



강력한 보안을 위해 **NFS**와 함께 **TLS**를 사용하십시오 ONTAP 9

NetApp
July 10, 2024

목차

강력한 보안을 위해 NFS와 함께 TLS를 사용하십시오	1
강력한 보안을 위해 NFS와 함께 TLS 사용 개요	1
NFS 클라이언트에 대해 TLS를 사용하거나 사용하지 않도록 설정합니다	1

강력한 보안을 위해 NFS와 함께 TLS를 사용하십시오

강력한 보안을 위해 NFS와 함께 TLS 사용 개요

TLS는 Kerberos 및 IPsec보다 덜 복잡하며 동일한 수준의 보안으로 암호화된 네트워크 통신을 가능하게 합니다. 관리자는 System Manager, ONTAP CLI 또는 ONTAP REST API를 사용하여 NFSv3 및 NFSv4.x 연결을 통해 강력한 보안을 위해 TLS를 사용, 구성 및 사용하지 않도록 설정할 수 있습니다.



NFS over TLS는 ONTAP 9.15.1에서 공개 미리 보기로 제공됩니다. 미리 보기 오퍼링에서는 ONTAP 9.15.1의 운영 워크로드에 TLS를 통한 NFS가 지원되지 않습니다.

ONTAP는 TLS 연결을 통한 NFS 연결에 TLS 1.3을 사용합니다.

요구 사항

NFS over TLS는 X.509 인증서가 필요합니다. ONTAP 클러스터에 CA 서명 서버 인증서를 설치하거나 NFS 서비스에서 직접 사용하는 인증서를 설치할 수 있습니다. 인증서는 다음 지침을 충족해야 합니다.

- 각 인증서는 공통 이름(CN)으로 NFS 서버(TLS를 설정/구성할 데이터 LIF)의 FQDN(정규화된 도메인 이름)을 구성해야 합니다.
- 각 인증서는 NFS 서버의 IP 주소 또는 FQDN(또는 둘 다)을 SAN(Subject Alternative Name)으로 구성해야 합니다. IP 주소와 FQDN이 모두 구성된 경우 NFS 클라이언트는 IP 주소 또는 FQDN을 사용하여 연결할 수 있습니다.
- 동일한 LIF에 여러 NFS 서비스 인증서를 설치할 수 있지만 NFS TLS 구성의 일부로 한 번에 하나만 사용할 수 있습니다.

NFS 클라이언트에 대해 TLS를 사용하거나 사용하지 않도록 설정합니다

NFS 클라이언트용 데이터 LIF에서 TLS를 사용하거나 사용하지 않도록 설정할 수 있습니다. TLS를 통해 NFS를 활성화하면 SVM은 TLS를 사용하여 NFS 클라이언트와 ONTAP 간에 네트워크를 통해 전송되는 모든 데이터를 암호화합니다. 이렇게 하면 NFS 연결의 보안이 향상됩니다.



NFS over TLS는 ONTAP 9.15.1에서 공개 미리 보기로 제공됩니다. 미리 보기 오퍼링에서는 ONTAP 9.15.1의 운영 워크로드에 TLS를 통한 NFS가 지원되지 않습니다.

TLS를 활성화합니다

NFS 클라이언트에 대해 TLS 암호화를 활성화하여 전송 중인 데이터의 보안을 강화할 수 있습니다.

시작하기 전에

- 을 참조하십시오 ["요구 사항"](#) NFS over TLS를 사용하는 것이 좋습니다.

- 을 참조하십시오 ["수동 페이지"](#)에 대한 자세한 내용은 `vserver nfs tls interface enable` 명령.

단계

1. TLS를 활성화할 스토리지 VM 및 논리 인터페이스(LIF)를 선택합니다.
2. 해당 스토리지 VM 및 인터페이스에서 NFS 연결에 TLS를 사용하도록 설정합니다. 괄호 안의 값을 사용자 환경의 정보로 대체:

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

3. 를 사용합니다 `vserver nfs tls interface show` 명령을 사용하여 결과를 봅니다.

```
vserver nfs tls interface show
```

예

다음 명령을 실행하면 에서 NFS over TLS가 사용되도록 설정됩니다 data1 의 LIF vs1 스토리지 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.

TLS를 비활성화합니다

전송 중인 데이터에 대해 강화된 보안이 더 이상 필요하지 않으면 NFS 클라이언트에 대해 TLS를 사용하지 않도록 설정할 수 있습니다.



TLS를 통해 NFS를 사용하지 않도록 설정하면 NFS 연결에 사용되는 TLS 인증서가 제거됩니다. 나중에 TLS를 통한 NFS를 활성화해야 하는 경우 활성화 중에 인증서 이름을 다시 지정해야 합니다.

시작하기 전에

을 참조하십시오 ["수동 페이지"](#)에 대한 자세한 내용은 `vserver nfs tls interface disable` 명령.

단계

1. TLS를 사용하지 않도록 설정할 스토리지 VM 및 논리 인터페이스(LIF)를 선택합니다.
2. 스토리지 VM 및 인터페이스에서 NFS 연결에 대해 TLS를 사용하지 않도록 설정합니다. 괄호 안의 값을 사용자 환경의 정보로 대체:

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

3. 를 사용합니다 `vserver nfs tls interface show` 명령을 사용하여 결과를 봅니다.

```
vserver nfs tls interface show
```

예

다음 명령은 에서 NFS over TLS를 사용하지 않도록 설정합니다 `data1` 의 LIF `vs1` 스토리지 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 구성을 편집합니다

TLS를 통한 기존 NFS 구성의 설정을 변경할 수 있습니다. 예를 들어, 이 절차를 사용하여 TLS 인증서를 업데이트할 수 있습니다.

시작하기 전에

을 참조하십시오 ["수동 페이지"](#)에 대한 자세한 내용은 `vserver nfs tls interface modify` 명령.

단계

1. NFS 클라이언트에 대한 TLS 구성을 수정할 스토리지 VM 및 논리 인터페이스(LIF)를 선택합니다.
2. 구성을 수정합니다. 를 지정할 경우 `status` 의 `enable` 또한 를 지정해야 합니다 `certificate-name`

매개 변수. 괄호 안의 값을 사용자 환경의 정보로 대체:

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

3. 를 사용합니다 vserver nfs tls interface show 명령을 사용하여 결과를 봅니다.

```
vserver nfs tls interface show
```

예

다음 명령을 실행하면 의 NFS over TLS 구성을 수정합니다 data2 의 LIF vs2 스토리지 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.

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.