



Utilizzo di TLS con NFS per una sicurezza elevata

ONTAP 9

NetApp
June 19, 2024

Sommario

- Utilizzo di TLS con NFS per una sicurezza elevata 1
- Panoramica sull'utilizzo di TLS con NFS per una sicurezza efficace 1
- Attiva o disattiva TLS per i client NFS 1

Utilizzo di TLS con NFS per una sicurezza elevata

Panoramica sull'utilizzo di TLS con NFS per una sicurezza efficace

TLS consente comunicazioni di rete crittografate con una protezione equivalente a e meno complessità rispetto a Kerberos e IPsec. In qualità di amministratore, è possibile attivare, configurare e disattivare TLS per garantire una sicurezza elevata con le connessioni NFSv3 e NFSv4.x utilizzando Gestione di sistema, l'interfaccia CLI di ONTAP o l'API REST di ONTAP.



NFS over TLS è disponibile in ONTAP 9.15.1 come anteprima pubblica. Come offerta di anteprima, NFS su TLS non è supportato per i carichi di lavoro di produzione in ONTAP 9.15.1.

ONTAP utilizza TLS 1,3 per connessioni NFS su TLS.

Requisiti

NFS su TLS richiede certificati X,509. È possibile creare un certificato server con firma CA nel cluster ONTAP oppure installare un certificato utilizzato direttamente dal servizio NFS. I certificati devono soddisfare le seguenti linee guida:

- Ciascun certificato deve essere configurato con il nome di dominio completo (FQDN) del server NFS (la LIF dati su cui verrà attivato/configurato TLS) come nome comune (CN).
- Ciascun certificato deve essere configurato con l'indirizzo IP o il FQDN del server NFS (o entrambi) come nome alternativo soggetto (SAN). Se sono configurati sia l'indirizzo IP che l'FQDN, i client NFS possono connettersi utilizzando l'indirizzo IP o l'FQDN.
- È possibile installare più certificati di servizio NFS per la stessa LIF, ma solo uno di essi può essere in uso alla volta come parte della configurazione NFS TLS.

Attiva o disattiva TLS per i client NFS

È possibile migliorare la sicurezza delle connessioni NFS configurando NFS su TLS in modo da crittografare tutti i dati inviati in rete tra il client NFS e ONTAP. Questo aumenta la sicurezza delle connessioni NFS. È possibile configurarlo su una macchina virtuale di storage esistente per cui è abilitato "NFS".



NFS over TLS è disponibile in ONTAP 9.15.1 come anteprima pubblica. Come offerta di anteprima, NFS su TLS non è supportato per i carichi di lavoro di produzione in ONTAP 9.15.1.

Attiva TLS

È possibile attivare la crittografia TLS per i client NFS per aumentare la sicurezza dei dati in transito.

Prima di iniziare

- Fare riferimento a ["requisiti"](#) Per NFS su TLS prima di iniziare.
- Consultare le pagine del manuale ONTAP per ulteriori informazioni sul comando di questa procedura.

Fasi

1. Scegli una macchina virtuale per lo storage e un'interfaccia logica (LIF) su cui abilitare TLS.
2. Abilitazione di TLS per le connessioni NFS su quella VM storage e sull'interfaccia.

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

3. Utilizzare `vserver nfs tls interface show` per visualizzare i risultati:

```
vserver nfs tls interface show
```

Esempio

Il seguente comando attiva NFS su TLS su data1 LIF del vs1 Macchina virtuale di storage:

```
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.

Disattiva TLS

Se non hai più bisogno di una maggiore sicurezza per i dati in transito, puoi disattivare TLS per i client NFS.

Prima di iniziare

Consultare le pagine del manuale ONTAP per ulteriori informazioni sul comando di questa procedura.

Fasi

1. Scegli una macchina virtuale per lo storage e un'interfaccia logica (LIF) su cui disattivare TLS.

2. Disattiva TLS per connessioni NFS su quella VM storage e sull'interfaccia.

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

3. Utilizzare `vserver nfs tls interface show` per visualizzare i risultati:

```
vserver nfs tls interface show
```

Esempio

Il seguente comando disattiva NFS su TLS su `data1` LIF del `vs1` Macchina virtuale di storage:

```
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.

Modificare una configurazione TLS

È possibile modificare le impostazioni di una configurazione NFS su TLS esistente. Ad esempio, è possibile utilizzare questa procedura per aggiornare il certificato TLS.

Prima di iniziare

Consultare le pagine del manuale ONTAP per ulteriori informazioni sul comando di questa procedura.

Fasi

1. Scegliere una macchina virtuale per lo storage e un'interfaccia logica (LIF) in cui modificare la configurazione TLS per i client NFS.
2. Modificare la configurazione. Se si specifica un `status` di `enable`, è necessario specificare anche `certificate-name` parametro. Sostituire i valori tra parentesi `<>` con le informazioni dell'ambiente:

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

3. Utilizzare `vserver nfs tls interface show` per visualizzare i risultati:

```
vserver nfs tls interface show
```

Esempio

Il seguente comando modifica la configurazione NFS su TLS su `data2` LIF del `vs2` Macchina virtuale di storage:

```
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.

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.