインターフェイスのNFS接続に対するTLSを無効にします。

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

3. を使用します `vserver nfs tls interface show` コマンドを使用して結果を表示します。

```
vserver nfs tls interface show
```

例

次のコマンドは、でNFS over TLSを無効にします。 `data1` SVMノLIF `vs1` Storage 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.
```

TLS設定の編集

NFS over TLSの既存の設定を変更できます。たとえば、この手順を使用してTLS証明書を更新できます。

作業を開始する前に

この手順のコマンドの詳細については、ONTAPのマニュアルページを参照してください。

手順

1. NFSクライアントのTLS設定を変更するStorage VMと論理インターフェイス（LIF）を選択してください。
2. 設定を変更します。を指定する場合 `status` の `enable`を指定する必要があります。 `certificate-name` パラメータ括弧<>の値は、環境の情報で置き換えます。

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

3. を使用します `vserver nfs tls interface show` コマンドを使用して結果を表示します。

```
vserver nfs tls interface show
```

例

次のコマンドは、SVM上のNFS over TLSの設定を変更します。 `data2` SVMノLIF `vs2` Storage 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.
```

著作権に関する情報

商標に関する情報