



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	1
NFSでのTLSを使用したセキュリティ強化の概要	1
NFSクライアントに対するTLSの有効化または無効化	1

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
```

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.

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
```

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.

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
```

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.

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。