Manage NVMe protocol

ONTAP 9

NetApp
February 02, 2026

Table of Contents

Manage NVMe protocol

Start the NVMe service for an SVM

Before you can use the NVMe protocol on your storage virtual machine (SVM), you must start the NVMe service on the SVM.

Before you begin

NVMe must be allowed as a protocol on your system.

The following NVMe protocols are supported:

Protocol	Beginning with …	Allowed by…
TCP	ONTAP 9.10.1	Default
FCP	ONTAP 9.4	Default

Steps

1. Change the privilege setting to advanced:

   ```
   set -privilege advanced
   ```

2. Verify that NVMe is allowed as a protocol:

   ```
   vserver nvme show
   ```

3. Create the NVMe protocol service:

   ```
   vserver nvme create
   ```

4. Start the NVMe protocol service on the SVM:

   ```
   vserver nvme modify -status -admin up
   ```

Delete NVMe service from an SVM

If needed, you can delete the NVMe service from your storage virtual machine (SVM).

Steps

1. Change the privilege setting to advanced:

   ```
   set -privilege advanced
   ```

2. Stop the NVMe service on the SVM:

   ```
   vserver nvme modify -status -admin down
   ```

3. Delete the NVMe service:

   ```
   vserver nvme delete
   ```

Resize a namespace

Beginning with ONTAP 9.10.1, you can use the ONTAP CLI to increase or decrease the size of a NVMe namespace. You can use System Manager to increase the size of a NVMe namespace.

Increase the size of a namespace

System Manager

1. Click **Storage > NVMe Namespaces**.
2. Hoover over the namespace you want to increase, click ⋮, and then click **Edit**.
3. Under **CAPACITY**, change the size of the namespace.

CLI

1. Enter the following command: `vserver nvme namespace modify -vserver` *`SVM_name`* `-path` *`path`* `–size` *`new_size_of_namespace`*

Decrease the size of a namespace

You must use the ONTAP CLI to decrease the size of a NVMe namespace.

1. Change the privilege setting to advanced:

   ```
   set –privilege advanced
   ```

2. Decrease the size of the namespace:

   ```
   vserver nvme namespace modify -vserver SVM_name -path namespace_path -size
   new_size_of_namespace
   ```

Convert a namespace into a LUN

Beginning with ONTAP 9.11.1, you can use the ONTAP CLI to convert in-place an existing NVMe namespace to a LUN.

Before you start

- Specified NVMe namespace should not have any existing maps to a Subsystem.
- Namespace should not be part of a snapshot or on the destination side of SnapMirror relationship as a read-only namespace.
- Since NVMe namespaces are only supported with specific platforms and network cards, this feature only works with specific hardware.

Steps

1. Enter the following command to convert an NVMe namespace to a LUN:

```
lun convert-from-namespace -vserver -namespace-path
```

Learn more about `lun convert-from-namespace` in the ONTAP command reference.

Set up in-band authentication over NVMe

Beginning with ONTAP 9.12.1 you can use the ONTAP command line interface (CLI) to configure in-band (secure), bidirectional and unidirectional authentication between an NVMe host and controller over the NVME/TCP and NVMe/FC protocols using DH-HMAC-CHAP authentication. Beginning with ONTAP 9.14.1, in-band authentication can be configured in System Manager.

To set up in-band authentication, each host or controller must be associated with a DH-HMAC-CHAP key which is a combination of the NQN of the NVMe host or controller and an authentication secret configured by the administrator. For an NVMe host or controller to authenticate its peer, it must know the key associated with the peer.

In unidirectional authentication, a secret key is configured for the host, but not the controller. In bidirectional authentication, a secret key is configured for both the host and the controller.

SHA-256 is the default hash function and 2048-bit is the default DH group.

System Manager

Beginning with ONTAP 9.14.1, you can use System Manager to configure in-band authentication while creating or updating an NVMe subsystem, creating or cloning NVMe namespaces, or adding consistency groups with new NVMe namespaces.

