



Managen des NVMe-Protokolls

ONTAP 9

NetApp
April 24, 2024

Inhalt

- Managen des NVMe-Protokolls 1
 - Starten Sie den NVMe-Service für eine SVM 1
 - Löschen des NVMe-Service aus einer SVM 1
 - Größe eines Namespace ändern 2
 - Konvertieren eines Namespace in eine LUN 2
 - In-Band-Authentifizierung über NVMe einrichten 3
 - In-Band-Authentifizierung über NVMe deaktiviert 5
 - Ändern der NVMe-Host-Priorität 6
 - Management automatischer Hosterkennung von NVMe/TCP Controllern 7
 - Deaktivieren Sie die Kennung der virtuellen NVMe-Host-Maschine 8

Managen des NVMe-Protokolls

Starten Sie den NVMe-Service für eine SVM

Bevor Sie das NVMe-Protokoll für Ihre Storage Virtual Machine (SVM) verwenden können, müssen Sie den NVMe-Service auf der SVM starten.

Bevor Sie beginnen

NVMe muss als Protokoll auf Ihrem System zugelassen sein.

Folgende NVMe-Protokolle werden unterstützt:

Protokoll	Beginnend mit ...	Zulässig von...
TCP	ONTAP 9.10.1	Standard
FCP	ONTAP 9.4	Standard

Schritte

1. Ändern Sie die Berechtigungseinstellung in erweitert:

```
set -privilege advanced
```

2. Vergewissern Sie sich, dass NVMe als Protokoll zulässig ist:

```
vserver nvme show
```

3. Erstellung des NVMe-Protokollservice:

```
vserver nvme create
```

4. Starten des NVMe-Protokollservice auf der SVM:

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

Löschen des NVMe-Service aus einer SVM

Bei Bedarf können Sie den NVMe-Service von Ihrer Storage Virtual Machine (SVM) löschen.

Schritte

1. Ändern Sie die Berechtigungseinstellung in erweitert:

```
set -privilege advanced
```

2. Beenden Sie den NVMe-Service auf der SVM:

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

3. Löschen Sie den NVMe-Service:


```
vserver nvme delete
```

Größe eines Namespace ändern

Ab ONTAP 9.10.1 können Sie mithilfe der ONTAP CLI den NVMe Namespace erhöhen oder verringern. Mit System Manager kann der NVMe Namespace vergrößert werden.

Vergrößern Sie den Namespace

System Manager

1. Klicken Sie auf **Storage > NVMe Namespaces**.
2. Klicken Sie auf den Namespace, den Sie vergrößern möchten , Und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie unter **CAPACITY** die Größe des Namespace.

CLI

1. Geben Sie den folgenden Befehl ein: `vserver nvme namespace modify -vserver SVM_name -path path -size new_size_of_namespace`

Verkleinern Sie die Größe eines Namespace

Sie müssen die ONTAP-CLI verwenden, um die Größe eines NVMe Namespace zu reduzieren.

1. Ändern Sie die Berechtigungseinstellung in erweitert:

```
set -privilege advanced
```

2. Verkleinern Sie die Größe des Namespace:

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

Konvertieren eines Namespace in eine LUN

Ab ONTAP 9.11.1 können Sie die ONTAP CLI verwenden, um einen vorhandenen NVMe Namespace in eine LUN zu konvertieren.

Bevor Sie beginnen

- Der angegebene NVMe-Namespace sollte keine vorhandenen Zuordnungen zu einem Subsystem haben.
- Namespace sollte nicht Teil einer Snapshot-Kopie oder auf der Zielseite der SnapMirror-Beziehung als schreibgeschützter Namespace sein.
- Da NVMe Namespaces nur für bestimmte Plattformen und Netzwerkkarten unterstützt werden, funktioniert diese Funktion nur mit bestimmten Hardware.

Schritte

1. Geben Sie den folgenden Befehl ein, um einen NVMe Namespace in eine LUN zu konvertieren:

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

In-Band-Authentifizierung über NVMe einrichten

Ab ONTAP 9.12.1 können Sie die ONTAP Befehlszeilenschnittstelle (CLI) verwenden, um die bandinterne (sichere), bidirektionale und unidirektionale Authentifizierung zwischen einem NVMe Host und Controller über die NVMe/TCP- und NVMe/FC-Protokolle unter Verwendung der DH-HMAC-CHAP-Authentifizierung zu konfigurieren. Ab ONTAP 9.14.1 kann die in-Band-Authentifizierung in System Manager konfiguriert werden.

