管理 NVMe 协议

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/ontap/san-admin/start-nvme-fc-service-svm-task.html on February 12, 2026. Always check docs.netapp.com for the latest.

目录

管理 NVMe 协议 1
- 启动 SVM 的 NVMe 服务 1
- 从 SVM 中删除 NVMe 服务 1
- 调整命名空间大小 2
  - 增加命名空间的大小 2
  - 减小命名空间的大小 2
- 将命名空间转换为LUN 2
  - 开始之前 2
- 设置基于NVMe的带内身份验证 3
- 禁用基于NVMe的带内身份验证 5
- 为NVMe/TCP设置TLS安全通道 6
- 禁用NVMe/TCP的TLS安全通道 8
- 更改NVMe主机优先级 8
- 在ONTAP中管理NVMe/TCP控制器的自动主机发现 9
  - 启用NVMe/TCP控制器的自动主机发现 9
  - 禁用NVMe/TCP控制器的主机自动发现 10
- 在ONTAP中禁用NVMe主机虚拟机标识符 10

管理 NVMe 协议

启动 SVM 的 NVMe 服务

在 Storage Virtual Machine （ SVM ）上使用 NVMe 协议之前，必须在 SVM 上启动 NVMe 服务。

开始之前

您的系统上必须允许使用 NVMe 作为协议。

支持以下 NVMe 协议：

协议	开头为 …	允许者 …
TCP	ONTAP 9.10.1	Default
FCP	ONTAP 9.4	Default

步骤

1. 将权限设置更改为高级：

   ```
   set -privilege advanced
   ```

2. 验证是否允许使用 NVMe 作为协议：

   ```
   vserver nvme show
   ```

3. 创建 NVMe 协议服务：

   ```
   vserver nvme create
   ```

4. 在 SVM 上启动 NVMe 协议服务：

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

从 SVM 中删除 NVMe 服务

如果需要，您可以从 Storage Virtual Machine （ SVM ）中删除 NVMe 服务。

步骤

1. 将权限设置更改为高级：

   ```
   set -privilege advanced
   ```

2. 停止 SVM 上的 NVMe 服务：

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

3. 删除 NVMe 服务：

```
vserver nvme delete
```

调整命名空间大小

从 ONTAP 9.10.1 开始，您可以使用 ONTAP 命令行界面增加或减小 NVMe 命名空间的大小。您可以使用 System Manager 增加 NVMe 命名空间的大小。

增加命名空间的大小

System Manager

1. 单击 * 存储 > NVMe 命名空间 * 。
2. 在要增加的命名空间上，单击，然后单击 **Edit**。
3. 在 * 容量 * 下，更改命名空间的大小。

命令行界面

1. 输入以下命令： `vserver nvme namespace modify -vserver` *`SVM_name`* `-path` *`path`* `-size` *`new_size_of_namespace`*

减小命名空间的大小

您必须使用 ONTAP 命令行界面减小 NVMe 命名空间的大小。

1. 将权限设置更改为高级：

```
set -privilege advanced
```

2. 减小命名空间的大小：

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

将命名空间转换为LUN

从ONTAP 9.11.1开始、您可以使用ONTAP命令行界面将现有NVMe命名空间原位转换为LUN。

开始之前

- 指定的NVMe命名空间不应与子系统具有任何现有映射。
- 命名空间不应作为快照的一部分、也不应作为只读命名空间位于SnapMirror关系的目标端。
- 由于NVMe命名空间仅支持特定平台和网卡、因此此功能仅适用于特定硬件。

步骤

1. 输入以下命令将NVMe命名空间转换为LUN：

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

   有关的详细信息 `lun convert-from-namespace`，请参见"ONTAP 命令参考"。

设置基于**NVMe**的带内身份验证

从ONTAP 9.12.1开始、您可以使用ONTAP命令行界面(CLI)通过DH-HMAC-CHAP身份验证、通过NVMe/TCP和NVMe/FC协议在NVMe主机和控制器之间配置带内(安全)双向和单向身份验证。从ONTAP 9.14.1开始、可以在System Manager中配置带内身份验证。