Steps

1. In System Manager, click **Hosts > NVMe Subsystem** and then click **Add**.
2. Add the NVMe subsystem name, and select the storage VM and host operating system.
3. Enter the Host NQN.
4. Select **Use in-band authentication** next to the Host NQN.
5. Provide the host secret and controller secret.

   The DH-HMAC-CHAP key is a combination of the NQN of the NVMe host or controller and an authentication secret configured by the administrator.

6. Select the preferred hash function and DH group for each host.

   If you don’t select a hash function and a DH group, SHA-256 is assigned as the default hash function and 2048-bit is assigned as the default DH group.

7. Optionally, click **Add** and repeat the steps as needed to add more host.
8. Click **Save**.
9. To verify that in-band authentication is enabled, click **System Manager > Hosts > NVMe Subsystem > Grid > Peek view**.

   A transparent key icon next to the host name indicates that unidirectional mode is enabled. An opaque key next to the host name indicates bidirectional mode is enabled.

CLI

Steps

1. Add DH-HMAC-CHAP authentication to your NVMe subsystem:

   ```
   vserver nvme subsystem host add -vserver <svm_name> -subsystem
   <subsystem> -host-nqn <host_nqn> -dhchap-host-secret
   <authentication_host_secret> -dhchap-controller-secret
   <authentication_controller_secret> -dhchap-hash-function <sha-
   256|sha-512> -dhchap-group <none|2048-bit|3072-bit|4096-bit|6144-
   bit|8192-bit>
   ```

   Learn more about `vserver nvme subsystem host add` in the ONTAP command reference.

2. Verify that the DH-HMAC CHAP authentication protocol is added to your host:

   ```
   vserver nvme subsystem host show
   ```

```
  [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
Function
  [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
                                                Authentication
Diffie-Hellman
                                                Group
  [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                                Authentication Mode
```

Learn more about `vserver nvme subsystem host show` in the ONTAP command reference.

3. Verify that the DH-HMAC CHAP authentication was performed during NVMe controller creation:

```
vserver nvme subsystem controller show
```

```
 [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
Function
 [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
                                                Authentication
Diffie-Hellman
                                                Group
 [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                                Authentication Mode
```

Related information

- vserver nvme subsystem controller show

Disable in-band authentication over NVMe

If you have configured in-band authentication over NVMe using DH-HMAC-CHAP, you can choose to disable it at any time.

If you are reverting from ONTAP 9.12.1 or later to ONTAP 9.12.0 or earlier, you must disable in-band authentication before you revert. If in-band authentication using DH-HMAC-CHAP is not disabled, revert will fail.

Steps

1. Remove the host from the subsystem to disable DH-HMAC-CHAP authentication:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. Verify that the DH-HMAC-CHAP authentication protocol is removed from the host:

```
vserver nvme subsystem host show
```

3. Add the host back to the subsystem without authentication:

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

Set up TLS secure channel for NVMe/TCP

Beginning with ONTAP 9.16.1, you can configure TLS secure channel for NVMe/TCP connections. You can use System Manager or the ONTAP CLI to either add a new NVMe subsystem with TLS enabled, or enable TLS for an existing NVMe subsystem. ONTAP does not support TLS hardware offload.

System Manager

Beginning with ONTAP 9.16.1, you can use System Manager to configure TLS for NVMe/TCP connections while creating or updating an NVMe subsystem, creating or cloning NVMe namespaces, or adding consistency groups with new NVMe namespaces.

Steps

1. In System Manager, click **Hosts > NVMe Subsystem** and then click **Add**.
2. Add the NVMe subsystem name, and select the storage VM and host operating system.
3. Enter the Host NQN.
4. Select **Require Transport Layer Security (TLS)** next to the Host NQN.
5. Provide the pre-shared key (PSK).
6. Click **Save**.
7. To verify that TLS secure channel is enabled, select **System Manager > Hosts > NVMe Subsystem > Grid > Peek view**.