Zur Einrichtung der bandinternen Authentifizierung muss jeder Host oder Controller einem DH-HMAC-CHAP-Schlüssel zugeordnet sein. Dieser Schlüssel ist eine Kombination aus NQN des NVMe-Hosts oder -Controllers und einem vom Administrator konfigurierten Authentifizierungsschlüssel. Damit ein NVMe-Host oder -Controller seinen Peer authentifizieren kann, muss er den dem Peer zugeordneten Schlüssel kennen.

Bei der unidirektionalen Authentifizierung wird ein geheimer Schlüssel für den Host konfiguriert, nicht jedoch für den Controller. Bei der bidirektionalen Authentifizierung wird ein geheimer Schlüssel sowohl für den Host als auch für den Controller konfiguriert.

SHA-256 ist die Standard-Hash-Funktion und 2048-Bit ist die Standard-DH-Gruppe.

System Manager

Ab ONTAP 9.14.1 können Sie die in-Band-Authentifizierung über System Manager bei der Erstellung oder Aktualisierung eines NVMe-Subsystems, der Erstellung oder dem Klonen von NVMe-Namespaces oder dem Hinzufügen von Konsistenzgruppen mit neuen NVMe-Namespaces konfigurieren.

Schritte

1. Klicken Sie im System Manager auf **Hosts > NVMe-Subsystem** und dann auf **Hinzufügen**.
2. Fügen Sie den Namen des NVMe-Subsystems hinzu und wählen Sie die Storage-VM und das Host-Betriebssystem aus.
3. Geben Sie die Host-NQN ein.
4. Wählen Sie **bandinterne Authentifizierung verwenden** neben dem Host-NQN.
5. Geben Sie den Host-Schlüssel und den Controller-Schlüssel ein.

Der DH-HMAC-CHAP-Schlüssel ist eine Kombination aus dem NQN des NVMe-Hosts oder -Controllers und einem vom Administrator konfigurierten Authentifizierungsschlüssel.

6. Wählen Sie die bevorzugte Hash-Funktion und die DH-Gruppe für jeden Host aus.

Wenn Sie keine Hash-Funktion und keine DH-Gruppe auswählen, wird SHA-256 als Standard-Hash-Funktion zugewiesen und 2048-Bit als Standard-DH-Gruppe zugewiesen.

7. Klicken Sie optional auf **Hinzufügen** und wiederholen Sie die Schritte, um weitere Hosts hinzuzufügen.
8. Klicken Sie Auf **Speichern**.
9. Um zu überprüfen, ob die bandinterne Authentifizierung aktiviert ist, klicken Sie auf **System Manager > Hosts > NVMe-Subsystem > Grid > Peek View**.

Ein transparentes Schlüsselsymbol neben dem Hostnamen zeigt an, dass der unidirektionale Modus aktiviert ist. Ein undurchsichtiger Schlüssel neben dem Hostnamen zeigt an, dass der bidirektionale Modus aktiviert ist.

CLI

Schritte

1. Fügen Sie Ihrem NVMe-Subsystem DH-HMAC-CHAP-Authentifizierung hinzu:

```
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>
```

2. Vergewissern Sie sich, dass das DH-HMAC CHAP-Authentifizierungsprotokoll Ihrem Host hinzugefügt wird:

```
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} ]
Diffie-Hellman
Group
[ -dhchap-mode {none|unidirectional|bidirectional} ]
Authentication Mode
```

3. Überprüfen Sie, ob die DH-HMAC CHAP-Authentifizierung während der Erstellung des NVMe-Controllers durchgeführt wurde:

```
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} ]
Diffie-Hellman
Group
[ -dhchap-mode {none|unidirectional|bidirectional} ]
Authentication Mode
```

In-Band-Authentifizierung über NVMe deaktiviert

Wenn Sie die bandinterne Authentifizierung über NVMe mit DH-HMAC-CHAP konfiguriert haben, können Sie diese jederzeit deaktivieren.

