



Use TLS with NFS for strong security

ONTAP 9

NetApp
June 04, 2024

Table of Contents

- Use TLS with NFS for strong security 1
 - Overview of using TLS with NFS for strong security 1
 - Enable or disable TLS for NFS clients 1

Use TLS with NFS for strong security

Overview of using TLS with NFS for strong security

TLS enables encrypted network communications with equivalent security to and less complexity than Kerberos and IPsec. As an administrator, you can enable, configure, and disable TLS for strong security with NFSv3 and NFSv4.x connections using System Manager, the ONTAP CLI, or the ONTAP REST API.



NFS over TLS is available in ONTAP 9.15.1 as a public preview. As a preview offering, NFS over TLS is not supported for production workloads in ONTAP 9.15.1.

ONTAP uses TLS 1.3 for NFS over TLS connections.

Requirements

NFS over TLS requires X.509 certificates. You can either create and install a CA-signed server certificate on the ONTAP cluster, or you can install a certificate that the NFS service uses directly. Your certificates should meet the following guidelines:

- Each certificate must be configured with the Fully Qualified Domain Name (FQDN) of the NFS server (the data LIF on which TLS will be enabled/configured) as a common name (CN).
- Each certificate must be configured with the IP address or FQDN of the NFS server (or both) as the Subject Alternative Name (SAN). If both IP address and FQDN are configured, NFS clients can connect using either the IP address or FQDN.
- You can install multiple NFS service certificates for the same LIF, but only one of them can be in use at a time as part of the NFS TLS configuration.

Enable or disable TLS for NFS clients

You can enable or disable TLS on a data LIF for NFS clients. When you enable NFS over TLS, the SVM uses TLS to encrypt all data sent over the network between the NFS client and ONTAP. This increases the security of NFS connections.



NFS over TLS is available in ONTAP 9.15.1 as a public preview. As a preview offering, NFS over TLS is not supported for production workloads in ONTAP 9.15.1.

Enable TLS

You can enable TLS encryption for NFS clients to increase security of data in transit.

Before you begin

- Refer to the [requirements](#) for NFS over TLS before you begin.
- Refer to the [manual page](#) for more information about the `vserver nfs tls interface enable` command.

Steps

1. Choose a storage VM and a logical interface (LIF) on which to enable TLS.
2. Enable TLS for NFS connections on that storage VM and interface. Replace values in brackets <> with information from your environment:

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

3. Use the `vserver nfs tls interface show` command to view the results:

```
vserver nfs tls interface show
```

Example

The following command enables NFS over TLS on the `data1` LIF of the `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.

Disable TLS

You can disable TLS for NFS clients if you no longer need the enhanced security for data in transit.



When you disable NFS over TLS, the TLS certificate used for the NFS connection is removed. If you need to enable NFS over TLS in the future, you will need to specify a certificate name again during enablement.

Before you begin

Refer to the [manual page](#) for more information about the `vserver nfs tls interface disable` command.

Steps

1. Choose a storage VM and a logical interface (LIF) on which to disable TLS.
2. Disable TLS for NFS connections on that storage VM and interface. Replace values in brackets <> with information from your environment:

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

3. Use the `vserver nfs tls interface show` command to view the results:

```
vserver nfs tls interface show
```

Example

The following command disables NFS over TLS on the `data1` LIF of the `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.

Edit a TLS configuration

You can change the settings of an existing NFS over TLS configuration. For example, you can use this procedure to update the TLS certificate.

Before you begin

Refer to the [manual page](#) for more information about the `vserver nfs tls interface modify` command.

Steps

1. Choose a storage VM and a logical interface (LIF) on which to modify the TLS configuration for NFS clients.
2. Modify the configuration. If you specify a status of `enable`, you also need to specify the `certificate-name` parameter. Replace values in brackets <> with information from your environment:

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

3. Use the `vserver nfs tls interface show` command to view the results:

```
vserver nfs tls interface show
```

Example

The following command modifies the NFS over TLS configuration on the `data2` LIF of the `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 information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.