要设置带内身份验证、每个主机或控制器都必须与DH-HMAC-CHAP密钥关联、该密钥是NVMe主机或控制器的NQN与管理员配置的身份验证密钥的组合。要使NVMe主机或控制器对其对等方进行身份验证、它必须知道与对等方关联的密钥。

在单向身份验证中、系统会为主机配置一个机密密钥、但不会为控制器配置此密钥。在双向身份验证中、系统会为主机和控制器配置一个机密密钥。

SHA-256是默认哈希函数、2048位是默认DH组。

System Manager

从ONTAP 9.14.1开始、您可以在创建或更新NVMe子系统、创建或克隆NVMe命名区或使用新NVMe命名区添加一致性组时使用System Manager配置带内身份验证。

步骤

1. 在System Manager中、单击*主机> NVMe子系统*、然后单击*添加*。
2. 添加NVMe子系统名称、然后选择Storage VM和主机操作系统。
3. 输入主机NQN。
4. 选择主机NQN旁边的*使用带内身份验证*。
5. 提供主机密钥和控制器密钥。

   DH-HMAC-CHAP密钥是NVMe主机或控制器的NQN与管理员配置的身份验证密钥的组合。

6. 为每个主机选择首选哈希函数和DH组。

   如果未选择哈希函数和DH组、则会将SHA-256分配为默认哈希函数、并将2048位分配为默认DH组。

7. (可选)单击*Add*并根据需要重复步骤以添加更多主机。
8. 单击 * 保存 * 。
9. 要验证是否已启用带内身份验证、请单击*系统管理器>主机> NVMe子系统>网格> Peek View*。

   主机名旁边的透明密钥图标表示已启用单向模式。主机名旁边的不透明密钥表示已启用双向模式。

命令行界面

步骤

1. 将DH-HMAC-CHAP身份验证添加到NVMe子系统：

```
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>
```

   有关的详细信息 `vserver nvme subsystem host add`，请参见"ONTAP 命令参考"。

2. 验证是否已将DH-HMAC CHAP身份验证协议添加到主机：

```
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
```

有关的详细信息 `vserver nvme subsystem host show`，请参见"ONTAP 命令参考"。

3. 验证是否在创建NVMe控制器期间执行了DH-HMAC CHAP身份验证：

```
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
```

相关信息

- "vserver nvme 子系统控制器显示"

禁用基于NVMe的带内身份验证

如果您已使用DH-HMAC-CHAP通过NVMe配置带内身份验证、则可以随时选择将其禁用。

如果要从ONTAP 9.12.1或更高版本还原到ONTAP 9.12.0或更早版本、则必须在还原之前禁用带内身份验证。如果未禁用使用DH-HMAC-CHAP的带内身份验证、则还原将失败。

步骤

1. 从子系统中删除主机以禁用DH-HMAC-CHAP身份验证：

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

2. 验证是否已从主机中删除DH-HMAC-CHAP身份验证协议：

```
vserver nvme subsystem host show
```

3. 将主机重新添加到子系统而不进行身份验证：

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

为NVMe/TCP设置TLS安全通道

从ONTAP 9.16.1 开始，您可以为 NVMe/TCP 连接配置 TLS 安全通道。您可以使用系统管理器或ONTAP CLI 添加启用了 TLS 的新 NVMe 子系统，或者为现有的 NVMe 子系统启用 TLS。ONTAP不支持 TLS 硬件卸载。

System Manager

从NVMe.161开始、您可以在创建或更新子系统、创建或克隆命名时间或使用新的NVMe/TCP命名时间添加一致性组时使用ONTAP 9为NVMe/TCP连接配置TLS。