CLI

Steps

1. Add an NVMe subsystem host that supports TLS secure channel. You can provide a pre-shared key (PSK) using the `tls-configured-psk` argument:

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -tls-configured-psk <key_text>
```

2. Verify that the NVMe subsystem host is configured for TLS secure channel. You can optionally use the `tls-key-type` argument to only display hosts that are using that key type:

```
vserver nvme subsystem host show -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -tls-key-type {none|configured}
```

3. Verify that the NVMe subsystem host controller is configured for TLS secure channel. You can optionally use any of the `tls-key-type`, `tls-identity`, or `tls-cipher` arguments to only display the controllers that have those TLS attributes:

```
vserver nvme subsystem controller show -vserver <svm_name>
-subsystem <subsystem> -host-nqn <host_nqn> -tls-key-type
{none|configured} -tls-identity <text> -tls-cipher
{none|TLS_AES_128_GCM_SHA256|TLS_AES_256_GCM_SHA384}
```

Related information

- vserver nvme subsystem

Disable TLS secure channel for NVMe/TCP

Beginning with ONTAP 9.16.1, you can configure TLS secure channel for NVMe/TCP connections. If you have configured TLS secure channel for NVMe/TCP connections, you can choose to disable it at any time.

Steps

1. Remove the host from the subsystem to disable TLS secure channel:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. Verify that TLS secure channel is removed from the host:

```
vserver nvme subsystem host show
```

3. Add the host back to the subsystem without TLS secure channel:

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

Related information

- vserver nvme subsystem host

Change NVMe host priority

Beginning with ONTAP 9.14.1, you can configure your NVMe subsystem to prioritize resource allocation for specific hosts. By default, when a host is added to the subsystem, it is assigned a regular priority. Hosts assigned a high priority are allocated larger I/O queue counts and queue-depths.

You can use the ONTAP command line interface (CLI) to manually change the default priority from regular to high. To change the priority assigned to a host, you must remove the host from the subsystem and then add it back.

Steps

1. Verify that the host priority is set to regular:

```
vserver nvme show-host-priority
```

   Learn more about `vserver nvme show-host-priority` in the ONTAP command reference.

2. Remove the host from the subsystem:

```
vserver nvme subsystem host remove –vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

Learn more about `vserver nvme subsystem host remove` in the ONTAP command reference.

3. Verify that the host is removed from the subsystem:

```
vserver nvme subsystem host show
```

Learn more about `vserver nvme subsystem host show` in the ONTAP command reference.

4. Add the host back to the subsystem with high priority:

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
-priority high
```

Learn more about `vserver nvme subsystem host add` in the ONTAP command reference.

Manage automated host discovery of NVMe/TCP controllers in ONTAP

Beginning with ONTAP 9.14.1, host discovery of controllers using the NVMe/TCP protocol is automated by default in IP-based fabrics.

Enable automated host discovery of NVMe/TCP controllers

If you previously disabled automated host discovery, but your needs have changed, you can re-enable it.

Steps

1. Enter advanced privilege mode:

```
set -privilege advanced
```

2. Enable automated discovery:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled true
```

3. Verify automated discovery of NVMe/TCP controllers is enabled.

```
vserver nvme show -fields mdns-service-discovery-enabled
```

Disable automated host discovery of NVMe/TCP controllers

If you do not need NVMe/TCP controllers to be automatically discovered by your host and you detect unwanted multicast traffic on your network, you should disable this functionality.

Steps

1. Enter advanced privilege mode:

```
set -privilege advanced
```

2. Disable automated discovery:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled false
```

3. Verify automated discovery of NVMe/TCP controllers is disabled.

```
vserver nvme show -fields mdns-service-discovery-enabled
```

Disable NVMe host virtual machine identifier in ONTAP

Beginning with ONTAP 9.14.1, by default, ONTAP supports the ability of NVMe/FC hosts to identify virtual machines by a unique identifier and for NVMe/FC hosts to monitor virtual machine resource utilization. This enhances host-side reporting and troubleshooting.

You can use the bootarg to disable this functionality. See the NetApp Knowledge Base: How to disable NVMe host virtual machine identifier in ONTAP.

Copyright information

Trademark information