Wenn Sie von ONTAP 9.12.1 oder höher auf ONTAP 9.12.0 oder früher zurücksetzen, müssen Sie die bandinterne Authentifizierung vor dem Zurücksetzen deaktivieren. Wenn die bandinterne Authentifizierung mit DH-HMAC-CHAP nicht deaktiviert ist, schlägt die Wiederherstellung fehl.

Schritte

1. Entfernen Sie den Host aus dem Subsystem, um die DH-HMAC-CHAP-Authentifizierung zu deaktivieren:

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

2. Vergewissern Sie sich, dass das DH-HMAC-CHAP-Authentifizierungsprotokoll vom Host entfernt wird:

```
vserver nvme subsystem host show
```

3. Fügen Sie den Host ohne Authentifizierung wieder zum Subsystem hinzu:

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

Ändern der NVMe-Host-Priorität

Ab ONTAP 9.14.1 können Sie das NVMe-Subsystem so konfigurieren, dass es die Ressourcenzuweisung für bestimmte Hosts priorisiert. Wenn ein Host dem Subsystem hinzugefügt wird, wird ihm standardmäßig eine reguläre Priorität zugewiesen. Hosts, denen eine hohe Priorität zugewiesen ist, werden eine größere Anzahl von I/O-Warteschlangen und eine größere Warteschlangentiefe zugewiesen.

Mithilfe der ONTAP Befehlszeilenschnittstelle (CLI) kann die Standardpriorität manuell von „Normal“ auf „hoch“ geändert werden. Um die einem Host zugewiesene Priorität zu ändern, müssen Sie den Host aus dem Subsystem entfernen und ihn dann wieder hinzufügen.

Schritte

1. Vergewissern Sie sich, dass die Host-Priorität auf „Normal“ eingestellt ist:

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

2. Entfernen Sie den Host aus dem Subsystem:

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

3. Überprüfen Sie, ob der Host aus dem Subsystem entfernt wurde:

```
vserver nvme subsystem host show
```

4. Fügen Sie den Host wieder dem Subsystem mit hoher Priorität hinzu:


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

Management automatischer Hosterkennung von NVMe/TCP Controllern

Ab ONTAP 9.14.1 ist die Host-Erkennung von Controllern über das NVMe/TCP-Protokoll in IP-basierten Fabrics standardmäßig automatisiert.

Automatische Host-Erkennung von NVMe/TCP Controllern

Wenn Sie die automatische Hosterkennung zuvor deaktiviert haben, Ihre Anforderungen jedoch geändert haben, können Sie sie erneut aktivieren.

Schritte

1. Wechseln Sie in den erweiterten Berechtigungsmodus:

```
set -privilege advanced
```

2. Automatische Erkennung aktivieren:

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

3. Überprüfen Sie, ob die automatische Erkennung von NVMe/TCP-Controllern aktiviert ist.

```
vserver nvme show
```

Deaktivieren Sie die automatische Host-Erkennung von NVMe/TCP-Controllern

Wenn NVMe/TCP-Controller nicht automatisch von Ihrem Host erkannt werden müssen und Sie unerwünschten Multicast-Datenverkehr in Ihrem Netzwerk erkennen, sollten Sie diese Funktion deaktivieren.

Schritte

1. Wechseln Sie in den erweiterten Berechtigungsmodus:

```
set -privilege advanced
```

2. Automatische Erkennung deaktivieren:

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

3. Vergewissern Sie sich, dass die automatische Erkennung von NVMe/TCP-Controllern deaktiviert ist.

```
vserver nvme show
```

Deaktivieren Sie die Kennung der virtuellen NVMe-Host-Maschine

Ab ONTAP 9.14.1 unterstützt ONTAP standardmäßig die Möglichkeit von NVMe/FC-Hosts, Virtual Machines über eine eindeutige Kennung zu identifizieren und für NVMe/FC-Hosts die Auslastung der Virtual-Machine-Ressourcen zu überwachen. Dies verbessert die hostseitige Berichterstellung und Fehlerbehebung.

Sie können diese Funktion mit dem Bootarg deaktivieren.

Schritt

1. Deaktivieren Sie die Kennung der virtuellen Maschine:

```
bootargs set fct_sli_appid_off <port>, <port>
```

Im folgenden Beispiel wird die VMID auf Port 0g und Port 0i deaktiviert.

```
bootargs set fct_sli_appid_off 0g,0i  
  
fct_sli_appid_off == 0g,0i
```

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.