



# Utilisation de TLS avec NFS pour une sécurité renforcée

ONTAP 9

NetApp  
May 17, 2024

# Sommaire

- Utilisation de TLS avec NFS pour une sécurité renforcée ..... 1
- Présentation de l'utilisation de TLS avec NFS pour une sécurité renforcée ..... 1
- Activez ou désactivez TLS pour les clients NFS ..... 1

# Utilisation de TLS avec NFS pour une sécurité renforcée

## Présentation de l'utilisation de TLS avec NFS pour une sécurité renforcée

TLS permet des communications réseau chiffrées avec une sécurité équivalente et moins complexe que Kerberos et IPsec. En tant qu'administrateur, vous pouvez activer, configurer et désactiver TLS pour une sécurité renforcée avec les connexions NFSv3 et NFSv4.x via System Manager, l'interface de ligne de commande ONTAP ou l'API REST ONTAP.



NFS over TLS est disponible dans ONTAP 9.15.1 en tant que préversion publique. À titre de préversion, NFS over TLS n'est pas pris en charge pour les workloads de production dans ONTAP 9.15.1.

ONTAP utilise TLS 1.3 pour les connexions NFS sur TLS.

### De formation

NFS sur TLS nécessite des certificats X.509. Vous pouvez soit créer un certificat de serveur d'installation signé par une autorité de certification sur le cluster ONTAP, soit installer un certificat que le service NFS utilise directement. Vos certificats doivent être conformes aux directives suivantes :

- Chaque certificat doit être configuré avec le nom de domaine complet (FQDN) du serveur NFS (la LIF de données sur laquelle TLS sera activé/configuré) en tant que nom commun (CN).
- Chaque certificat doit être configuré avec l'adresse IP ou le nom de domaine complet du serveur NFS (ou les deux) en tant que nom secondaire de l'objet (SAN). Si l'adresse IP et le nom de domaine complet sont configurés, les clients NFS peuvent se connecter à l'aide de l'adresse IP ou du nom de domaine complet.
- Vous pouvez installer plusieurs certificats de service NFS pour la même LIF, mais un seul d'entre eux peut être utilisé à la fois dans le cadre de la configuration NFS TLS.

## Activez ou désactivez TLS pour les clients NFS

Vous pouvez améliorer la sécurité des connexions NFS en configurant NFS sur TLS de manière à chiffrer toutes les données envoyées sur le réseau entre le client NFS et ONTAP. Cela augmente la sécurité des connexions NFS. Vous pouvez le configurer sur une VM de stockage existante activée pour "NFS".



NFS over TLS est disponible dans ONTAP 9.15.1 en tant que préversion publique. À titre de préversion, NFS over TLS n'est pas pris en charge pour les workloads de production dans ONTAP 9.15.1.

### Activez TLS

Vous pouvez activer le chiffrement TLS pour les clients NFS afin d'augmenter la sécurité des données en

transit.

### Avant de commencer

- Reportez-vous à la ["de formation"](#) Pour NFS sur TLS avant de commencer.
- Reportez-vous aux pages de manuel ONTAP pour plus d'informations sur la commande dans cette procédure.

### Étapes

1. Il convient de choisir une machine virtuelle de stockage et une interface logique (LIF) sur laquelle activer TLS.
2. Activez TLS pour les connexions NFS sur cette machine virtuelle et cette interface de stockage.

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

3. Utilisez le `vserver nfs tls interface show` pour afficher les résultats :

```
vserver nfs tls interface show
```

### Exemple

La commande suivante active NFS sur TLS sur le data1 LIF du vs1 VM de stockage :

```
vserver nfs tls interface enable -vserver vs1 -lif data1 -certificate-name  
cert_vs1
```

```
vserver nfs tls interface show
```

```
          Logical  
Vserver   Interface   Address      TLS Status  TLS Certificate  
Name  
-----  
vs1       data1          10.0.1.1    enabled    cert_vs1  
vs2       data2          10.0.1.2    disabled   -  
2 entries were displayed.
```

### Désactiver TLS

Vous pouvez désactiver TLS pour les clients NFS si vous n'avez plus besoin de la sécurité améliorée pour les données en transit.

### Avant de commencer

Reportez-vous aux pages de manuel ONTAP pour plus d'informations sur la commande dans cette procédure.

### Étapes

1. Choisissez une VM de stockage et une interface logique (LIF) sur laquelle désactiver TLS.
2. Désactivez TLS pour les connexions NFS sur cette VM et cette interface de stockage.

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

3. Utilisez le `vserver nfs tls interface show` pour afficher les résultats :

```
vserver nfs tls interface show
```

### Exemple

La commande suivante désactive NFS sur TLS sur le `data1` LIF du `vs1` VM de stockage :

```
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.

## Modifier une configuration TLS

Vous pouvez modifier les paramètres d'une configuration NFS sur TLS existante. Par exemple, vous pouvez utiliser cette procédure pour mettre à jour le certificat TLS.

### Avant de commencer

Reportez-vous aux pages de manuel ONTAP pour plus d'informations sur la commande dans cette procédure.

### Étapes

1. Choisir une VM de stockage et une interface logique (LIF) sur laquelle modifier la configuration TLS pour les clients NFS.
2. Modifier la configuration. Si vous spécifiez un `status` de `enable`, vous devez également spécifier le `certificate-name` paramètre. Remplacez les valeurs entre parenthèses `<>` par les informations de

votre environnement :

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

3. Utilisez le `vserver nfs tls interface show` pour afficher les résultats :

```
vserver nfs tls interface show
```

### Exemple

La commande suivante modifie la configuration NFS sur TLS sur le `data2` LIF du `vs2` VM de stockage :

```
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.

## Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

## Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.