NVMeプロトコルを管理します。

ONTAP 9

NetApp
December 20, 2024

目次

NVMeプロトコルを管理します。

SVMのNVMeサービスを開始する

Storage Virtual Machine（SVM）でNVMeプロトコルを使用する前に、SVMでNVMeサービスを開始する必要があります。

開始する前に

システムでNVMeプロトコルが許可されている必要があります。

次のNVMeプロトコルがサポートされます。

プロトコル	先頭のドキュメント	許可するユーザ
TCP	ONTAP 9 10.1	デフォルト
FCP	ONTAP 9.4	デフォルト

手順

1. 権限の設定をadvancedに変更します。

   ```
   set -privilege advanced
   ```

2. NVMeプロトコルが許可されていることを確認します。

   ```
   vserver nvme show
   ```

3. NVMeプロトコルサービスを作成します。

   ```
   vserver nvme create
   ```

4. SVMでNVMeプロトコルサービスを開始します。

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

SVMからNVMeサービスを削除する

必要に応じて、Storage Virtual Machine（SVM）からNVMeサービスを削除できます。

手順

1. 権限の設定をadvancedに変更します。

   ```
   set -privilege advanced
   ```

2. SVMでNVMeサービスを停止します。

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

3. NVMeサービスを削除します。

   ```
   vserver nvme delete
   ```

ネームスペースのサイズを変更する

ONTAP 9 .10.1以降では、ONTAP CLIを使用してNVMeネームスペースのサイズを拡張または縮小できます。System Managerを使用して、NVMeネームスペースのサイズを拡張できます。

ネームスペースのサイズを拡張する

System Manager

1. Storage > NVMe Namespaces * をクリックします。
2. 拡張するネームスペースにカーソルを合わせ、をクリックし、 *[編集]*をクリックします。
3. 容量 * で、ネームスペースのサイズを変更します。

CLI

1. 次のコマンドを入力します。 `vserver nvme namespace modify -vserver` *`SVM_name`* `-path` *`path`* `-size` *`new_size_of_namespace`*

ネームスペースのサイズを縮小する

NVMeネームスペースのサイズを縮小するには、ONTAP CLIを使用する必要があります。

1. 権限の設定をadvancedに変更します。

   ```
   set -privilege advanced
   ```

2. ネームスペースのサイズを縮小します。

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

ネームスペースを**LUN**に変換する

開始する前に

11.1以降では、**ONTAP CLI**を使用して、既存の**NVMe**ネームスペースをインプレースで**ONTAP 9**に変換できます。

- 指定したNVMeネームスペースにサブシステムへの既存のマッピングが含まれていないことを確認してください。
- ネームスペースをSnapshotコピーの一部にしたり、SnapMirror関係のデスティネーション側で読み取り専用ネームスペースとして使用したりすることはできません。

- NVMeネームスペースは特定のプラットフォームとネットワークカードでのみサポートされるため、この機能は特定のハードウェアでのみ機能します。

手順

1. 次のコマンドを入力して、NVMeネームスペースをLUNに変換します。

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

NVMe経由のインバンド認証の設定

12.1以降でONTAP 9は、ONTAPコマンドラインインターフェイス（CLI）を使用して、DH-HMAC-CHAP認証を使用して、NVMe/TCPおよびNVMe/FCプロトコルを介したNVMeホストとコントローラ間のインバンド（セキュア）双方向および単方向認証を設定できます。ONTAP 9.14.1以降では、インバンド認証をSystem Managerで設定できます。

インバンド認証を設定するには、各ホストまたはコントローラにDH-HMAC-CHAPキーを関連付ける必要があります。DH-HMAC-CHAPキーは、NVMeホストまたはコントローラのNQNと管理者が設定した認証シークレットを組み合わせたものです。NVMeホストまたはコントローラがピアを認証するには、ピアに関連付けられたキーを認識している必要があります。

単方向認証では、コントローラではなくホストにシークレットキーが設定されます。双方向認証では、ホストとコントローラの両方にシークレットキーが設定されます。

SHA-256がデフォルトのハッシュ関数で、2048ビットがデフォルトのDHグループです。

System Manager

14.1以降では、サブシステムの作成または更新、NVMeネームスペースの作成またはクローニング、新しいONTAP 9ネームスペースを使用した整合グループの追加時に、System Managerを使用してインバンド認証を設定できます。