步骤

1. 在System Manager中、单击*主机> NVMe子系统*、然后单击*添加*。
2. 添加NVMe子系统名称、然后选择Storage VM和主机操作系统。
3. 输入主机NQN。
4. 选择主机NQN旁边的*需要传输层安全(TLS)*。
5. 提供预共享密钥(PSK)。
6. 单击 * 保存 * 。
7. 要验证是否已启用TLS安全通道、请选择*系统管理器>主机> NVMe子系统>网格> Peek View*。

命令行界面

步骤

1. 添加支持TLS安全通道的NVMe子系统主机。您可以使用 `tls-configured-psk`争论：

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

2. 验证是否已为NVMe子系统主机配置TLS安全通道。您可以选择使用 `tls-key-type`参数仅显示正在使用该密钥类型的主机：

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

3. 验证是否已为NVMe子系统主机控制器配置TLS安全通道。您可以选择使用任何 `tls-key-type`、 `tls-identity`或 `tls-cipher`参数仅显示具有这些TLS属性的控制器：

```
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}
```

相关信息

- "Vserver NVMe子系统"

禁用NVMe/TCP的TLS安全通道

从tls.16.1开始、您可以为NVMe/TCP连接配置ONTAP 9安全通道。如果您已为NVMe/TCP连接配置TLS安全通道、则可以随时选择将其禁用。

步骤

1. 从子系统中删除主机以禁用TLS安全通道：

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

2. 验证是否已从主机中删除TLS安全通道：

```
vserver nvme subsystem host show
```

3. 将主机添加回不具有TLS安全通道的子系统：

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

相关信息

- "Vserver NVMe子系统主机"

更改NVMe主机优先级

从ONTAP 9.14.1开始、您可以对NVMe子系统进行配置、以确定特定主机的资源分配优先级。默认情况下、将主机添加到子系统时、系统会为其分配常规优先级。分配了高优先级的主机将分配更大的I/O队列计数和队列深度。

您可以使用ONTAP命令行界面(CLI)手动将默认优先级从常规更改为高。 要更改分配给主机的优先级、您必须从子系统中删除该主机、然后将其重新添加。

步骤

1. 验证主机优先级是否设置为常规：

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

   有关的详细信息 `vserver nvme show-host-priority`，请参见"ONTAP 命令参考"。

2. 从子系统中删除主机：

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

有关的详细信息 `vserver nvme subsystem host remove`，请参见"ONTAP 命令参考"。

3. 验证是否已从子系统中删除此主机：

```
vserver nvme subsystem host show
```

有关的详细信息 `vserver nvme subsystem host show`，请参见"ONTAP 命令参考"。

4. 将主机重新添加到具有高优先级的子系统：

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

有关的详细信息 `vserver nvme subsystem host add`，请参见"ONTAP 命令参考"。

在ONTAP中管理NVMe/TCP控制器的自动主机发现

从ONTAP 9.14.1开始、在基于IP的网络结构中、使用NVMe/TCP协议自动发现控制器。

启用NVMe/TCP控制器的自动主机发现

如果您之前禁用了自动主机发现、但需求发生了变化、则可以重新启用它。

步骤

1. 进入高级权限模式：

```
set -privilege advanced
```

2. 启用自动发现：

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

3. 验证是否已启用NVMe/TCP控制器的自动发现。

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

禁用NVMe/TCP控制器的主机自动发现

如果您不需要主机自动发现NVMe/TCP控制器、并且在网络上检测到不需要的多播流量、则应禁用此功能。

步骤

1. 进入高级权限模式：

```
set -privilege advanced
```

2. 禁用自动发现：

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

3. 验证是否已禁用NVMe/TCP控制器的自动发现。

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

在ONTAP中禁用NVMe主机虚拟机标识符

从ONTAP 9.14.1开始、默认情况下、ONTAP支持NVMe/FC主机通过唯一标识符标识虚拟机、并支持NVMe/FC主机监控虚拟机资源利用率。这样可以增强主机端报告和故障排除功能。

您可以使用 bootarg 来禁用此功能。查看"NetApp知识库：如何在ONTAP中禁用 NVMe 主机虚拟机标识符"。

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。