



Hohe Sicherheit durch Verwendung von TLS mit NFS

ONTAP 9

NetApp
June 19, 2024

Inhalt

- Hohe Sicherheit durch Verwendung von TLS mit NFS 1
- Übersicht über die Verwendung von TLS mit NFS für hohe Sicherheit 1
- Aktivieren oder deaktivieren Sie TLS für NFS-Clients 1

Hohe Sicherheit durch Verwendung von TLS mit NFS

Übersicht über die Verwendung von TLS mit NFS für hohe Sicherheit

TLS ermöglicht verschlüsselte Netzwerkkommunikation mit gleichwertiger Sicherheit und geringerer Komplexität als Kerberos und IPsec. Als Administrator können Sie TLS für eine hohe Sicherheit bei NFSv3- und NFSv4.x-Verbindungen mit System Manager, der ONTAP-CLI oder der ONTAP-REST-API aktivieren, konfigurieren und deaktivieren.



NFS über TLS ist in ONTAP 9.15.1 als öffentliche Vorschau verfügbar. NFS über TLS wird in ONTAP 9.15.1 als Vorschauangebot für Produktions-Workloads nicht unterstützt.

ONTAP verwendet TLS 1.3 für NFS- über TLS-Verbindungen.

Anforderungen

NFS über TLS erfordert X.509-Zertifikate. Sie können entweder ein CA-signiertes Serverzertifikat auf dem ONTAP-Cluster installieren oder ein Zertifikat installieren, das der NFS-Service direkt verwendet. Ihre Zertifikate sollten die folgenden Richtlinien erfüllen:

- Jedes Zertifikat muss mit dem Fully Qualified Domain Name (FQDN) des NFS-Servers (der Daten-LIF, auf der TLS aktiviert/konfiguriert wird) als Common Name (CN) konfiguriert werden.
- Jedes Zertifikat muss mit der IP-Adresse oder dem FQDN des NFS-Servers (oder beides) als alternativer Antragstellernamen (SAN) konfiguriert sein. Wenn sowohl IP-Adresse als auch FQDN konfiguriert sind, können NFS-Clients eine Verbindung entweder über die IP-Adresse oder den FQDN herstellen.
- Sie können mehrere NFS-Servicezertifikate für dieselbe LIF installieren, aber nur eines davon kann gleichzeitig als Teil der NFS-TLS-Konfiguration verwendet werden.

Aktivieren oder deaktivieren Sie TLS für NFS-Clients

Sie können die Sicherheit von NFS-Verbindungen verbessern, indem Sie NFS über TLS so konfigurieren, dass alle Daten, die zwischen dem NFS-Client und ONTAP über das Netzwerk gesendet werden, verschlüsselt werden. Dies erhöht die Sicherheit von NFS-Verbindungen. Sie können dies auf einer vorhandenen Storage-VM konfigurieren, die für aktiviert ist **"NFS"**.



NFS über TLS ist in ONTAP 9.15.1 als öffentliche Vorschau verfügbar. NFS über TLS wird in ONTAP 9.15.1 als Vorschauangebot für Produktions-Workloads nicht unterstützt.

Aktivieren Sie TLS

Sie können die TLS-Verschlüsselung für NFS-Clients aktivieren, um die Sicherheit von Daten bei der Übertragung zu erhöhen.

Bevor Sie beginnen

- Siehe "[Anforderungen](#)" Für NFS über TLS, bevor Sie beginnen.
- Weitere Informationen zu diesem Befehl finden Sie auf den Seiten des ONTAP-Handbuchs.

Schritte

1. Wählen Sie eine Storage-VM und eine logische Schnittstelle (LIF) zur Aktivierung von TLS aus.
2. Aktivieren Sie TLS für NFS-Verbindungen auf dieser Storage-VM und Schnittstelle.

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

3. Verwenden Sie die `vserver nfs tls interface show` Befehl zum Anzeigen der Ergebnisse:

```
vserver nfs tls interface show
```

Beispiel

Mit dem folgenden Befehl wird NFS über TLS auf dem aktiviert `data1` LIF von `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 deaktivieren

Sie können TLS für NFS-Clients deaktivieren, wenn Sie die erhöhte Sicherheit für die während der Übertragung verwendeten Daten nicht mehr benötigen.

Bevor Sie beginnen

Weitere Informationen zu diesem Befehl finden Sie auf den Seiten des ONTAP-Handbuchs.

Schritte

1. Wählen Sie eine Storage-VM und eine logische Schnittstelle (LIF) zum Deaktivieren von TLS aus.

2. Deaktivieren Sie TLS für NFS-Verbindungen auf dieser Storage-VM und Schnittstelle.

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

3. Verwenden Sie die `vserver nfs tls interface show` Befehl zum Anzeigen der Ergebnisse:

```
vserver nfs tls interface show
```

Beispiel

Mit dem folgenden Befehl wird NFS über TLS auf dem deaktiviert `data1` LIF von `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.

Bearbeiten einer TLS-Konfiguration

Sie können die Einstellungen einer vorhandenen NFS-over-TLS-Konfiguration ändern. Mit diesem Verfahren können Sie beispielsweise das TLS-Zertifikat aktualisieren.

Bevor Sie beginnen

Weitere Informationen zu diesem Befehl finden Sie auf den Seiten des ONTAP-Handbuchs.

Schritte

1. Wählen Sie eine Storage-VM und eine logische Schnittstelle (Logical Interface, LIF) aus, auf der die TLS-Konfiguration für NFS-Clients geändert werden soll.
2. Ändern Sie die Konfiguration. Wenn Sie ein `status` von `enable` angeben, müssen Sie auch die `certificate-name` Parameter angeben. Ersetzen Sie Werte in Klammern `<>` durch Informationen aus Ihrer Umgebung:

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

3. Verwenden Sie die `vserver nfs tls interface show` Befehl zum Anzeigen der Ergebnisse:

```
vserver nfs tls interface show
```

Beispiel

Mit dem folgenden Befehl wird die Konfiguration von NFS über TLS auf dem geändert `data2` LIF von `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.

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.