手順

1. System Managerで、**[ホスト]>[NVMe**サブシステム**]***をクリックし、[追加]*をクリックします。
2. NVMeサブシステム名を追加し、Storage VMとホストオペレーティングシステムを選択します。
3. ホストのNQNを入力します。
4. [Host NQN]の横にある*[Use in-band authentication]*を選択します。
5. ホストシークレットとコントローラシークレットを指定します。

   DH-HMAC-CHAPキーは、NVMeホストまたはコントローラのNQNと管理者が設定した認証シークレットを組み合わせたものです。

6. ホストごとに使用するハッシュ関数とDHグループを選択します。

   ハッシュ関数とDHグループを選択しない場合、SHA-256がデフォルトのハッシュ関数として割り当てられ、2048ビットがデフォルトのDHグループとして割り当てられます。

7. 必要に応じて、*[追加]*をクリックし、必要に応じて手順を繰り返してホストを追加します。
8. [保存（ Save ）] をクリックします。
9. インバンド認証が有効になっていることを確認するには、*[システムマネージャ]>[ホスト]>[NVMeサブシステム]>[グリッド]>[ピークビュー]*をクリックします。

   ホスト名の横にあるトランスペアレントキーアイコンは、単方向モードがイネーブルであることを示します。ホスト名の横にある不透明キーは、双方向モードが有効であることを示します。

CLI

手順

1. NVMeサブシステムにDH-HMAC-CHAP認証を追加します。

```
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. DH-HMAC CHAP認証プロトコルがホストに追加されたことを確認します。

```
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
```

3. NVMeコントローラの作成時にDH-HMAC CHAP認証が実行されたことを確認します。

```
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
```

NVMe経由のインバンド認証を無効にする

DH-HMAC-CHAPを使用してNVMe経由のインバンド認証を設定している場合は、いつでも無効にすることができます。

ONTAP 9.12.1以降からONTAP 9.12.0以前にリバートする場合は、リバート前にインバンド認証を無効にする必要があります。DH-HMAC-CHAPを使用するインバンド認証が無効になっていない場合、リバートは失敗します。

手順

1. ホストをサブシステムから削除してDH-HMAC-CHAP認証を無効にします。

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

2. DH-HMAC-CHAP認証プロトコルがホストから削除されたことを確認します。

```
vserver nvme subsystem host show
```

3. 認証を使用せずにホストをサブシステムに再度追加します。

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

NVMe/TCP用のTLSセキュアチャネルのセットアップ

ONTAP 9 .16.1以降では、NVMe/TCP接続用にTLSセキュアチャネルを設定できます。System ManagerまたはONTAP CLIを使用して、TLSが有効になっている新しいNVMeサブシステムを追加するか、既存のNVMeサブシステムに対してTLSを有効にすることができます。

System Manager

NVMe.16.1以降では、サブシステムの作成または更新、ネームスペースの作成またはクローニング、新しいONTAP 9ネームスペースを使用した整合性グループの追加時に、System Managerを使用してNVMe/TCP接続用のTLSを設定できます。

手順

1. System Managerで、**[ホスト]>[NVMe**サブシステム**]***をクリックし、[追加]*をクリックします。
2. NVMeサブシステム名を追加し、Storage VMとホストオペレーティングシステムを選択します。
3. ホストのNQNを入力します。
4. [Host NQN]の横にある*[Require Transport Layer Security（TLS）]*を選択します。
5. 事前共有キー（PSK）を指定します。
6. [保存（ Save ）] をクリックします。
7. TLSセキュアチャネルが有効になっていることを確認するには、*[システムマネージャ]>[ホスト]>[NVMeサブシステム]>[グリッド]>[ピークビュー]*を選択します。

CLI

手順

1. TLSセキュアチャネルをサポートするNVMeサブシステムホストを追加します。引数を使用して事前共有キー（PSK）を指定することも、引数を使用して生成されたPSKを使用すること `tls-generated-psk`もできます `tls-configured-psk`。

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> {-tls-configured-psk <key_text> |
-tls-generated-psk true}
```

