



将**TLS**与**NFS**结合使用可增强安全性

ONTAP 9

NetApp
June 19, 2024

目录

将TLS与NFS结合使用可增强安全性	1
概述如何将TLS与NFS结合使用以增强安全性	1
为NFS客户端启用或禁用TLS	1

将TLS与NFS结合使用可增强安全性

概述如何将TLS与NFS结合使用以增强安全性

TLS支持加密网络通信、安全性与Kerberos和IPsec相当、复杂性比Kerberos和IPsec低。作为管理员、您可以使用System Manager、ONTAP命令行界面或ONTAP REST API启用、配置和禁用TLS、以增强NFSv3和NFSv4.x连接的安全性。



基于TLS的NFS在ONTAP 9.15.1中提供公开预览版。作为预览选项、ONTAP 9.15.1中的生产工作负载不支持基于TLS的NFS。

ONTAP对基于TLS的NFS连接使用TLS 1.3。

要求

基于TLS的NFS需要X.509证书。您可以在ONTAP集群上创建安装CA签名的服务器证书、也可以安装NFS服务直接使用的证书。您的证书应符合以下准则：

- 必须为每个证书配置一个公用名(Common Name、CN)、即NFS服务器的完全限定域名(FQDN)(要启用/配置TLS的数据LIF)。
- 必须为每个证书配置NFS服务器(或两者)的IP地址或FQDN作为使用者替代名称(SAN)。如果同时配置了IP地址和FQDN、则NFS客户端可以使用IP地址或FQDN进行连接。
- 您可以为同一个LIF安装多个NFS服务证书、但在NFS TLS配置中、一次只能使用其中一个证书。

为NFS客户端启用或禁用TLS

您可以在NFS客户端的数据LIF上启用或禁用TLS。启用基于TLS的NFS时、SVM将使用TLS对通过网络在NFS客户端和ONTAP之间发送的所有数据进行加密。这样可以提高NFS连接的安全性。



基于TLS的NFS在ONTAP 9.15.1中提供公开预览版。作为预览选项、ONTAP 9.15.1中的生产工作负载不支持基于TLS的NFS。

启用TLS

您可以为NFS客户端启用TLS加密、以提高传输中数据的安全性。

开始之前

- 请参见 ["要求"](#) 适用于基于TLS的NFS。
- 请参见 ["手册页"](#) 有关的详细信息、请参见 `vserver nfs tls interface enable` 命令：

步骤

1. 选择要启用TLS的Storage VM和逻辑接口(LIF)。
2. 为该Storage VM和接口上的NFS连接启用TLS。将括号<>中的值替换为您环境中的信息：

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

3. 使用 `vserver nfs tls interface show` 命令以查看结果：

```
vserver nfs tls interface show
```

示例

以下命令将在上启用基于TLS的NFS data1 的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.

禁用TLS

如果您不再需要增强传输中数据的安全性、则可以为NFS客户端禁用TLS。



禁用基于TLS的NFS时、用于NFS连接的TLS证书将被删除。如果将来需要启用基于TLS的NFS、则需要在启用期间重新指定证书名称。

开始之前

请参见 ["手册页"](#) 有关的详细信息、请参见 `vserver nfs tls interface disable` 命令：

步骤

1. 选择要禁用TLS的Storage VM和逻辑接口(LIF)。
2. 对该Storage VM和接口上的NFS连接禁用TLS。将括号<>中的值替换为您环境中的信息：

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

3. 使用 `vserver nfs tls interface show` 命令以查看结果:

```
vserver nfs tls interface show
```

示例

以下命令将在上禁用基于TLS的NFS data1 的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.

编辑TLS配置

您可以更改基于TLS的现有NFS配置的设置。例如、您可以使用此操作步骤更新TLS证书。

开始之前

请参见 ["手册页"](#) 有关的详细信息、请参见 `vserver nfs tls interface modify` 命令:

步骤

1. 选择要修改NFS客户端的TLS配置的Storage VM和逻辑接口(LIF)。
2. 修改配置。如果指定 `status` 的 `enable`, 您还需要指定 `certificate-name` 参数。将括号<>中的值替换为您环境中的信息:

```
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` 命令以查看结果:

```
vserver nfs tls interface show
```

示例

以下命令将在上修改基于TLS的NFS配置 data2 的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.

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。