2. NVMeサブシステムホストがTLSセキュアチャネル用に設定されていることを確認します。オプションで引数を使用すると、そのキータイプを使用しているホストのみを表示でき `tls-key-type`ます。

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

3. NVMeサブシステムのホストコントローラがTLSセキュアチャネル用に設定されていることを確認します。必要に応じて、 `tls-identity`、、または `tls-cipher`引数を使用して、それらのTLS属性を持つコントローラのみを表示でき `tls-key-type`ます。

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

詳細

これらのコマンドについては、ONTAPのマニュアルページを参照してください。

- "Vserver nvmeサブシステムhost add"
- "vserver nvme subsystem host show」コマンドを使用します"
- "vserver nvme subsystem controller show」というコマンドを使用します"

NVMe/TCPのTLSセキュアチャネルを無効にする

ONTAP 9 .16.1以降では、NVMe/TCP接続用にTLSセキュアチャネルを設定できます。NVMe/TCP接続用にTLSセキュアチャネルを設定している場合は、いつでも無効にすることができます。

手順

1. サブシステムからホストを削除してTLSセキュアチャネルを無効にします。

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

2. TLSセキュアチャネルがホストから削除されたことを確認します。

```
vserver nvme subsystem host show
```

3. TLSセキュアチャネルがないサブシステムにホストを再度追加します。

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

詳細

これらのコマンドについては、ONTAPのマニュアルページを参照してください。

- "Vserver nvmeサブシステムhost add"
- "Vserver NVMeサブシステムホストが削除されます"
- "vserver nvme subsystem host show」コマンドを使用します"

NVMeホスト優先度の変更

nvme .14.1以降では、ONTAP 9サブシステムを設定して、特定のホストに対するリソース割り当ての優先順位を設定できます。デフォルトでは、ホストがサブシステムに追加されると、通常の優先度が割り当てられます。高い優先度を割り当てられたホストには、より多くのI/Oキュー数とキュー深度が割り当てられます。

ONTAPのコマンドラインインターフェイス（CLI）を使用して、デフォルト優先度を手動で標準から高に変更できます。ホストに割り当てられている優先度を変更するには、サブシステムからホストを削除してから再度追加する必要があります。

手順

1. ホストプライオリティがRegularに設定されていることを確認します。

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

2. サブシステムからホストを削除します。

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

3. ホストがサブシステムから削除されたことを確認します。

```
vserver nvme subsystem host show
```

4. 優先度が高いサブシステムにホストを再度追加します。

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

NVMe / TCPコントローラのホストの自動検出を管理します。

ONTAP 9 14.1以降、IPベースのファブリックでは、NVMe/TCPプロトコルを使用するコントローラのホスト検出がデフォルトで自動化されます。

NVMe / TCPコントローラのホスト検出を自動化

以前に自動ホスト検出を無効にしていたが、ニーズが変わった場合は、再度有効にすることができます。

手順

1. advanced権限モードに切り替えます。

```
set -privilege advanced
```

2. 自動検出を有効にします。

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

3. NVMe/TCPコントローラの自動検出が有効になっていることを確認します。

```
vserver nvme show
```

NVMe / TCPコントローラのホストの自動検出を無効にする

NVMe / TCPコントローラをホストで自動的に検出する必要がなく、ネットワークで不要なマルチキャストトラフィックが検出された場合は、この機能を無効にする必要があります。

手順

1. advanced権限モードに切り替えます。

```
set -privilege advanced
```

2. 自動検出を無効にします。

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

3. NVMe/TCPコントローラの自動検出が無効になっていることを確認します。

```
vserver nvme show
```

NVMeホスト仮想マシン識別子の無効化

ONTAP 9 14.1以降では、デフォルトで、ONTAPでNVMe/FCホストが一意の識別子で仮想マシンを識別し、NVMe/FCホストが仮想マシンのリソース利用率を監視できるようになりました。これにより、ホスト側のレポート作成とトラブルシューティングが強化されます。

この機能は、bootargを使用して無効にできます。

ステップ

1. 仮想マシンIDを無効にします。

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

次の例は、ポート0gとポート0iのVMIDを無効にします。

```
bootargs set fct_sli_appid_off 0g,0i

fct_sli_appid_off == 0g,0i
```

著作権に関する情報

商標に関する情報